LANDTAG
NORDRHEIN-WESTFALEN
18. WAHLPERIODE

VORLAGE
18/2354

Alle Abgeordneten

Ministerium der Finanzen
des Landes Nordrhein-Westfalen
Der Minister

07. März 2024

Vorlage
an den Unterausschuss Personal
des Haushalts- und Finanzausschusses
des Landtags Nordrhein-Westfalen

Bericht der Landesregierung zur Digitalisierungsoffensive in der Finanzverwaltung

Sitzung des Unterausschusses Personal des Haushalts- und Finanzausschusses des Landtags Nordrhein-Westfalen am 12. März 2024

Anlagen: 6

1. Bundesamt für Sicherheit in der Informationstechnik (Oktober 2023): „Die Lage der IT-Sicherheit in Deutschland 2023“
2. Bundesamt für Sicherheit in der Informationstechnik (Version 1.0): „BSI-Standard 200-2. IT-Grundschutz-Methodik“
3. Pressemitteilung - Ministerium der Finanzen des Landes Nordrhein-Westfalen (23.10.2023): „Grundsteinlegung in Kaarst: Meilenstein für das neue Rechenzentrum der Finanzverwaltung“
4. Pressemitteilung - Ministerium der Finanzen des Landes Nordrhein-Westfalen (15.01.2024): „Landesamt zur Bekämpfung der Finanzkriminalität nimmt die Arbeit auf“
5. Vorlage 18/1482 (12.08.2023): „Modernisierungsprogramm ‚Finanzverwaltung *für* Nordrhein-Westfalen‘“
6. Vorlage 18/1665 (21.09.2023): „Erläuterung zur Verpflichtungsermächtigung im Haushaltsplanentwurf 2024, Einzelplan 20, zur Finanzierung des Neubauvorhabens Verwaltungszentrum Haroldstraße 5 in Düsseldorf“

Im Zukunftsvertrag der schwarz-grünen Koalition haben sich die Koalitionspartner auf eine Modernisierung und Digitalisierung der Finanzverwal-

Dienstgebäude und
Lieferanschrift:
Jägerhofstr. 6
40479 Düsseldorf
Telefon (0211) 4972-0
Telefax (0211) 4972-1217
Poststelle@fm.nrw.de
www.fm.nrw.de

Öffentliche Verkehrsmittel:
U74 bis U79
Haltestelle
Heinrich Heine Allee

tung verständigt. Sie haben das Ziel wie folgt formuliert: „*Die Leistungsfähigkeit der Finanzverwaltung wollen wir durch geeignete Maßnahmen – digitale Kooperation, sichere und gemeinsame Datensysteme, Nutzung der elektronischen Steuerakte und verstärkter Einsatz von KI – ganzheitlich weiter stärken. Wir werden daher die Steuerfahndung und die Steuerveranlagung stärken und aufgabengerecht und gezielt fortentwickeln.*" (Zukunftsvertrag für Nordrhein-Westfalen, S. 140). Nachfolgender Bericht stellt die aktuelle Lage, den bisher erreichten Umsetzungsstand und die weiteren Schritte der Digitalisierungsoffensive in der Finanzverwaltung dar.

Mit ihren rund 33.000 Beschäftigten in unterschiedlichen Behörden bildet die Finanzverwaltung des Landes Nordrhein-Westfalen eine zentrale Säule der gesamten Landesverwaltung. Die Finanzverwaltung umfasst die Steuerverwaltung mit dem Kerngeschäft der Festsetzung und Erhebung von Steuern, aber auch viele andere Aufgabenbereiche, die im Landesamt für Finanzen (LaFin), dem Landesamt für Besoldung und Versorgung (LBV NRW), dem Rechenzentrum der Finanzverwaltung Nordrhein-Westfalen (RZF) und dem Bau- und Liegenschaftsbetrieb Nordrhein-Westfalen (BLB NRW) bearbeitet werden. Angesichts vielfältiger Aufgaben ist ein zentraler Schlüssel für die Handlungs- und Zukunftsfähigkeit der Finanzverwaltung ein optimales Zusammenwirken ihrer Beschäftigten dank innovativer, aber auch insbesondere arbeitserleichternden IT-Lösungen. Je stärker technische Lösungen mit den Arbeitsabläufen der Beschäftigten der Finanzverwaltung verwoben werden, desto zentraler werden Fragen der Leistungsfähigkeit, der Betriebsstabilität sowie der Betriebs- und Cybersicherheit der IT.

Die IT-Leistungen der Finanzverwaltung gliedern sich im Kern in die Schwerpunkte *Steuer-IT* und bestimmte Aufgaben der *ressort- und behördenübergreifenden Digitalisierung* mit jeweils spezifischen Themen. Darüber hinaus gibt es auch ressortinterne IT-Leistungen innerhalb der Finanzverwaltung, die das Rechenzentrum der Finanzverwaltung erbringt.

Angesichts gestiegener Erwartungen von Bürgerinnen und Bürgern, Beschäftigen und Unternehmen an die öffentliche Verwaltung und vor dem Hintergrund des Modernisierungsbedarfs im Bereich der IT, des Fachkräftemangels und zunehmender Bedrohungslagen für die IT-Sicherheit

besteht für die Finanzverwaltung ein erheblicher Aufgabenumfang im komplexen Umfeld der IT.

Die IT ist entscheidend für die Zukunftsfähigkeit der (Finanz-) Verwaltung

Der Staat ist handlungs- und innovationsfähig durch eine leistungsstarke öffentliche Verwaltung. Die zukunftssichere Ausrichtung der Finanzverwaltung sowie ihrer Leistungen hängt maßgeblich von der IT ab, die gut auf administrative Strukturen und Prozesse abzustimmen ist. Nur durch die gezielte Nutzung von Digitalisierungspotentialen kann eine Verwaltung ihre Aufgaben auf einem hohen Qualitätsniveau erfüllen, resilient und zuverlässig agieren und den steigenden Anforderungen an einen durchsetzungsfähigen Staat gerecht werden.

Die Finanzverwaltung und insbesondere die darin eingebettete Steuerverwaltung stehen im unmittelbaren Kontakt mit Bürgerinnen und Bürgern sowie mit Unternehmen. Dabei setzt sie die Möglichkeiten und Chancen der Digitalisierung bereits heute in besonderem Maße um. Einerseits kann sie digital eingehende Informationen (Input) unmittelbar digital verarbeiten, zum Beispiel über ELSTER eingereichte Steuerunterlagen. Andererseits kann sie offizielle Schreiben (Output) digital übermitteln, etwa bei der Zustellung von digitalen Einkommensteuerbescheiden direkt in ELSTER.

Allerdings stellen multiple und konvergierende Krisen dabei große Herausforderungen dar. Der demographische Wandel führt zu einem verschärften Wettbewerb um die besten Talente in der öffentlichen Verwaltung, sowohl allgemein in der Fachverwaltung, als auch besonders ausgeprägt im Bereich der IT. Gleichzeitig sind Bund und Länder mit angespannten Haushaltslagen und sinkenden Steuereinnahmen konfrontiert, die ihnen nur enge finanzielle Spielräume – etwa für transformative Investitionen und Innovationen – lassen. Neben der Bewältigung dieser Herausforderungen stehen auch die Bekämpfung von Finanzkriminalität und die Erfordernisse der IT-Sicherheit und Betriebssicherheit an vorderster Stelle eines verantwortungsvollen staatlichen (Verwaltungs-)Handelns aus der Perspektive einer Finanzverwaltung.

Trotz sich ändernder Erwartungen von Bürgerinnen und Bürgern, von Beschäftigten, aber auch von der Wirtschaft und ihren Unternehmen an einen durchsetzungsfähigen und leistungsstarken Staat zeigt sich die Finanzverwaltung dank leistungsfähiger IT-Strukturen und kompetentem sowie engagiertem IT-Personal auch im Korsett angespannter Haushaltslagen handlungsfähig. Die IT der Finanzverwaltung muss daher an klaren, politisch-strategischen Zielen ausgerichtet bleiben, um dauerhaft ihre Prozesse und Verwaltungsleistungen in hoher Qualität sicherzustellen.

Stringente IT-Steuerung für die Digitalisierungsoffensive der Finanzverwaltung durch erhöhte Strategiefähigkeit

Um die Chancen der Digitalisierung für die Finanzverwaltung bestmöglich zu erschließen und zu nutzen sowie die im Folgenden benannten Handlungsfelder mit besonders hohem Bedarf an IT-Steuerung gezielt zu besetzen, wird die Strategie der Finanzverwaltung priorisiert vorangetrieben. Dazu erarbeitet das Ministerium der Finanzen eine übergreifende Digital-Rahmenstrategie inklusive der Betrachtung von Chancen der Künstlichen Intelligenz (KI) für die Finanzverwaltung.

Elementarer Bestandteil dieser strategischen Ausrichtung ist es, die Finanzverwaltung „KI-ready" zu machen. Das bedeutet, dass Maßnahmen ergriffen werden, um die organisatorischen, technischen und ggf. rechtlichen Voraussetzungen zu schaffen, damit KI für geeignete Anwendungsfälle erprobt und eingesetzt werden kann. Dazu gehört auch der geplante Aufbau einer KI-Community in der Finanzverwaltung sowie einem fortgeführten Austausch mit Verwaltungen, Wirtschaft und Wissenschaft. Die exponentielle Entwicklung der KI-Technologien erfordert es, die Verwaltung durch Wissensaufbau, Schaffung von Rahmenbedingungen und agiler Bereitschaft so aufzustellen, dass – teilweise in ihren Ausprägungen nicht vorhersehbaren – Technologiesprünge zügig, aber unter Wahrung der Belange von Datenschutz und Ethik, gewinnbringend für die Finanzverwaltung und damit für die gesamte Landesverwaltung erschlossen werden können.

Voraussetzung hierfür ist eine Governance und Positionierung, die festlegt, unter welchen Rahmenbedingungen und zu welchem Zweck KI eingesetzt wird. Neben dezidierten Sach- und Personalmitteln zum Aufbau

unterstützender Strukturen für den Einsatz von KI, ist auch ein dezentraler anwendungsbezogener KI-Kompetenzaufbau in der Finanzverwaltung notwendig. Dies erfordert einen besonderen Steuerungs- und Ressourcenaufwand.

Gleichzeitig ist im Umgang mit KI für die Finanzverwaltung der „Human in the loop" Ansatz zu verfolgen: Demnach verbleibt die Entscheidungshoheit mindestens für Geschäftsprozesse bei den hervorragend qualifizierten Beschäftigten in der Finanzverwaltung, sodass der Fokus des KI-Einsatzes auf Instrumente der KI in assistierenden Funktionen liegt. Dies schafft Freiräume, menschliche Fähigkeiten weniger bei Routinetätigkeiten und verstärkter für verantwortungsvolle Aufgaben einzusetzen und komplexe Sachverhalte in der notwendigen Tiefe bearbeiten zu können.

Im Rahmen der Koordinierten Neuen Software-Entwicklung der Steuerverwaltung – kurz KONSENS – prüft Nordrhein-Westfalen in Kooperation mit Bayern die Möglichkeit und Chancen des verstärkten Einsatzes von KI, um interne Arbeitsabläufe perspektivisch zu beschleunigen, diese effizienter und effektiver auszugestalten sowie die Leistungserbringung gegenüber Bürgerinnen und Bürgern, Unternehmen und steuerberatenden Berufen zu verbessern.

Handlungsfelder mit besonders hohem Bedarf an IT-Steuerung

Die Finanzverwaltung ist untergliedert in die Steuerverwaltung als Einnahmeverwaltung, z. B. mit der Bekämpfung von Finanzkriminalität, und die übrige Finanzverwaltung mit Aufgaben u.a. im Bereich der Besoldungs- und Versorgungsangelegenheiten oder im Bereich von Bau- und Liegenschaftsmanagement.

Die Digitalisierung stellt für die unterschiedlichen Bereiche der Finanz- und Steuerverwaltung – das Ministerium der Finanzen, die Oberfinanzdirektion, das Landesamt für Finanzen, das Landesamt für Besoldung und Versorgung, das Rechenzentrum der Finanzverwaltung, das Landesamt zur Bekämpfung der Finanzkriminalität, den Bau- und Liegenschaftsbetrieb des Landes sowie den Schulungs- und Fortbildungseinrichtungen der Finanzverwaltung – jeweils unterschiedliche Herausforderungen und Chancen dar. Aufgrund seiner Rechtsstellung organisiert der Bau- und

Liegenschaftsbetrieb Nordrhein-Westfalen seine IT-Leistungen eigenständig und stellt diese strategisch auf. Um die Strukturen und Leistungen der Finanzverwaltung, aber auch der Landesverwaltung insgesamt, effizient, effektiv und zukunftsfähig aufzustellen, werden innerhalb dieser Verwaltungseinheiten diverse IT-Vorhaben bereits umgesetzt oder erscheinen aus strategischer Sicht perspektivisch sinnvoll.

Für die Steuerverwaltung im Besonderen wirkt Nordrhein-Westfalen über das Ministerium der Finanzen im Rahmen der länderübergreifenden Koordinierten Neuen Software-Entwicklung der Steuerverwaltung – kurz KONSENS – gemeinsam mit den anderen Ländern und im Schulterschluss mit dem Bund darauf hin, den Steuervollzug mittels bundeseinheitlicher Digitalisierungsmaßnahmen sicherzustellen. Das Rechenzentrum der Finanzverwaltung implementiert die fertigen KONSENS-Produkte in die IT-Landschaft der Steuerverwaltung Nordrhein-Westfalen.

Darüber hinaus steuert das Ministerium der Finanzen zusätzlich zu eigenen, über das Rechenzentrum der Finanzverwaltung betriebenen IT-Leistungen mit Schwerpunkt in der Steuerverwaltung, auch Digitalisierungsprojekte für die gesamte Landesverwaltung – insbesondere das Personalwirtschaftssystem my.NRW, das System für Haushalts- und Rechnungswesen EPOS.NRW, das Bezügeverwaltungsverfahren NRWave und die erforderliche Migration dieser SAP-Systeme auf S/4-HANA
Die Handlungsfelder der IT-Leistungen der Finanzverwaltung gliedern sich im Kern in die Schwerpunkte Steuer-IT und bestimmte Aufgaben der ressort- und behördenübergreifenden Digitalisierung, von denen sich konkrete Handlungsfelder mit hohem Bedarf an IT-Steuerung ableiten lassen.

Schwerpunkt Steuer-IT

1. Handlungsfeld: Weiterentwicklung des Gesamtvorhabens KONSENS durch die länderübergreifende Bund-Länder-Arbeitsgruppe auf Staatssekretärs-Ebene

Die Entwicklung, der Betrieb und die Pflege von Software der Steuerverwaltung bilden den Kern der länderübergreifenden Koordinierten Neuen Software-Entwicklung der Steuerverwaltung – kurz KONSENS. Es dient

der Vereinheitlichung und fortlaufenden Modernisierung der IT-Unterstützung in der deutschen Steuerverwaltung sowie der Verbesserung der Services für Bürgerinnen und Bürger, Unternehmen und die Steuerberaterschaft.

KONSENS ist beispielgebend für das gute, länderübergreifende Zusammenwirken der Bereiche (Steuer-)Verwaltung, Organisation und Automation. So können übergeordnete politische Ziele wie die Autofallquote (vollmaschinelle Steuerveranlagung) nur umgesetzt werden, wenn rechtliche und organisatorische Vorgaben mit den technischen Möglichkeiten der IT verknüpft werden.

Nordrhein-Westfalen, als starker Partner im Gesamtvorhaben KONSENS mit dem größten Finanzierungsanteil und als Mitglied der Steuerungsgruppe-IT, kommt dabei eine besondere Verantwortung zu. Die Steuerungsgruppe-IT trifft im Gesamtvorhaben KONSENS grundlegende Festlegungen u.a. zur IT-Strategie, zur IT-Infrastruktur, zu IT-Standards und der Gesamtarchitektur. Darüber hinaus legt sie allgemeine Regelungen zur Ausgestaltung und Konkretisierung der Bestimmungen zu Budget und Kostentragung fest. Als eines von fünf auftragnehmenden Ländern (Baden-Württemberg, Bayern, Hessen, Niedersachsen und Nordrhein-Westfalen) ist Nordrhein-Westfalen Mitglied der Steuerungsgruppe-IT, in der auch der Bund vertreten ist.

Auf Initiative Nordrhein-Westfalens hat die Finanzministerkonferenz am 02. Juni 2023 die Einrichtung einer Bund-Länder-Arbeitsgruppe auf Staatssekretärsebene (STS-AG) zur Optimierung und Weiterentwicklung der Strukturen und Prozesse sowie zur Evaluation der Finanzierung im Gesamtvorhaben KONSENS beschlossen. Die Finanzministerkonferenz hat den Bericht der STS-AG mit 22 Handlungsempfehlungen am 30. November 2023 zur Kenntnis genommen, die darin enthaltenen Lösungsvorschläge gebilligt und die STS-AG gebeten, die Umsetzungsphase der Handlungsempfehlungen zielgerichtet zu begleiten und eine Evaluierung dieser zur Finanzministerkonferenz bis Ende des Jahres 2024 vorzulegen.

Die enge Begleitung der Umsetzungsphase erfolgt innerhalb eines Kernteams der STS-AG, in dem der nordrhein-westfälische Staatssekretär der Finanzen neben Berlin, Baden-Württemberg, Bayern, Hamburg, Hessen,

Niedersachsen, Thüringen und dem Bund mitarbeitet. Das Kernteam tagt derzeit in der Regel 14-tägig und organisiert anlassbezogen themenspezifische Vertiefungsworkshops.

Zur Unterstützung der STS-AG wurde die Strategische Stabsstelle KONSENS eingerichtet. Auch hier ist Nordrhein-Westfalen vertreten. Ziel ist, insbesondere die Harmonisierung der Kernverfahren, also die bundesweite Vereinheitlichung der IT-Verfahren, für die Festsetzung, Erhebung und Grundinformation in den Finanzämtern voranzutreiben. Darüber hinaus befasst sich die Stabsstelle u. a. mit der adressatengerechten Kommunikation an die Leitungsebenen, um diesen mit einem ganzheitlichen Informationssystem künftig eine verbesserte Steuerung zu ermöglichen.

Weitere Handlungsempfehlungen der STS-AG beziehen sich u.a. auf die weitere Standardisierung der Software in KONSENS mit neuer Technik unter Berücksichtigung von Cloud- und Containertechnologie, die beschleunigte Übernahme fertiggestellter Produkte in den produktiven Einsatz und die Beschleunigung der Entwicklung der wichtigsten Aufgaben für eine elektronische Aktenführung.

Die aktuell durch die Staatssekretärsebene der Länder und des Bundes gesteuerte enge Begleitung der Verwaltungsdigitalisierung unterstreicht das Ziel, das Gesamtvorhaben KONSENS an den administrativ-strategischen Prioritäten für die IT der Steuerverwaltung auszurichten. Der effizient gesteuerte Einsatz von IT-Lösungen wirkt dabei als Treiber für Transformationsprozesse in einer modernen und leistungsstarken öffentlichen Finanzverwaltung.

2. Handlungsfeld: Stärkung und Modernisierung des Rechenzentrums der Finanzverwaltung

Das Rechenzentrum der Finanzverwaltung (RZF) entwickelt IT-Produkte für die bundesweite Nutzung im KONSENS-Verbund und es ist gleichzeitig Motor und Rückgrat für das digitale Finanzamt in Nordrhein-Westfalen. Die IT-Leistungen zur sicheren, effizienten und bürgerorientierten Verarbeitung sensibler Steuerdaten werden im RZF gepflegt und betrieben. Auch die Entwicklung erfolgt im RZF bzw. durch Übernahme aus dem KONSENS-Verbund. Das Rechenzentrum der Finanzverwaltung ist ein

Full-Service Dienstleister, der zur Wahrung des gesetzlichen Steuergeheimnisses eigenständig für die Steuerverwaltung tätig ist.

Die Leistungsfähigkeit des RZF ist deshalb von zentraler Bedeutung für die Zukunftsfähigkeit der Steuerverwaltung. Moderne IT-Entwicklungen zeigen Chancen und Instrumente auf, um energie- und klimapolitischen Herausforderungen, dem demographischen Wandel und dem Fachkräftemangel mittels technischer Innovationen zu begegnen und die öffentliche Verwaltung zukunftssicher aufzustellen. Dazu zählen neue Technologien und Konzepte von Cloud-Computing oder die Automation von Verwaltungsabläufen und damit verbundener Flexibilisierung und Agilisierung von Arbeitsprozessen.

Zudem kann der gezielte (assistierende) Einsatz von KI in der Finanzverwaltung bei der Bekämpfung von Finanzkriminalität, die zunehmend im digitalen Raum stattfindet, und dem erhöhten Bedarf an Maßnahmen zur Gewährleistung von IT-, Betriebs- und Cybersicherheit die Handlungsfähigkeit der öffentlichen Verwaltung erheblich stärken.

Die Bedrohungslage der IT-Sicherheit in Deutschland war gemäß dem Bericht des Bundesamts für Sicherheit und Informationstechnik (BSI) im Jahr 2023 „*unverändert* [...] *angespannt bis kritisch*"[1] (Vgl. Anl. 1). Deshalb ist das fortwährende Ziel, „*die Resilienz schnellstmöglich zu erhöhen*, [...], *Cybersicherheit pragmatisch zu gestalten*, [...], [und] *die Digitalisierung zu beschleunigen, um mit den Entwicklungen unserer Zeit Schritt zu halten*"[2] (Vgl. Anl. 1). Hierbei empfiehlt das BSI eine organisatorische Trennung und etwa die Verantwortlichkeiten des „*Informationssicherheitsbeauftragten direkt der obersten Leitungsebene zuzuordnen*"[3] (Vgl. Anl. 2). Die Rolle und Verantwortlichkeiten der politisch-strategischen Ebene rücken hierbei in den Fokus, denn „*Cybersicherheit ist komplex*" und nur mit „*Klarheit über Sicherheitseigenschaften und die sichere Verwendung* [von Schlüsseltechnologien wie z. B. KI und Cloud] [...], *bringen wir Handlungssicherheit*"[4] (Vgl. Anl. 1).

---

[1] Bundesamt für Sicherheit in der Informationstechnik (Oktober 2023): „Die Lage der IT-Sicherheit in Deutschland 2023", S. 85. Zuletzt abgerufen am 04.03.2024 unter: Lagebericht2023.pdf (bund.de) .
[2] Ebd., S. 87.
[3] Bundesamt für Sicherheit in der Informationstechnik (Version 1.0): „BSI-Standard 200-2. IT-Grundschutz-Methodik", S. 40. Zuletzt abgerufen am 04.03.2024 unter: https://www.bsi.bund.de/dok/10027846 .
[4] Die Lage der IT-Sicherheit in Deutschland 2023, S. 5.

Die Gewährleistung von IT-, Betriebs- und Cybersicherheit stellt daher eine zentrale Anforderung an eine handlungsfähige öffentliche Verwaltung dar. Angesichts der Tatsache, dass auch bei einem höchsten Maße an Sicherheitsvorkehrungen ein Restrisiko für nicht auszuschließende Bedrohungen bleibt, ist das Ziel in der Finanzverwaltung, das Bewusstsein für die Risiken zu schaffen, durch Resilienz und mittels Möglichkeiten der Digitalisierung und organisatorischer Regelungen die Cybersicherheit aktiv zu gestalten und handlungsfähig zu bleiben.

Mit dem neu eingeführten und in 2019 erstmals nach ISO 20.000 zertifizierten IT-Service Management der Steuerverwaltung können sowohl die Anforderungen der Digitalisierung als auch querschnittliche Anforderungen zeitnah und wirksam umgesetzt werden. Mit dem Service Desk wird die landesweite Erreichbarkeit der IT für die Anwenderinnen und Anwender in den Finanzämtern zu den garantierten Servicezeiten sichergestellt. Durch die neu geschaffenen Prozesse des Störungs- und Problem Managements erfolgt eine vollständige Störungserfassung und eine priorisierte und effiziente Störungsbeseitigung. Es erfolgt eine regelmäßige Re-Zertifizierung.

Mit dem Neubau eines energieeffizienten, sicheren und attraktiven Neubaus in Kaarst, in den das Personal des Rechenzentrums der Finanzverwaltung im Jahr 2026 einziehen wird, hat das Ministerium der Finanzen die Weichenstellung für das „neue Rechenzentrum" gelegt[5] (Vgl. Anl. 3). Die technische Inbetriebnahme ist im Jahr 2025 geplant. Der Neubau umfasst ein Verwaltungsgebäude, das Rechenzentrum und eine Druckstraße. Auf rund 37.000 Quadratmetern Fläche werden ab 2026 ca. 1.000 Landesbedienstete tätig sein. Der topmoderne Neubau schafft exzellente Arbeitsbedingungen für die IT-Profis der Finanzverwaltung und trägt mit hohen Anforderungen an die Nachhaltigkeit unserer Verantwortung für Umwelt- und Klimaschutz Rechnung.

Das neue Rechenzentrum wird ein wesentlicher Baustein für die digitale, bürgerfreundliche Steuerverwaltung der Zukunft. Im Jahr 2023 wurden zahlreiche Maßnahmen zur Modernisierung des Rechenzentrums der Fi-

[5] Ministerium der Finanzen des Landes Nordrhein-Westfalen (23.10.2023): „Grundsteinlegung in Kaarst: Meilenstein für das neue Rechenzentrum der Finanzverwaltung. Zuletzt abgerufen am 04.03.2024 unter: https://www.finanzverwaltung.nrw.de/uebersicht-rubrik-aktuelles-und-presse/pressemitteilungen/grundsteinlegung-kaarst-meilenstein-fuer .

nanzverwaltung, beispielsweise in der IT-Personalgewinnung und -entwicklung und der Stärkung der Krisenresilienz (u.a. Sekundärstandort und Rechenzentrums-Architektur) angestoßen.
Auch die Strukturen und Prozesse werden weiterentwickelt, etwa durch Agile Softwareentwicklung, bei der – entgegen der traditionellen Softwareentwicklung, in der zunächst langwierige Lastenhefte erstellt werden, bevor die Softwareentwicklung beginnt – in kurzen Sprints mit enger Kommunikation zwischen Nutzern, Auftraggebern und Entwicklern frühzeitig ein lauffähiges Produkt bereitgestellt, das um weitere Anforderungen in den Sprints jeweils ergänzt wird.

Im Bereich von DevOps als zeitgemäßer Organisationsform der Softwareentwicklung und des Betriebs, rücken diese organisatorisch und prozessual enger zusammen, damit neue Anforderungen schneller in die laufende Software einfließen können. Diese bereits angestoßenen Maßnahmen werden in den Jahren 2024 ff. konzentriert gesteuert und erfordern einen hohen Arbeitsaufwand.

3. Handlungsfeld: Landesamt zur Bekämpfung der Finanzkriminalität Nordrhein-Westfalen

Das am 1. Januar 2024 gegründete Landesamt zur Bekämpfung der Finanzkriminalität ist die bundesweit erste, zentralisierte Landesbehörde zur Bekämpfung der Finanzkriminalität[6] (Vgl. Anl. 4).

Ein Schwerpunkt der künftigen Arbeit des LBF NRW werden Ermittlungen im digitalen Raum sein. Daraus ergeben sich für das LBF NRW erhöhte Anforderungen an die Bereitstellung von hochspezialisierten IT-Leistungen. Zur Koordination und Bündelung der Digitalisierungs- und IT-Expertise wird im Landesamt eigens ein neues IT-Kompetenzzentrum aufgebaut, um das Phänomen zunehmend internationaler, vernetzter und digitaler werdender Finanzkriminalität noch wirksamer zu bekämpfen.

---

[6] Ministerium der Finanzen des Landes Nordrhein-Westfalen (15.01.2024): „Landesamt zur Bekämpfung der Finanzkriminalität nimmt die Arbeit auf". Zuletzt abgerufen am 04.03.2024 unter: https://www.finanzverwaltung.nrw.de/uebersicht-rubrik-aktuelles-und-presse/pressemitteilungen/landesamt-zur-bekaempfung-der .

Eine zentrale Aufgabe der neuen Einheit ist, neueste Methoden der digitalen Forensik und unterstützende KI-Anwendungen mit Blick auf die spezifischen Anforderungen der Ermittlungsarbeit der Fahndung weiterzuentwickeln und in den jeweiligen Ermittlungseinheiten zur Anwendung zu bringen. Um diesen Anforderungen bestmöglich gerecht zu werden, wird das IT-Kompetenzzentrum in einem hohen Maß auf interne und externe Vernetzung und Kollaboration setzen.

Intern sind die Prozesse so angelegt, dass das Rechenzentrum der Finanzverwaltung den weiteren Auf- und Ausbau des LBF NRW hoch priorisiert und als zentraler Technologiepartner eng mit dem Kompetenzzentrum zusammenarbeiten wird. Das Rechenzentrum der Finanzverwaltung erbringt für das LBF NRW dabei IT-Leistungen, stellt IT-Ausstattung bereit und berät in Fragen zu Digitalisierung, Informationssicherheit und technologischen Innovationen.

Mit Blick auf die Größe und Bedeutung der Aufgabe wird das Kompetenzzentrum auch den Austausch und die Zusammenarbeit mit externen Partnern intensivieren, um die jeweils besten technischen Lösungen zur Bekämpfung der Finanzkriminalität zur Verfügung stellen zu können.

4. Handlungsfeld: Modernisierungsprogramm „Finanzverwaltung für Nordrhein-Westfalen“

Das Modernisierungsprogramm „Finanzverwaltung für Nordrhein-Westfalen“ setzt Projekte um, die für die Zukunftsfähigkeit der Steuerverwaltung von strategischer Bedeutung sind[7] (Vgl. Anl. 5). Schwerpunkte bilden dabei die Verbesserung der Prozesse in der Finanzverwaltung nach innen und nach außen, sowie die Steigerung der Attraktivität der Finanzverwaltung als Arbeitgeberin in Zeiten des demographischen Wandels und der Fachkräfteknappheit.

Die Leistungen und Abläufe in der Finanzverwaltung sollen durch einen weiter steigenden Grad an Automation künftig noch kunden- und beschäftigtenfreundlicher werden und sich noch mehr an den Bedürfnissen der

[7] Vorlage 18/1482. Zuletzt abgerufen am 04.03.2024 unter: https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV18-1482.pdf .

Bürgerinnen und Bürger sowie Unternehmen und steuerberatenden Berufe orientieren. Zu den prioritären Zielen gehört dabei zum Beispiel die „Erhöhung der Autofallquote". Der Autofall beschreibt die vollmaschinelle Steuerveranlagung und nutzt die Chancen der Digitalisierung für eine automatisierte, massenhafte Bearbeitung von Steuererklärungen. In der Folge können sich die Beschäftigten der Finanzverwaltung auf die Bearbeitung komplexer Aufgaben und Steuerfälle konzentrieren.

Das Modernisierungsprogramm ist auch ein Digitalisierungsprogramm, nicht zuletzt aufgrund seines eigenen Teilprogramms „Digitalisierung". Dieses nimmt eine Querschnittsfunktion ein, denn es unterstützt die Umsetzung zahlreicher Programm-Maßnahmen wie die Ermöglichung eines „papierlosen Büros" durch eine einheitliche Softwareumgebung, in der Posteingang, Bearbeitung von Steuerfällen und Postausgang lückenlos digital bearbeitet werden können. Des Weiteren werden Beschäftigte bei der Einführung neuer IT-Produkte durch sog. „digITeams" in den Finanzämtern begleitet und unterstützt. Schließlich sollen die Beschäftigten durch ein neues Informations- und Kommunikationskonzept gezielter und umfassender über IT-Leistungen und deren Anwendung informiert werden.

In der Entwicklung geeigneter digitaler Strukturen und Prozesse ist zudem die Barrierefreiheit in der Finanzverwaltung ein wichtiges Ziel bei der Umsetzung. Dazu wurde unter anderem zum 01.01.2024 das Kompetenzzentrum Barrierefreie IT („KomBIT") im Rechenzentrum der Finanzverwaltung geschaffen. Es hat das Ziel, Transparenz und Bewusstsein für Barrierefreiheit in der IT in der Finanzverwaltung zu schaffen und dafür zu werben, dass die vielfältigen und vielschichtigen gesetzlichen Rahmenbedingungen eingehalten werden.

Der Beitrag der IT zur Schaffung zukunftsfähiger Lösungen ist demnach für das Modernisierungsprogramm „Finanzverwaltung für Nordrhein-Westfalen" unentbehrlich und eine an den Zielen des Programms ausgerichtete Steuerung der IT-Leistungen von besonderer Bedeutung. Gleichzeitig ist eine noch stärkere Verzahnung zwischen Fach-, Organisations- und IT-Seite erforderlich, um die Ziele des Programms effektiv zu erreichen. Dies stellt wie im Gesamtvorhaben KONSENS erhöhte Anforderungen an das Zusammenspiel der IT mit dem (Steuer-)Fach- und Organisa-

tionsbereich. So hängt die Umsetzung zahlreicher Maßnahmen des Programms von der Bereitstellung von IT-Produkten aus KONSENS ab, bevor sie fachlich und organisatorisch in die Fläche gebracht werden können. Dafür müssen sich die Länder auf eine gemeinsame Priorisierung verständigen. Um die Prioritäten Nordrhein-Westfalens bei derartigen Priorisierungsentscheidungen zu platzieren, ist die kontinuierliche strategische Steuerung und die Rückkopplung mit anderen strategisch relevanten Prozessen wie dem Modernisierungsprogramm Finanzverwaltung für Nordrhein-Westfalen und den Fach- und Organisationsbereichen unerlässlich.

Schwerpunkt ressort- und behördenübergreifende Digitalisierung

1. Handlungsfeld: Weiterentwicklung Projekte my.NRW und „Zukunftsfähige Beihilfesachbearbeitung (IBSY.NRW)“

Das digitale Personalwirtschaftssystem „my.NRW“ ermöglicht, das Personalmanagement des Landes wirtschaftlicher, effektiver und effizienter wahrzunehmen. Der Projektauftrag sieht vor, die in der Landesverwaltung vorhandenen Personalverwaltungssysteme, -verfahren und -prozesse zu vereinheitlichen, zu digitalisieren und medienbruchfrei umzusetzen. Ziel ist dabei, eine landeseinheitliche E-Personalakte einzuführen und ein Beschäftigtenportal aufzubauen, über das alle Beschäftigten einen standardisierten Zugang zu ihren Personalprozessen erhalten. In Zeiten des demographischen Wandels und des verstärkten Wettbewerbs um die besten Talente bildet my.NRW ein zentrales Instrument des modernen öffentlichen Dienstes und einer handlungs- und leistungsfähigen öffentlichen Verwaltung.

Von einer erfolgreichen Umsetzung von my.NRW können mehr als 500.000 Beschäftigte und Pensionäre des Landes profitieren. Damit ist das Projekt my.NRW das aktuell größte Digitalisierungsprojekt in der Landesverwaltung von Nordrhein-Westfalen.

Das Projekt ist 2019 gestartet, die Projektleitung liegt in der Federführung des Ministeriums der Finanzen. my.NRW wurde im Jahr 2022 in der Staatskanzlei und im Jahr 2023 im Ministerium für Kinder, Jugend, Fami-

lie, Gleichstellung, Flucht und Integration (MKJFGFI) sowie dem Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie (MWIKE) implementiert. Die Umsetzungsplanung sieht für die kommenden Jahre die Rollouts im Ministerium für Umwelt, Naturschutz und Verkehr (MUNV), im Ministerium für Kultur und Wissenschaft (MKW) sowie in weiten Teilen des Ministeriums des Innern (IM), im Ministerium für Arbeit, Gesundheit und Soziales (MAGS), im Ministerium für Landwirtschaft und Verbraucherschutz (MLV), im Ministerium für Heimat, Kommunales, Bau und Digitalisierung (MHKBD), im Landesbetrieb Information und Technik NRW (IT.NRW) und den Geschäftsbereichen (nachgeordnete Bereiche) von MWIKE, MKW und MAGS sowie den weiteren Ressorts vor.

Die Entwicklung und das Anforderungsmanagement im Projekt zeigen, dass die Herausforderung darin liegt, technisch umsetzbare dienstliche und organisatorische Vorschriften zu schaffen und diese zur einheitlichen Anwendung zu bringen. Nur so können die Chancen von my.NRW für eine effiziente, effektive und leistungsstarke Personalwirtschaft genutzt werden. Im Jahr 2024 wird das Projekt unter Leitung des Ministeriums der Finanzen in enger Zusammenarbeit mit den Ressorts priorisiert und weiterentwickelt. Die Staatssekretärsebene wird dabei eine stärkere Rolle als zentrale Steuerungsinstanz einnehmen.

Das Projekt „Zukunftsfähige Beihilfesachbearbeitung“ (IBSY.NRW) hat die Modernisierung aller Abläufe zum Thema Beihilfe von der Beantragung bis zur Auszahlung zum Gegenstand. Im Zentrum steht die Einführung eines neuen Sachbearbeitungssystems für alle Beihilfestellen des Landes und, als Serviceangebot, für die Kommunen. Mit dem neuen System wird erstmals die Möglichkeit einer vollmaschinellen Bearbeitung von Anträgen geschaffen. Den Kern dazu bildet ein Regelsystem, das die Beihilfeverordnung des Landes abbildet. Die maschinelle Bearbeitung soll zu einer Entlastung der Beihilfestellen und zu einer insgesamt höheren Effizienz führen.

Die Beantragung von Beihilfeleistungen für alle beihilfeberechtigten Landesbeschäftigten ist bereits seit einigen Jahren digital mit der eingeführten „Beihilfe App“ über ein Smartphone möglich. Ergänzend soll künftig auch der Abruf der Bescheide über die App ermöglicht werden.

Perspektivisch wird darüber hinaus eine Integration in das Beschäftigtenportal von my.NRW angestrebt, um damit die Vision eines One-Stop-Shops für alle Beschäftigten umzusetzen.

Insgesamt sollen my.NRW und IBSY.NRW zu einer höheren Mitarbeiterfreundlichkeit und zu einer konsequenteren Digitalisierung der Prozesse der Personalwirtschaft beitragen.

2. Handlungsfeld: Landesamt für Finanzen

Das Landesamt für Finanzen nimmt als Landesoberbehörde zahlreiche Aufgaben für die gesamte Landesverwaltung wahr. Dazu zählt der gesamte Zahlungsverkehr des Landes über die Landeshauptkasse NRW oder das landesweite Personalmarketing „Karriere.NRW".

Ein weiterer Themenschwerpunkt ist die Zuständigkeit für den Rückgriff UVG (Unterhaltsvorschussgesetz). Dieser Bereich stellt besondere Anforderungen an die IT. Die UVG-Abteilungen des LaFin wurden daher 2019 als digitale Modellbehörde gegründet. Die Bearbeitung der Vorgaben aus dem UVG soll dadurch möglichst effektiv erfolgen. Das LaFin führte schon vor der Corona-Krise besonders umfangreiche Regelungen für das mobile Arbeiten ein und stellte im UVG-Bereich auf die Nutzung der E-Verwaltungsakte um.

Der zielgerichtete Einsatz IT-gestützter Systeme zur weiteren Effizienzsteigerung von Verwaltungsprozessen findet im Landesamt für Finanzen konkrete Anwendung. Im Rahmen eines Projekts wird derzeit eine neue IT-Systemlandschaft zur Unterstützung der UVG-Fachabteilung im Landesamt für Finanzen eingeführt. Dabei wird ein Controlling-System für die UVG-Sachbearbeitung aufgebaut und Prozessoptimierungen in der UVG-Sachbearbeitung entwickelt und umgesetzt. Das Ziel ist die IT-gestützte vollständige und rechtskonforme Durchführung des UVG-Rückgriffs und die flexiblere Umsetzung von Anpassungen in der IT-Systemlandschaft UVG-Rückgriff. Dabei sollen die Prozesse im UVG-Rückgriff mittels IT-Einsatz effizienter gestaltet werden und gleichzeitig die Arbeitszufriedenheit der Beschäftigten in der UVG-Fachabteilung durch die Nutzung moderner, IT-gestützter Fachverfahren gestärkt werden. Das Landesamt für

Finanzen wird damit in seiner Rolle als digitale Modellbehörde stetig weiterentwickelt und die staatlichen Handlungsmöglichkeiten bei der Erfüllung der Vorgaben aus dem UVG durch gesteigerte IT-Leistungen maßgeblich gestärkt. Die IT-gestützten Möglichkeiten der Finanzverwaltung leisten hiermit einen erheblichen Beitrag zur Erfüllung gesetzlicher Vorgaben für ein verlässliches staatliches Verwaltungshandeln.

3. Handlungsfeld: Steuerung der SAP-Verfahren und Migration auf S4/HANA

Im Zuständigkeitsbereich des Ministeriums der Finanzen basieren die für die gesamte Landesverwaltung bedeutenden Verfahren EPOS.NRW, NRWave (Bezügeverfahren des Landes für Beamte, Angestellte und Pensionäre) und my.NRW auf der SAP-Technologie. Sie werden im SAP.CC bei IT.NRW weiterentwickelt, gehostet und betrieben.

Die Steuerungsprozesse für die SAP-Verfahren hängen untereinander zusammen, da die Verfahren dieselbe Technologie einsetzen, beim IT-Dienstleister IT.NRW gemeinsam betrieben und aus demselben Haushaltskapitel in Kapitel 12 010 finanziert werden.
Die Firma SAP führt mit „S4/HANA“ eine neue Version des technischen Grundsystems für alle SAP-Verfahren ein, das eine Prozess- und Datenzentrierung der Verfahren ermöglicht. Für das bisherige Grundsystem hat SAP das Ende des regulären Supports für Ende 2027 angekündigt. Darüber hinaus soll der Support für das alte Grundsystem bis Ende 2030 zu erhöhten Kosten möglich sein und voraussichtlich mit qualitativen Einschränkungen zur Verfügung stehen. Es besteht Handlungsdruck, die SAP-Verfahren des Ministeriums für Finanzen für die Prozesse in der gesamten Landesverwaltung zu migrieren. Dazu ist angesichts des signifikanten Aufwands eine Fokussierung erforderlich. Für die SAP-Verfahren des Ministeriums der Finanzen stehen daher Systemmigrationen bevor, die als komplexe, erfolgskritische Großprojekte einen erheblichen Steuerungs- und Arbeitsaufwand implizieren.

4. Handlungsfeld: Verwaltungsgebäude H5: Neubau Haroldstraße 5

Der in Planung befindliche Neubau soll von mehreren Ministerien genutzt werden und eine hochmoderne Arbeitsumgebung bieten. Daher muss die Informationstechnik des Verwaltungszentrums die fachlichen Anforderungen mehrerer Ministerien erfüllen, die Anforderungen des „New Work" berücksichtigen und auf die ständig wachsende Cyber-Bedrohungslage ausgerichtet sein. Beim Neubau des Verwaltungszentrums H5 werden die Ziele der klimaneutralen Landesverwaltung sowie aktuelle Sicherheitsanforderungen erfüllt und der strategischen Portfolioentwicklung des Landes Rechnung getragen[8] (Vgl. Anl. 6). Daraus erwachsen konkrete Anforderungen an die IT und bei der Konzeption und Umsetzung ist eine enge Abstimmung im Dialog mit anderen Ministerien und den Dienstleistern Rechenzentrum der Finanzverwaltung und IT.NRW erforderlich.

Dr. Marcus Optendrenk

[8] Vorlage 18/1665. Zuletzt abgerufen am 04.03.2024 unter: https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV18-1665.pdf .

Anlage 1

Die Lage der IT-Sicherheit in Deutschland 2023

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Vorwort

Nancy Faeser, Bundesministerin des Innern und für Heimat

Die Digitalisierung eröffnet für unser Land neue Horizonte. Sie ebnet vielfältige Wege, unsere Wirtschaft zu stärken, mehr gesellschaftliche Teilhabe zu ermöglichen und unsere Verwaltung schlicht bürgernäher und effizienter zu machen.

Die Anwendung Künstlicher Intelligenz, das viel zitierte „Internet der Dinge“ oder die Möglichkeit, komplexe Prozesse digital zu steuern, bieten jedoch nicht nur Chancen. Sie stellen auch Risiken dar. Und diese Risiken werden größer, je stärker diese Technologien sich verbreiten. Das Potenzial für Missbrauch wächst, neue Angriffsflächen entstehen. Das zu wissen, ist wichtig – und muss stärker ins öffentliche Bewusstsein rücken. Nur wer mögliche Gefahren kennt und erkennt, ist in der Lage, richtige Entscheidungen zu treffen und geeignete Maßnahmen zu ergreifen, um sich und andere zu schützen. Das ist für unsere digitale und damit öffentliche Sicherheit fundamental.

Mit dem vorliegenden Bericht zur Lage der IT-Sicherheit in Deutschland 2023 leistet das Bundesamt für Sicherheit in der Informationstechnik (BSI) einen wichtigen Beitrag, um unser Risikobewusstsein zu schärfen.

Nur so werden Gesellschaft, Wirtschaft, Politik und Verwaltung in die Lage versetzt, Angriffen aus dem Cyberraum zielsicher vorzubeugen. Nur so können sie die notwendigen Vorkehrungen treffen, um auf einen möglichen Vorfall zu reagieren. Nur so können sie solche Ernstfälle auch realitätsnah proben und simulieren. Das ist unerlässlich, denn die Bürgerinnen und Bürger müssen darauf vertrauen können, dass wir gut vorbereitet sind.

Gemeinsam mit allen Bundesländern hat das Bundesministerium des Innern und für Heimat in diesem Jahr erneut eine länder- und ressortübergreifende Krisenmanagement-Übung (LÜKEX) durchgeführt. Beteiligt waren eine Vielzahl von Bundesbehörden sowie Unternehmen, die Kritische Infrastrukturen betreiben. Geübt wurde, wie Staats- und Regierungsfunktionen nach einem Cyberangriff aufrechterhalten werden können. Und es hat sich gezeigt: Wir sind gut auf den Ernstfall vorbereitet.

Aber wir haben auch gelernt: Es braucht den intensiven Austausch von Informationen und koordiniertes Handeln, um Bedrohungen aus dem Cyberraum erfolgreich zu begegnen. Deshalb müssen Bund und Länder diesen Gefahren gemeinsam entgegentreten. Ein starker Partner ist dabei das BSI. Es warnt nicht nur vor möglichen Bedrohungen und Gefährdungen, sondern sorgt zusammen mit den anderen Sicherheitsbehörden für verlässliche Cybersicherheit. Umso mehr verdient der vorliegende Bericht viele interessierte Leserinnen und Leser. Ich wünsche eine spannende Lektüre!

Vorwort

Claudia Plattner, Präsidentin des
Bundesamts für Sicherheit in der Informationstechnik

Im Juni 2023 wurde die Nationale Sicherheitsstrategie des Bundes verabschiedet. In dem 76-seitigen Dokument kommt das Wort „Cyber“ ganze 62 Mal vor. Allein das macht die Bedeutung der Cybersicherheit für die umfassende Sicherheit Deutschlands und mithin jeder Bürgerin und jedes Bürgers augenscheinlich. Und es deckt sich mit der im BSI-Lagebericht festgestellten angespannten bis kritischen Lage:

Die anhaltende Digitalisierung und zunehmende Vernetzung vergrößert die Angriffsflächen – und diese werden genutzt. Im Bericht verzeichnen wir einen Anstieg der Bedrohung im Bereich Schwachstellen. So werden täglich knapp 70 neue Schwachstellen in Softwareprodukten entdeckt – rund 25 Prozent mehr als im vorherigen Berichtszeitraum. Auch die rasante Weiterentwicklung neuer und angepasster Angriffsmethoden und der zunehmende Dienstleistungscharakter (*Cybercrime-as-a-Service*) sind besorgniserregend. Dabei bleibt *Ransomware* die Haupt-bedrohung.

Was also tun? Wir müssen

- Resilienzen so schnell wie möglich erhöhen, um Angriffen vorzubeugen,
- die Cybersicherheit aktiv gestalten, um "vor die Welle" zu kommen,
- gleichzeitig die Digitalisierung voranbringen, denn nur so werden wir auch in den Zukunftstechnologien sicher und wettbewerbsfähig.

Unser Ziel ist es, *Resilienz*en zu erhöhen, indem unsere Empfehlungen, Vorgaben und Hilfestellungen stärker angewandt werden. Die dringendsten Themen in der Umsetzung sind *Patch*ing, Updates und sicheres Identity-Access-Management, um Angriffen vorzubeugen. Hinzu kommt, *Backup*s, Datensicherungen und Notfallpläne als Reaktion auf einen Vorfall zu erstellen und vor allem auch zu erproben. Dafür müssen wir Produkte und Services, die den notwendigen Sicherheitsanforderungen genügen und niederschwellig einsetzbar sind, als Hilfe zur Selbsthilfe bereitstellen und deren Anwendung fördern wie auch fordern können.

Indem wir wichtige Standards und Produkte für mehr und mehr Cyberthemen und Technologien auch auf europäischer Ebene mitgestalten, kommen wir vor die Welle. So erhöhen wir die Cybersicherheit systematisch für Organisationen ebenso wie für Verbraucherinnen und Verbraucher.

Als BSI sind wir auch in der Entwicklung und Forschung zu den für die Digitalisierung notwendigen Schlüsseltechnologien dabei – von KI, *Cloud*, eID oder Smart Metering bis hin zu sicheren modernen Netzen. Indem wir schnell Klarheit über Sicherheitseigenschaften und die sichere Verwendung schaffen, bringen wir Handlungssicherheit. Auf diese Weise leisten wir unseren Beitrag für eine sichere Digitalisierung und beschleunigen diese zugleich.

Für all das sind und wollen wir weiterhin Möglichmacher und Gestalter sein! Wir können ein starker Partner in der deutschen Sicherheitsarchitektur sein.

Als BSI werden wir unsere Befugnisse nutzen: Wir müssen Sicherheitsthemen benennen und Lösungen zuführen können. Denn Cybersicherheit ist komplex und betrifft – wie nicht zuletzt dieser Lagebericht zeigt – alle, von Verwaltungsbehörden über KMU bis hin zu den einzelnen Bürgerinnen und Bürgern.

Unsere oberste Priorität ist es, Deutschland digital und sicher aufzustellen. Das gelingt nur mit koordinierter Zusammenarbeit aller Akteure in den Kommunen, den Ländern und im Bund, international sowie in ganz Europa! Dabei gilt es, auch in den Austausch mit Wirtschaft, Wissenschaft und Gesellschaft zu treten. Wir verstehen Cybersicherheit als Gemeinschaftsaufgabe, die auf Transparenz als Grundlage für Vertrauen beruht!

Inhalt

Vorfälle & Abbildungen

Verzeichnis ausgewählter Vorfälle:

Abbildungsverzeichnis:

1. — Einleitung

Als die Cybersicherheitsbehörde des Bundes beobachtet das Bundesamt für Sicherheit in der Informationstechnik (BSI) kontinuierlich die Gefährdungslage der IT-Sicherheit in Deutschland. Im Fokus des BSI stehen Cyberangriffe auf staatliche sowie öffentliche Institutionen, Unternehmen und Privatpersonen, aber auch Maßnahmen zur Prävention und Bekämpfung dieser Lagen. Der vorliegende Bericht zieht eine Bilanz für die Zeit vom 1. Juni 2022 bis zum 30. Juni 2023 (Berichtszeitraum).

Der Zeitraum weicht von dem des Berichts „Die Lage der IT-Sicherheit in Deutschland 2022“ ab, was in einer Veränderung der Zeiträume begründet liegt, in denen die Daten erfasst und ausgewertet werden. Um eine Vergleichbarkeit der Daten mit dem vorherigen Berichtszeitraum (1. Juni 2021–31. Mai 2022) und dem Berichtszeitraum des Berichts „Die Lage der IT-Sicherheit in Deutschland 2024“ (1. Juli 2023–30. Juni 2024) sicherzustellen, werden an den Stellen, an denen es möglich ist, Tagesdurchschnittswerte genutzt oder die Zahlen denen des gleichen Zeitraums aus dem Vorjahr gegenübergestellt.

Der vorliegende Bericht greift aktuelle und anhaltende Cyberbedrohungen auf und bewertet die IT-Sicherheitslage im Kontext des russischen Angriffskriegs auf die Ukraine. Anhand konkreter Beispiele aus unterschiedlichen Bereichen zeichnet der Bericht den Weg und die typischen Methoden der Angreifer nach, um zugleich aufzuzeigen, wie sich Nutzerinnen und Nutzer schützen können.

Teil A dieses Berichts gibt einen Überblick der allgemeinen Bedrohungslage und aktueller Cyberbedrohungen, unterteilt in Angriffsmittel, Angriffsarten und Schwachstellen. Hinzu kommt eine Zusammenfassung der Entwicklungen im Bereich Künstlicher Intelligenz (KI) und von deren Auswirkungen auf die Bedrohungslage. Trifft eine Cyberbedrohung wie zum Beispiel ein Schadprogramm auf eine Schwachstelle, entsteht eine Gefährdung. Während Bedrohungen also unabhängig von konkreten Angriffsflächen in Wirtschaft, Staat und Gesellschaft bestehen und damit allgemeine Phänomene auf Angreiferseite beschreiben, entstehen durch zunehmende Angriffsflächen aufseiten potenzieller Opfer konkrete Gefährdungen. Solche Gefährdungen für Staat, Wirtschaft und Gesellschaft werden in Teil B dargestellt. Schließlich werden in Teil C am Beispiel herausgehobener Themen aktuelle Entwicklungen im Bereich Cybersicherheit beschrieben.

Der Bericht „Die Lage der IT-Sicherheit in Deutschland 2023“ setzt erstmals Schwerpunkte bei der Darstellung der Arbeit des BSI. Tiefergehende Informationen zu weiteren Themen wie zum Beispiel Digitaler Verbraucherschutz, Automotive und Cybersicherheit im Gesundheitswesen finden Sie in den jeweiligen Berichten oder Lagebildern genauso wie in anderen Veröffentlichungen des BSI.

Weiterführende Informationen finden Sie hier:[a]

Lagebild Gesundheit

Lagebild Automotive

Bericht Digitaler Verbraucherschutz

Weitere BSI-Publikationen

Bedrohungslage

Teil A: Bedrohungslage

2. — Zusammenfassung und Bewertung

Insgesamt zeigte sich im aktuellen Berichtszeitraum eine angespannte bis kritische Lage. Die Bedrohung im Cyberraum ist damit so hoch wie nie zuvor. Wie schon in den vergangenen Jahren wurde eine hohe Bedrohung durch Cyberkriminalität beobachtet. *Ransomware* blieb die Hauptbedrohung. Auf Angreiferseite konnte hier eine von wechselseitigen Abhängigkeiten und Konkurrenzdruck geprägte Schattenwirtschaft cyberkrimineller Arbeitsteilung festgestellt werden. Kleine und mittlere Unternehmen (KMU) sowie besonders Kommunalverwaltungen und kommunale Betriebe wurden überproportional häufig angegriffen. Im Kontext des russischen Angriffskriegs gegen die Ukraine bestand eine Bedrohung vor allem durch prorussische Hacktivismus-Angriffe, die aber keinen nachhaltigen Schaden verursachten und eher als Propagandamittel zu werten sind. Ein Anstieg der Bedrohung konnte ferner im Bereich Schwachstellen festgestellt werden. Hier wurden im Berichtszeitraum täglich 68 neue Schwachstellen in Softwareprodukten registriert – rund 24 Prozent mehr als im Berichtszeitraum davor.

Ausbau cyberkrimineller Schattenwirtschaft

Der Berichtszeitraum war gekennzeichnet durch den weiteren Ausbau einer cyberkriminellen Schattenwirtschaft. Die bereits in den vergangenen Berichtszeiträumen begonnene Ausdifferenzierung der cyberkriminellen „Wertschöpfungskette“ von *Ransomware*-Angriffen wurde im aktuellen Berichtszeitraum durch die Angreifer fortlaufend weiterentwickelt. Vom Zugang in ein Opfernetzwerk über die benötigte *Ransomware* bis hin zur Unterstützung bei Lösegeldverhandlungen können Angreifer inzwischen Werkzeuge für jeden Schritt eines komplexen Angriffs als Dienstleistung einkaufen. Die Arbeitsteilung unter den cyberkriminellen Anbietern dieser Werkzeuge führt dabei zu einer doppelten Skalierung der Bedrohung: Zum einen können cyberkriminelle Anbieter sich auf einzelne Werkzeuge spezialisieren und diese somit schneller weiterentwickeln und verbessern. Zum anderen können die verbesserten Werkzeuge auf diese Weise auch schneller einer größeren Zahl interessierter Angreifer zur Verfügung gestellt werden. Letztere, die sogenannten *Affiliates*, spezialisieren sich auf die tatsächliche Durchführung der *Ransomware*-Angriffe und zahlen von den eingetriebenen Lösegeldern Provisionen an die cyberkriminellen Anbieter der verwendeten Dienstleistungen.

Cyberresilienz

Cyberkriminelle Angreifer gingen im Berichtszeitraum zunehmend den Weg des geringsten Widerstands und wählten verstärkt solche Opfer aus, die ihnen leicht angreifbar erschienen. Nicht mehr die Maximierung des potenziellen Lösegelds stand im Vordergrund, sondern das rationale Kosten-Nutzen-Kalkül. So wurden vermehrt kleine und mittlere Unternehmen sowie Behörden der Landes- und Kommunalverwaltungen, wissenschaftliche Einrichtungen sowie Schulen und Hochschulen Opfer von *Ransomware*-Angriffen. Cyberresilienz ist daher das Gebot der Stunde.

***DDoS*-Hacktivismus**

Im Kontext des russischen Angriffskriegs gegen die Ukraine kam es im Berichtszeitraum zu einer Reihe prorussischer Hacktivismus-Angriffe in Deutschland. Die Hacktivistengruppen verwendeten dafür ausschließlich Distributed-Denial-of-Service-Angriffe (*DDoS-Angriffe*), die vornehmlich auf die Verfügbarkeit von Internetdiensten zielen und keinen nachhaltigen Schaden bewirken können wie etwa *Ransomware*-Angriffe. *DDoS*-Hacktivismus ist daher im Wesentlichen als Propagandawerkzeug zu werten, welches gesellschaftliche Verunsicherung stiften und das Vertrauen in die Fähigkeit des Staates zum Schutz und zur Versorgung der Bevölkerung unterminieren soll.

Advanced Persistent Threats

Im Berichtszeitraum waren *Advanced Persistent Threats* (APTs) mit dem Ziel der Informationsbeschaffung prägend. Während in Südost- und Zentralasien beispielsweise Telekommunikationsanbieter angegriffen wurden, standen in Europa und Nordamerika unter anderem Regierungseinrichtungen im Fokus. Anders stellte sich die Lage in der Ukraine dar, in der sowohl Cyberspionage

als auch einfache Cybersabotage zu beobachten war. Technisch war zu beobachten, dass Angriffe über verwundbare Server am Netzwerkperimeter eine Vielzahl an Schwachstellen ausnutzten.

Schwachstellen

Im Berichtszeitraum wurden durchschnittlich täglich knapp 70 neue Schwachstellen in Softwareprodukten entdeckt – rund 15 Prozent davon waren kritisch. Cybererpresser nutzten zum Beispiel zwei Schwachstellen in Filesharing-Produkten, um Daten von zahlreichen Betroffenen in Deutschland und der Welt abzugreifen und anschließend mit deren Veröffentlichung zu drohen. Aufgrund der Verbreitung der schwachstellenbehafteten Produkte ist von einer sehr großen Zahl von Betroffenen auszugehen. Darüber hinaus illustrierte ein Angriff auf die Webportale verschiedener Fahrzeughersteller die möglichen Schadwirkungen, die durch unzureichend abgesicherte Webserver entstehen: Angreifern war es dadurch möglich, sich als Händler auszugeben, somit Zugriff auf Fahrzeugfunktionen fremder Autos zu erlangen und diese über die offizielle Hersteller-App zu steuern.

Eine ausführliche Betrachtung der genannten Punkte folgt in den folgenden Kapiteln.

3. — Angriffsmittel

Cyberangriffe werden mithilfe von Schadprogrammen ausgeführt. Diese kommen auf unterschiedlichsten Wegen (zum Beispiel E-Mail-Anhang, *maliziöse* Webserver, *Exploit* usw.) zum Einsatz und ermöglichen dadurch verschiedenste Arten von Cyberangriffen (vgl. Kapitel *Angriffsarten*, Seite 14). Werden zahlreiche Computersysteme mit einem Schadprogramm infiziert und dadurch fernsteuerbar, so spricht man von einem *Botnetz*, welches seinerseits für Cyberangriffe genutzt werden kann.

3.1 — Neue Schadprogramm-Varianten

Zu Schadprogrammen zählen alle Computerprogramme, die schädliche Operationen ausführen können oder andere Programme dazu befähigen, dies zu tun. Schadprogramme gelangen unter anderem im Anhang von oder über Verlinkungen in E-Mails auf einen Computer. Wenn die Nutzerin oder der Nutzer auf einen *maliziösen* Anhang klickt oder auf einen Link, der auf eine *maliziöse* Webseite führt, kann sich das Schadprogramm installieren. Neben der E-Mail als Einfallstor zählen gefälschte

Durchschnittlicher täglicher Zuwachs neuer Schadprogramm-Varianten
Anzahl in Tausend

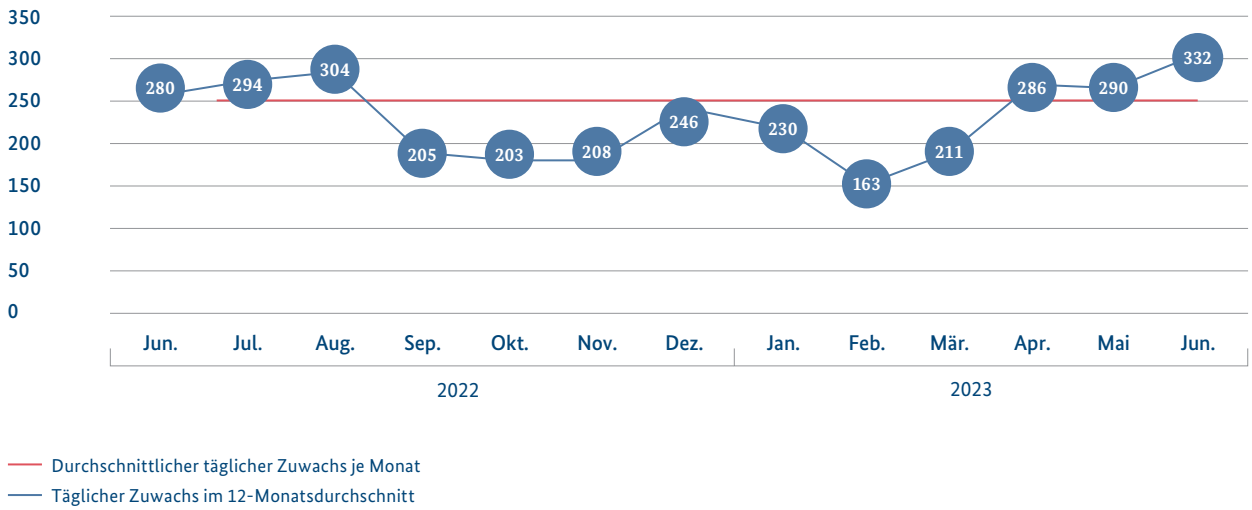


Abbildung 1: Durchschnittlicher täglicher Zuwachs neuer Schadpraogramm-Varianten
Quelle: *Malware*-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH

Links in Webseiten sowie der Missbrauch von legitimen Programmen zum Beispiel in Supply-Chain-Angriffen zu den typischen *Angriffsvektoren*. Für die Infektion angegriffener IT-Systeme nutzen Schadprogramme in der Regel Schwachstellen. Diese treten in Software- oder Hardwareprodukten, in vernetzten Geräten sowie an Netzübergängen auf. Darüber hinaus wird, wie im Fall von *Social Engineering*, der Faktor „Mensch" für Cyberangriffe immer bedeutsamer.

Die einzelnen Schadprogramme unterscheiden sich im Hinblick auf ihre Funktionalität, wobei ein Schadprogramm auch mehrere Funktionalitäten aufweisen kann. Als *Ransomware* bezeichnet man beispielsweise Schadprogramme, die durch Verschlüsselung den Zugang zu Daten oder Systemen einschränken, damit der Angreifer anschließend ein Lösegeld (engl. ransom) erpressen kann (vgl. Kapitel *Ransomware*, Seite 14). Schadprogramme, die sich als gutartige Software tarnen oder in legitimen Dateien verstecken, werden als Trojanische Pferde bezeichnet. *Bots* heißen Schadprogramme, die sich zum Beispiel mithilfe von sogenannten *Command-and-Control-Servern* fernsteuern lassen (vgl. Kapitel *Botnetze*, Seite 13).

Nimmt ein Angreifer in einem Schadprogramm Änderungen am Programmcode vor, entsteht eine neue Variante. Als neu gilt somit jede Variante, die im Hinblick auf ihre Prüfsumme (*Hashwert*) einzigartig ist. Während für bekannte Schadprogramm-Varianten Detektionsmethoden existieren, sind neue Varianten unmittelbar nach ihrem Auftreten unter Umständen noch nicht als Schadprogramm erkennbar und daher besonders bedrohlich. Im Berichtszeitraum wurden durchschnittlich täglich 250.000 neue Schadprogramm-Varianten bekannt. Das waren 22 Prozent weniger als im vergangenem Berichtszeitraum – ein Wert, der nach den großen Emotet-Wellen in den Jahren 2021 und 2022 eine Rückkehr zur durchschnittlichen Bedrohungslage anzeigt.

Schutz gegen Angriffe mit Schadprogrammen bietet neben regelmäßigen Sicherheitsupdates unter anderem Antivirensoftware, die die Schadsoftware entdecken, an einer erfolgreichen Ausführung hindern und vom System wieder entfernen kann. Manche Angriffsarten nehmen aber auch tiefgreifende Veränderungen am infizierten System vor, die sich nicht einfach rückgängig machen lassen.

3.2 — *Botnetze*

Ein mit Schadsoftware infiziertes System, das über ein zentrales Steuerungssystem, den *Command-and-Control-Server*, ferngesteuert werden kann, bezeichnet man als *Bot*. Unter einem *Botnetz* versteht man den Zusammenschluss mehrerer *Bot*s, die von einem sogenannten *Bot*master zentral ferngesteuert werden. Heutzutage können nahezu alle internetfähigen Systeme von *Bot*software befallen werden. Somit können neben klassischen Computersystemen auch Smartphones, Tablets, Router oder auch Geräte des Internets der Dinge (*Internet of Things*, *IoT*) wie Webcams oder Smart-TVs kompromittiert und übernommen werden.

Da aktuelle *Bot*software modular aufgebaut ist, können Angreifer die Funktionalitäten des *Botnetz*es auf ihren Bedarf zuschneiden und über Updates dynamisch anpassen. Neben gezielten Angriffen auf die persönlichen Daten der Opfersysteme (Informationsdiebstahl) können auch die Ressourcen des kontrollierten Systems für eigene Zwecke (z. B. Cryptomining) oder den Angriff auf Dritte (z. B. *DDoS-Angriffe*, *Spam*versand etc.) genutzt werden.

Im Berichtszeitraum wurden *Botnetz*e wie in den Vorjahren primär zum Diebstahl persönlicher Informationen (vgl. zum Thema *Information Stealer* das Kapitel *Ransomware*, Seite 14) sowie zur Verteilung weiterer Schadsoftware verwendet. Hierbei liegt der Schwerpunkt der vom BSI beobachteten *Botnetz*e klar auf mobilen Betriebssystemen auf Basis von Android. Klassische Desktop-Betriebssysteme verlieren weiter an Bedeutung.

Im Berichtszeitraum wurden durchschnittlich täglich rund 21.000 infizierte Systeme in Deutschland erkannt und vom BSI an die deutschen *Provider* gemeldet. Die Tageswerte schwankten dabei erheblich. In der Spitze wurden 45.000 infizierte Systeme gemeldet. Die *Provider* ermittelten und benachrichtigten die betroffenen Kunden. Die Anzahl der Gesamtinfektionen dürfte jedoch deutlich höher liegen, da in vielen Fällen Mehrfachinfektionen vorliegen. Die Infektionsdaten stammen überwiegend von BSI-eigenen sowie externen *Sinkhole*-Systemen, die anstelle der regulären *Command-and-Control-Server* die Kontaktanfragen von *Bot*s entgegennehmen und protokollieren. Eine Beschreibung des Sinkholing-Verfahrens sowie Steckbriefe zu den am häufigsten

gemeldeten Schadprogrammfamilien werden auf der BSI-Webseite angeboten:

Weiterführende Informationen finden Sie hier:[b]

Basierend auf Erfahrungen aus *Botnetz*abschaltungen ist davon auszugehen, dass die Dunkelziffer an Infektionen deutlich höher liegt und sich für Deutschland mindestens in einem siebenstelligen Bereich bewegt. Durch die zunehmende Professionalisierung der Angreifer und deren Fokussierung auf bestimmte Opfer ist gegenüber den Vorjahren ein Rückgang der ermittelten Infektionszahlen bei großen *Botnetz*en zu verzeichnen. Durch die steigende Anzahl verwundbarer Mobil- und *IoT*-Geräte sowie die Verfügbarkeit von Schadsoftwarecodes im Internet ist jedoch anzunehmen, dass sogenannte *Script-Kiddies* oder politisch motivierte Gelegenheitstäter Systeme infizieren, um *Botnetze* für *DDoS-Angriffe* aufzubauen.

Wie auch in den Vorjahren ist die Bedrohungslage durch *Botnetze* hoch. Die aus dem Sinkholing ermittelten Infektionszahlen stellen dabei eine Untergrenze dar, auch weil nur ein Ausschnitt der aktuell bekannten *Botnetze* aktiv erfasst werden kann. *Botnetz*familien wie Emotet, Flu*Bot* oder Glupteba ergreifen Gegenmaßnahmen, um das klassische domänennamenbasierte Sinkholing zu umgehen, indem sie beispielsweise IP-Adressen, getunnelte DNS-Verbindungen (DNS over HTTPS, DoH) oder *Blockchain*-Techniken zur Verschleierung der Kommunikation zwischen Steuerungsservern und *Bots* einsetzen.

4. — Angriffsarten

Für wesentliche Angriffsarten wird im Folgenden die Lageentwicklung im Berichtszeitraum dargestellt. Wegen des herausgehobenen Gefährdungspotenzials liegt der Schwerpunkt der Darstellung auf der Bedrohungslage im Phänomenbereich „*Ransomware*“. Es folgen Lageerkenntnisse im Bereich *Advanced Persistent Threats* und im Kontext des russischen *Angriffskrieges* gegen die Ukraine sowie zum Bereich „Distributed Denial of Service“ und zum neuen Phänomen des politisch motivierten *DDoS*-Hacktivismus. Darüber hinaus wird auch auf *Spam* und *Phishing* sowie auf Angriffe im Kontext Kryptografie eingegangen.

4.1 — *Ransomware*

Bei einem *Ransomware*-Angriff handelt es sich um eine Form der digitalen Erpressung. Die Angreifer nutzen beispielsweise Fehler wie falsche Bedienung, Fehlkonfigurationen, veraltete Softwareversionen oder mangelhafte Datensicherungen aus, um Systeme tiefgreifend zu infiltrieren und Daten zu verschlüsseln. Für die Entschlüsselung verlangen die Angreifer ein Lösegeld. Häufig wird diese Erpressung noch mit der Drohung einer Veröffentlichung zuvor gestohlener Daten kombiniert. Diese Form der Erpressung ist auch als *Double Extortion* bekannt. Das Lösegeld fungiert in solchen Fällen in der Regel auch als Schweigegeld. Die Zahlung wird meist in elektronischen Währungen (üblicherweise *Bitcoin* oder *Monero*) gefordert.

Die Effektivität von *Ransomware* beruht auf ihrer unmittelbaren Wirkung. Im Unterschied zu klassischer Schadsoftware wie Banking-Trojanern, *Botnetz*en oder *Phishing*-Mails tritt der Schaden direkt ein und hat konkrete Konsequenzen für die Betroffenen. Bei einem *Ransomware*-Angriff können zum Beispiel alle gespeicherten Dokumente verloren gehen sowie wichtige Unternehmensdaten oder kritische Dienstleistungen nicht mehr verfügbar sein. Gegen solche Angriffe helfen am besten präventive Maßnahmen. Es gilt: Vorbeugen ist besser als heilen.

Weil der Druck zur Schadensbegrenzung der Betroffenen nach einem *Ransomware*-Angriff enorm hoch ist, zahlen viele Opfer das geforderte Lösegeld in der Hoffnung, schnell wieder arbeitsfähig zu sein. Es gibt jedoch keine Garantie dafür, dass die Cybererpresser die verschlüsselten Daten tatsächlich wieder freigeben oder die gestohlenen Daten tatsächlich löschen. Auch besteht die Möglichkeit, dass das vom Angreifer zur Verfügung gestellte Entschlüsselungstool fehlerhaft ist. Das BSI rät darum ausdrücklich von der Zahlung eines Lösegelds ab. Zudem müssen einmal ausgeleitete Daten grundsätzlich als kompromittiert betrachtet werden.

Potenzielle Opfer sind Institutionen jeder Art und Größe – vom Kleinstunternehmen über Behörden und KRITIS-Unternehmen bis hin zu internationalen Konzernen, von der Kommunalverwaltung über Krankenhäuser bis hin zu wissenschaftlichen Einrichtungen, Schulen und Universitäten. Darüber hinaus werden dem BSI hin und wieder auch Massenkampagnen bekannt, die auch Verbraucherinnen und Verbraucher direkt betreffen, zum Beispiel gegen Network-Attached-Storage-(NAS-)Systeme.

Einen vollständigen Schutz vor *Ransomware*-Angriffen gibt es nicht, denn Angreifer können auch neue Angriffswege nutzen, für die noch keine Detektions- und Abwehrmethoden entwickelt wurden. Bestimmte Angriffe zum Beispiel auf Unternehmen, Behörden und IT-Dienstleister können aber durchaus auch verhindert werden. *Backup*s und Notfallpläne unterstützen dabei, die Auswirkungen im Ernstfall zu begrenzen oder sogar vollständig zu kompensieren.

4.1.1 — Angreifermotivation und Angriffsablauf

Ransomware-Angriffe werden überwiegend aus finanziell-motivierten Gründen von cyberkriminellen Angreifern verübt. Allerdings können APT-Angreifer *Ransomware* auch nutzen, um andere Angriffe zu verschleiern oder von diesen abzulenken. Zudem kann *Ransomware* auch zur reinen Sabotage eingesetzt werden. In diesem Fall agiert die *Ransomware* als *Wiper* und die verschlüsselten Daten lassen sich technisch nicht wiederherstellen (vgl. Kapitel *Advanced Persistent Threats und Bedrohungen im Kontext des Ukraine-Kriegs*, Seite 25).

4.1.1.1 — Cyberkriminelle Angriffe auf staatliche Einrichtungen

Durch den zunehmenden Dienstleistungscharakter der arbeitsteiligen cyberkriminellen Schattenwirtschaft (vgl. Kapitel *Cyberkriminelle Schattenwirtschaft*, Seite 16) bieten sich deren Services auch für andere Cyberangreifer, insbesondere APT-Gruppen, an.

Größere *Ransomware*-Angriffe gegen wichtige staatliche Einrichtungen gab es im August 2022 in Montenegro mit der *Ransomware* Cuba sowie mit einer noch unbekannten *Ransomware* im September in Bosnien-Herzegowina. In beiden Staaten wurde unter anderem das Parlament angegriffen.

Im Berichtszeitraum wurden zudem mehrere *Ransomware*-Vorfälle bekannt, die öffentlicher Berichterstattung zufolge wahrscheinlich staatlich gesteuert waren. So wurden zwischen Juli und September 2022 Angriffe auf albanische Regierungsinstitutionen mit der *Ransomware* GoneXML und dem *Wiper* ZeroShred berichtet. Diese Angriffe wurden in der Fach-Community der iranischen Gruppe Banished Kitten zugeordnet. Darüber hinaus gibt es immer wieder Berichte über den Einsatz von *Ransomware* gegen israelische Organisationen durch iranische Angreifer, bei denen die finanzielle Motivation infrage gestellt wird. Im Oktober 2022 wurde durch das Microsoft Treat Intelligence Center (MSTIC) der Einsatz der *Ransomware* Prestige unter anderem gegen Unternehmen in Polen bekannt. Im November ordnete MSTIC diese Angriffe mit hoher Wahrscheinlichkeit IRIDIUM/Sandworm zu. Diese staatlich gesteuerte Gruppe hatte unter dem Deckmantel *Ransomware* auch Sabotage-Angriffe in der Ukraine durchgeführt. Im weiteren Verlauf des Ukraine-Kriegs verzichtete die Gruppe jedoch auf die Tarnung als *Ransomware* und setzte direkt *Wiper* ein. Im Kontext des Ukraine-Kriegs besteht in der IT-Sicherheitscommunity der Verdacht, dass einige cyberkriminelle Angreifer im Auftrag des russischen Staates agieren. Dem BSI liegen hierzu jedoch keine Erkenntnisse vor.

Bei cyberkriminellen Angriffen gegen staatliche Institutionen wird eine rein finanzielle Motivation oftmals infrage gestellt. Insbesondere bei höheren staatlichen Stellen wird die Bereitschaft zur Zahlung eines Lösegelds zunehmend unwahrscheinlicher. Es ist anzunehmen, dass solche Angriffe andere Hintergründe haben, wie etwa Interessen eines anderen Staates, eine ideologische Motivation der Angreifer oder auch ein Bedürfnis der Angreifer nach Anerkennung in der cyberkriminellen Community und Aufmerksamkeit in der Presse. Weiterhin kann es auch zu Verwechselung der Angriffsziele aufseiten der Angreifer kommen. Die Mehrheit der cyberkriminellen Angriffe sind nach Einschätzung des BSI opportunistische Angriffe (vgl. Vorfall *Ransomware-Angriffe auf Kommunalverwaltungen und kommunale Versorgungsbetriebe*, Seite 69).

Welche Motivation die Angreifer jeweils treibt, lässt sich meist nicht eindeutig beantworten. Die Angreifermotivation kann jedoch einen erheblichen Unterschied im Verlauf des Angriffs und auch bei der Angriffsbewältigung machen, etwa bei der Frage, ob es überhaupt um Lösegeld geht oder zum Beispiel um den Geltungsdrang des Angreifers.

4.1.1.2 — Angriffsablauf

Cyberkriminelle Angreifer werden anhand der eingesetzten Schadsoftware und Vorgehensweise in Gruppen zusammengefasst. So wird beispielsweise die *Ransomware*

Alphv (auch bekannt als BlackCat) von einer anderen Gruppierung eingesetzt als die *Ransomware* LockBit 3.0.

Angriffsphase 1 – Erstinfektion: Ein *Ransomware*-Angriff beginnt häufig mit einer *maliziö*sen E-Mail, der Kompromittierung eines Fernzugriff-Zugangs (Remote-Zugang) wie zum Beispiel Remote Desktop Protocol (RDP) oder der Ausnutzung von Schwachstellen (vgl. Kapitel *Schwachstellen in Softwareprodukten*, Seite 33). Diese initiale Infektion stellt den Ausgangspunkt für das weitere Vorgehen des Angreifers dar. Wenn der Einbruch von einem *Access Broker*, also einem „Makler" für erbeutete Zugangsdaten, ausging, können mitunter Wochen und Monate vergehen, bis der Zugang an einen *Ransomware*-Angreifer verkauft wird.

Angriffsphasen 2 und 3 – Rechteerweiterung und Ausbreitung: Nach dem Einbruch verfügt der Angreifer nur über diejenigen Zugriffsrechte, die der kompromittierte Account besitzt. Deshalb laden Angreifende in der Regel weitere Schadsoftware nach, um die erlangten Zugriffsrechte zu erweitern und zum Beispiel an Administratorrechte zu gelangen. Ein Administrator kann zum Beispiel Software installieren oder auch deinstallieren. Mit erweiterten Zugriffsrechten breitet sich der Angreifer (teil-) automatisiert im Netzwerk der betroffenen Organisation aus – bis hinein in die zentralen Komponenten der Rechteverwaltung (z. B. Active Directory) – und versucht, diese vollständig zu übernehmen. Passiert dies, ist das Unternehmens- oder Behördennetzwerk vollständig kompromittiert und nicht mehr vertrauenswürdig. Die Angreifer besitzen dann alle Rechte, um beispielsweise Benutzerkonten mit Administratorrechten anzulegen, Daten einzusehen oder auch sogenannte *Backdoor*s einzurichten, Schadprogramme, die einen permanenten Zugriff auf das kompromittierte System ermöglichen.

Angriffsphase 4 – Datenabfluss: Anschließend können Angreifer Daten entwenden (Datenexfiltration), um später mit deren Veröffentlichung zu drohen, falls ein Opfer nicht zu einer Lösegeld- oder Schweigegeldzahlung bereit ist.

Angriffsphase 5 – Verschlüsselung: Daten werden auf möglichst vielen Systemen verschlüsselt, insbesondere auf *Backup*-Systemen, in der Regel ohne das Betriebssystem selbst zu beeinträchtigen. Stattdessen hinterlassen die Angreifer Nachrichten mit Hinweisen, wie die Opfer Kontakt für Löse- oder Schweigegeldverhandlungen aufnehmen können. Einzelne Angreifergruppen verzichten inzwischen auch ganz auf die Verschlüsselung und erpressen direkt mit den gestohlenen Daten.

Angriffsphase 6 – Incident Response: Die Betroffenen stehen vor der Herausforderung, ihre Systeme und Daten wiederherzustellen. Je nach Ausmaß der Betroffenheit muss dafür ein Übergangsbetrieb organisiert und der Vorfall an die Stakeholder, also an Eigentümer, Kunden und Partner, kommuniziert werden. In der Regel wird in dieser Phase ein IT-Sicherheitsdienstleister hinzugezogen, der Erfahrung in der Bewältigung von IT-Sicherheitsvorfällen hat.

4.1.2 — Cyberkriminelle Schattenwirtschaft

Ransomware-Angriffe stellen unverändert die größte cyberkriminelle Bedrohung dar. Dabei trifft die zunehmend professionelle Arbeitsteilung der Angreifergruppen auf die zunehmend vernetzte Welt von teils multinationalen Unternehmen. Im Falle eines erfolgreichen *Ransomware*-Angriffs bleiben Schäden oft nicht mehr nur auf regionale Betriebseinheiten beschränkt, sondern breiten sich unter Umständen unabhängig von nationalen und territorialen Grenzen weltweit im Unternehmensnetzwerk aus.

Angesichts der millionenschweren Lösegelder, die *Ransomware*-Angriffe abwerfen, entwickelt sich auf Angreiferseite eine von wechselseitigen Abhängigkeiten und Konkurrenzdruck geprägte Schattenwirtschaft cyberkrimineller Arbeitsteilung: von der notwendigen technischen Infrastruktur und *Malware* über *Access Broker* bis zum cyberkriminellen Callcenter. Wenn sich eine neue Methode für Angriffe anbietet, bildet sich daraus früher oder später eine cyberkriminelle Dienstleistung, die diese Methode vielen Angreifern zugänglich macht.

Bestandteile eines Cyberangriffs werden an jeweils spezialisierte Angreifergruppen ausgelagert, vergleichbar mit dem Outsourcing von Dienstleistungen. Es wird als *Cybercrime-as-a-Service* (*CCaaS*, Cyberstraftat als Dienstleistung) bezeichnet. *CCaaS* erlaubt es einem Angreifer, nahezu jeden Schritt eines Angriffs als Dienstleistung von anderen Cyberkriminellen zu beziehen oder zumindest die dafür notwendige Schadsoftware. Dies ist ein herausragender Faktor für die Entwicklung der Bedrohungslage, denn die Spezialisierung auf eine bestimmte Dienstleistung ermöglicht es Angreifern, diese gezielt zu entwickeln und ihre Effektivität zu steigern. Darüber hinaus stehen die Dienstleistungen vielen Angreifern gleichzeitig zur Verfügung. Dadurch verkürzt sich der Zeitraum zwischen der Entwicklung einer neuen

Methode und deren verbreitetem Einsatz stark oder fällt ganz weg. Dies erklärt auch zum Teil die dynamischen Entwicklungen, die in den vergangenen Jahren im cyberkriminellen Raum beobachtet wurden.

Beispielhaft sei an dieser Stelle das Phänomen des Access-as-a-Service (AaaS) herausgegriffen. Die Angreifer werden hier häufig als *Access Broker* bezeichnet. Sie erbeuten auf verschiedenste Weise Identitätsdaten oder Zugänge zu konkreten Computersystemen. Im Kontext von *Ransomware* treten insbesondere zwei Formen des AaaS auf: der Diebstahl von Identitäts- und Zugangsdaten über *Information Stealer* zum einen und die Kompromittierung von Netzwerken zum anderen.

Diebstahl von Identitäts- und Zugangsdaten: *Information Stealer* sind Schadprogramme, die Angreifer über E-Mails mit *maliziö*sem Anhang oder Link auf einen schadcodebehafteten Webserver verteilen (sogenannter *Malware-Spam*). Darüber hinaus tarnen Angreifer *Information Stealer* als legitime Software, die sie im Internet zum Download anbieten. *Information Stealer* zielen darauf ab, verschiedenste Informationen auf einem kompromittierten System zu sammeln. Dazu zählen zum Beispiel in Browsern hinterlegte Zugangsdaten, etwaige Krypto-Wallets und Informationen weiterer Softwareprodukte, die Aufschluss über eine Person oder Zugang zu Vermögenswerten erlauben könnten. Diese Daten werden nach der Infektion eines Systems gesammelt und an den Angreifer ausgeleitet. Dieser zusammengestellte Datensatz wird als Log bezeichnet und zum Beispiel auf Untergrundmarktplätzen wie Russian Market, 2easy oder Genesis Market für 10 bis 60 US-Dollar pro Log verkauft. Die Logs enthalten überwiegend Identitätsdaten und können für Angriffe im Rahmen des Identitätsdiebstahls verwendet werden. Befinden sich in diesen Logs Zugangsdaten zu einem Firmennetz oder Session-Cookies einer *Cloud*anwendung, können diese für einen *Ransomware*-Angreifer ein Einfallstor in das entsprechende Netzwerk darstellen.

Kompromittierung von Netzwerken: Im Unterschied zu einem *Ransomware*-Angriff richtet ein *Access Broker* keinen unmittelbaren Schaden an. Sein Ziel ist es, einen anhaltenden Zugang in das kompromittierte Netzwerk zu schaffen. Dieser wird über Untergrundforen und private Kanäle zum Beispiel an *Ransomware*-Angreifer oder auch APT-Gruppen weiterverkauft. Gelingt es dem *Access Broker* dabei bereits, die erlangten Zugriffsrechte zu erweitern, steigt der Verkaufswert dieses Zugangs.

Noch bis in den vergangenen Berichtszeitraum hinein waren *maliziö*se Office-Dokumente das häufigste Angriffsmittel für die initiale Infektion. Im Laufe des Jahres 2022 ersetzten Angreifer diese durch *maliziö*se Container-Dateien mit Formaten wie ISO oder IMG. Opfer erhielten dabei zwar weiterhin E-Mails mit den *maliziö*sen Anhängen oder Links zum Download der Anhänge, jedoch änderten die Angreifer die Auswahl dafür verwendeter Dateien. Grund dafür dürfte die standardmäßige Deaktivierung von Makros in Office-Produkten durch Microsoft gewesen sein.

Die Verwendung von *maliziö*sen Container-Dateien war für Angreifer besonders Erfolg versprechend, da eine Schwachstelle dafür sorgte, dass das *Mark-of-the-Web* (*MOTW*, eine zusätzliche Schutzmaßnahme für Endgeräte) nicht an Dateien innerhalb des Containers weitergegeben wurde. Am 8. November 2022 wurde die Schwachstelle behoben. In der Folge wurden *maliziö*se Container-Dateien in Angriffskampagnen seltener verwendet. Anfang 2023 wechselten die Angreifer dann mehrheitlich zu *maliziö*sen OneNote-Dateien für *Spam*- und *Phishing*-Mails.

OneNote-Dateien sind so ausgestaltet, dass sie verschiedene andere Dateien enthalten können. Mit ähnlichen Methoden wie bei *maliziö*sen Office-Dokumenten (zum Beispiel *Social Engineering*) können Opfer dazu verleitet werden, diese eingebetteten *maliziö*sen Dateien auszuführen.

Neben dem Einsatz von *Spam*- und *Phishing*-Mails zur Verteilung von *Malware* kam es im Berichtszeitraum gehäuft zu Callback-*Phishing* sowie SEO Poisoning und Malvertising.

Callback-*Phishing*: Hierbei sendet der Angreifer eine fingierte Rechnung oder ein ähnliches Dokument, um das Opfer zum Anruf bei einem Callcenter unter der Kontrolle des Angreifers zu bewegen. Das Callcenter leitet das Opfer dann zum Download und zur Ausführung der *Malware* an.

SEO Poisoning und Malvertising: Beide Methoden setzen oftmals auf legitime Software als Deckmantel. So ahmen die Angreifer die Webseiten und Webdomains legitimer Softwareprodukte nach. Fällt ein Opfer hierauf herein, lädt es sich neben der legitimen Software auch eine *Malware* nach, die im Hintergrund ausgeführt wird, ohne dass das Opfer es bemerkt. SEO Poisoning kommt vom englischen Begriff für Suchmaschinenoptimierung (Search Engine Optimization, SEO). Dabei wird die Web-

seite des Angreifers über die Position in den Suchergebnissen einer Suchmaschine ausgespielt. Der Angreifer versucht deshalb, eine möglichst hohe Platzierung in den Suchergebnissen zu erreichen. Bei Malvertising, zusammengesetzt aus *Malware* und Advertising, wird *Malware* gemeinsam mit legitimen Werbeanzeigen ausgespielt. Ein Nutzer wird auch hier zum Download einer zumeist legitimen Software verleitet, die mit *Malware* kombiniert wurde. Darin besteht der Unterschied zu *Drive-by-Exploits*, bei denen allein das Besuchen einer Webseite zu einer Kompromittierung führt.

Grundsätzlich passen Angreifer ihre Vorgehensweise zeitnah an, wenn sich die Gegebenheiten ändern.

Ransomware-as-a-Service

Die aktivsten und damit auch bedrohlichsten *Ransomware*-Familien wurden im Berichtszeitraum in Form von *Ransomware* als Dienstleistung (*Ransomware*-as-a-Service, *RaaS*) betrieben und angeboten. Insbesondere die *RaaS* LockBit 3.0 und die *RaaS* Alphv stechen heraus. Im Mittelpunkt stand die Entwicklung von exklusiven Services für besonders erfolgreiche *Affiliates*. Dabei werden den *Affiliates*, die hohe Provisionen an Lösegeldern einbringen, zusätzliche Dienstleistungen jenseits der *Ransomware* zur Verfügung gestellt.

Sowohl LockBit 3.0 als auch Alphv boten so zum Beispiel im Berichtszeitraum ausgewählten *Affiliates* zusätzliche *Ransomware*-Varianten an, die auf einem anderen *Quellcode* aufbauten und weitere Funktionen umfassten. Auch weiterführende Services wie *DDoS-Angriffe*, Unterstützung bei der Verhandlung oder exklusive *Access Broker* wurden von Betreibern einiger *RaaS* angeboten.

Cyberkriminelle Gruppen konkurrieren durchaus um ihre *Affiliates*, daher spielt in der Szene auch die Reputation der eigenen „Marke“ eine wichtige Rolle. Diese Art der Rivalität führt zu einer zunehmenden Verschärfung der Bedrohungslage. Ein entscheidendes Argument für einen *Affiliate* bei der Auswahl der *RaaS* ist beispielsweise, wie viel Druck auf einen Betroffenen ausgeübt werden kann. So führt der Konkurrenzkampf zwischen cyberkriminellen Gruppen zu einer Maximierung des Drucks auf betroffene Opfer. Andere Unterscheidungsmerkmale zwischen *RaaS*-Angeboten sind auch der Anteil am Lösegeld, der beim *Affiliate* verbleibt, oder die fortlaufende Verbesserung der *Ransomware* selbst. Zum einen können solche exklusiven Services die erfolgreichsten *Affiliates* längerfristig an eine *RaaS* binden. Zum anderen dürften diese Services andere *Affiliates* dazu motivieren, aktiver zu werden oder höhere Lösegelder zu verlangen.

Bemerkenswert für die *RaaS* LockBit 3.0 war im Sommer 2022 die Einführung einer monetären Belohnung für das Auffinden von Schwachstellen (*Bug Bounty*) für die *RaaS* selbst. Ganz ähnlich zu legitimen Bug-Bounty-Programmen rufen die Angreifer dabei dazu auf, Schwachstellen in der *Ransomware* oder dem *RaaS*-Angebot oder auch die Möglichkeit von Rückschlüssen auf die Identität der Angreifer gegen die Auszahlung einer Bounty zu melden.

Too big to stay afloat

Es zeigen sich also Parallelen zwischen der legalen Wirtschaft und der cyberkriminellen Schattenwirtschaft, die sich, getrieben durch *Ransomware*-Angriffe, in den vergangenen Jahren weiterentwickelt hat. So ähnelt die Aufteilung von Aspekten eines Angriffs wie AaaS und *RaaS* dem Outsourcing von Aufgaben an Dienstleister. Die Maximierung des Erpressungsdrucks dient den Angreifern auch dazu, möglichst hohe Lösegelder einzunehmen, was dem Streben nach Gewinn in der Wirtschaft in der Intention nicht unähnlich ist.

Unternehmen und Institutionen, die als zu groß oder zu wichtig gelten, um zu scheitern, werden gemeinhin als „too big to fail“ bezeichnet. Dazu gehörten zum Beispiel in der weltweiten Finanzkrise 2008 zahlreiche Banken, die nur mit staatlichen Hilfen vor der Insolvenz gerettet werden konnten. Im Gegensatz zu Unternehmen und Institutionen können cyberkriminelle Gruppen jedoch nicht „too big to fail“ werden. Sie werden stattdessen „too big to stay afloat“ (zu groß, um den Kopf über Wasser zu halten). Ist eine Gruppe von Cyberkriminellen erfolgreich, steigt ihre öffentliche Bekanntheit und damit auch die Aufmerksamkeit, die sie bei Sicherheitsfachleuten und Strafverfolgungsbehörden genießt. Daher war es bisher nur eine Frage der Zeit, bis solche Gruppen unschädlich gemacht werden konnten oder sich gezwungen sahen unterzutauchen. So wurde etwa Emotet im Januar 2021 erstmals abgeschaltet. Die *RaaS* DarkSide löste sich nach einem besonders erfolgreichen Cyberangriff auf und auch die *RaaS* REvil verschwand nach einem besonders erfolgreichen Angriff. Das „Conti-Syndikat“ zersplitterte im Mai 2022, mutmaßlich wegen unterschiedlicher Auffassungen zum russischen Angriffskrieg gegen die Ukraine.

4.1.3 — Schweigegeld-Erpressung mit Datenleaks und weitere Erpressungsmethoden

Seit 2021 gehen *Ransomware*-Angriffe in der Regel mit einem Datenleak einher. Dieses Vorgehen ist bekannt als Schweigegeld-Erpressung oder *Double Extortion*. Die Leak-Opfer-Statistik des BSI gibt Aufschluss über die Opfer von Schweigegeld-Erpressungen. Zu diesem Zweck beobachtet das BSI sogenannte Leak-Seiten, auf denen Angreifer die Namen und die erbeuteten Daten von Opfern ihrer *Ransomware*-Angriffe veröffentlichen, wenn diese kein Lösegeld zahlen. Durch die Veröffentlichung ihrer Daten auf einer Leak-Seite werden *Ransomware*-Opfer gleichsam zum zweiten Mal Opfer einer Cybererpressung.

Über diese Leak-Seiten lassen sich also mutmaßliche Opfer erfassen, denen mit der Veröffentlichung ihrer Daten gedroht wurde. Die Leak-Opfer-Statistik ist insoweit keine Statistik über *Ransomware*-Angriffe, sondern über Opfer von Schweigegeld-Erpressungen. Daher wird auch von mutmaßlichen Opfern gesprochen, denn die Nennung auf einer Leak-Seite unter Kontrolle eines Angreifers bedeutet nicht zwingend, dass es tatsächlich auch zu einem Angriff kam. In einigen Fällen nennen Angreifer Namen auch nur zum Zwecke der Erpressung, ohne dass tatsächlich ein Angriff stattgefunden hat.

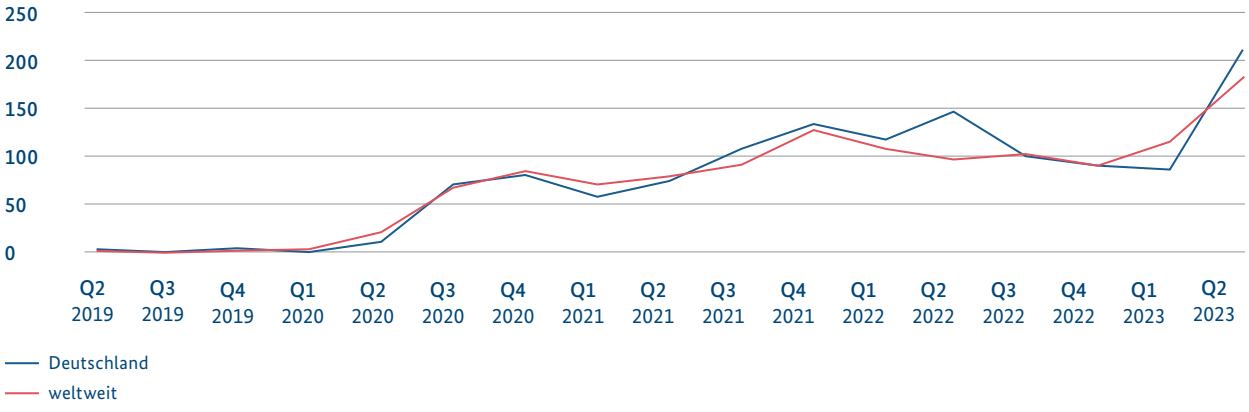
Mit der Beobachtung von Leak-Seiten wird nur ein Teil der *Ransomware*-Opfer erfasst. So werden in der Regel nur diejenigen Organisationen auf Leak-Seiten genannt und veröffentlicht, die die Zahlung eines Löse- oder Schweigegelds verweigern. Ein großes Dunkelfeld an *Ransomware*-Opfern verbleibt daher. Daher gibt diese Erfassung auch keinen Aufschluss darüber, wie viele der tatsächlichen Opfer sich zur Zahlung eines Löse- oder Schweigegeldes entscheiden. Zudem gibt der Zeitpunkt der Veröffentlichung keinen Aufschluss über den Zeitpunkt des *Ransomware*-Angriffs, der bereits lange zuvor stattgefunden haben kann. Die Kategorisierung der so erfassten mutmaßlichen Opfer nach Ländern ist darüber hinaus nur eine Annäherung, da sie in der Regel nach dem Standort der Hauptniederlassung des mutmaßlichen Opfers erfolgt. Das angegriffene Netzwerksegment kann sich daher insbesondere bei global agierenden Unternehmen auch in anderen Teilen der Welt befunden haben.

Die ersten Cyberangriffe mit Schweigegeld-Erpressung und Leak-Seiten wurden 2019 beobachtet. Im ersten Quartal 2019 griff die sich selbst „Team Snatch“ nennende cyberkriminelle Gruppe einige Opfer an. Im vierten Quartal 2019 begann die cyberkriminelle Gruppe hinter der *RaaS* Maze, *Ransomware*-Angriffe mit Leaks zu kombinieren.

Im Jahr 2020 setzte sich diese Vorgehensweise bei verschiedenen cyberkriminellen Gruppen durch, worüber das BSI als *Proliferation* cyberkrimineller Vorgehensweisen berichtete (vgl. Die Lage der IT-Sicherheit in Deutschland 2022). Mit dem Jahr 2021 wurden Double-Extortion-Angriffe zur Regel bei einem *Ransomware*-Angriff. Diese Entwicklung zeigte sich in der stetigen Zunahme bis ins vierte Quartal 2021.

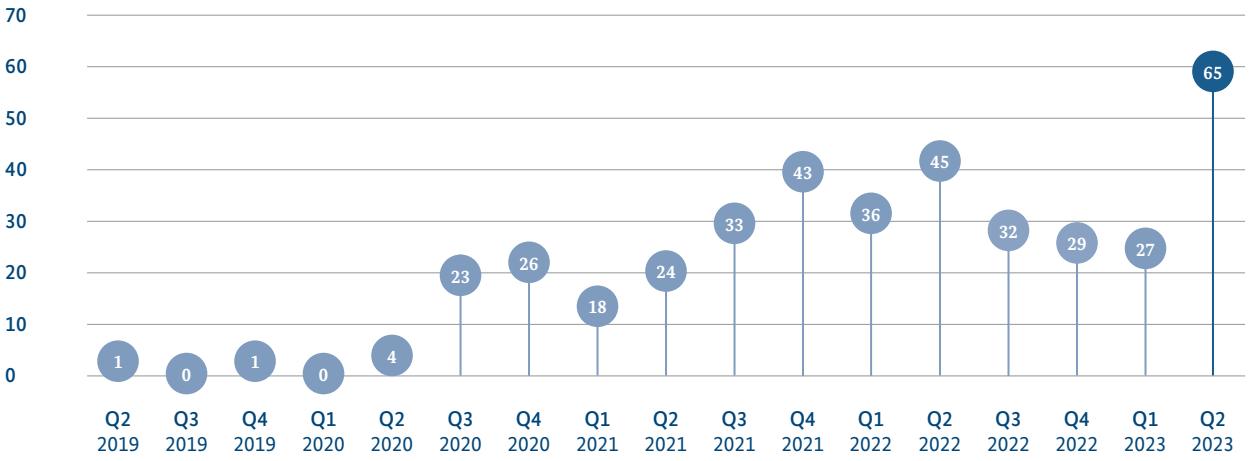
Mutmaßliche Opfer auf Leak-Seiten aus Deutschland und weltweit im Vergleich
2021 = 100

Abbildung 2: Mutmaßliche Opfer auf Leak-Seiten aus Deutschland und weltweit im Vergleich (2021=100)
Quelle: Leak-Opfer-Statistik des BSI



Mutmaßliche Opfer aus Deutschland auf Leak-Seiten
Anzahl

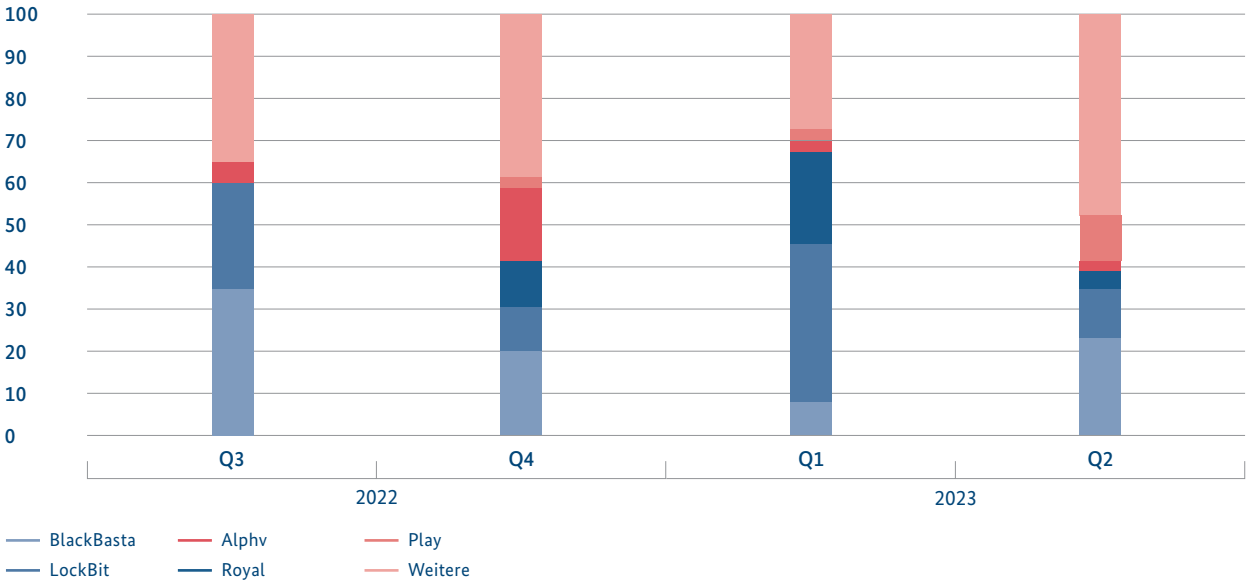
Abbildung 3: Mutmaßliche Opfer aus Deutschland auf Leak-Seiten (Anzahl)
Quelle: Leak-Opfer-Statistik des BSI



Mit 1.003 so erfassten mutmaßlichen Opfern weltweit im vierten Quartal 2021 und 45 Opfern aus Deutschland im zweiten Quartal 2022 waren die vorläufigen Höhepunkte der Zeitreihe erreicht. Sowohl bei der weltweiten Betrachtung als auch der Beschränkung auf die Deutschland zugeordneten Opfer ist in den folgenden Quartalen eine leichte Abnahme und anschließende Stabilisierung zu beobachten. Im zweiten Quartal 2023 war dann die höchste Zahl an Leak-Opfern seit Beginn der Erfassung zu verzeichnen. Grund dafür waren zwei neue Leak-Seiten. MalasLocker war eine bislang einmalige Kampagne mit vermutlich hacktivistischem Hintergrund. Die Seite 8Base dagegen steht mit mindestens zwei *Ransomware*-Familien in Verbindung und dürfte sich etabliert haben.

Mutmaßliche Opfer aus Deutschland nach Leak-Seiten
Anteile in %

Abbildung 4: Mutmaßliche Opfer aus Deutschland auf Leak-Seiten (Anteile)
Quelle: Leak-Opfer-Statistik des BSI



Mutmaßliche Opfer weltweit nach Leak-Seiten
Anteile in %

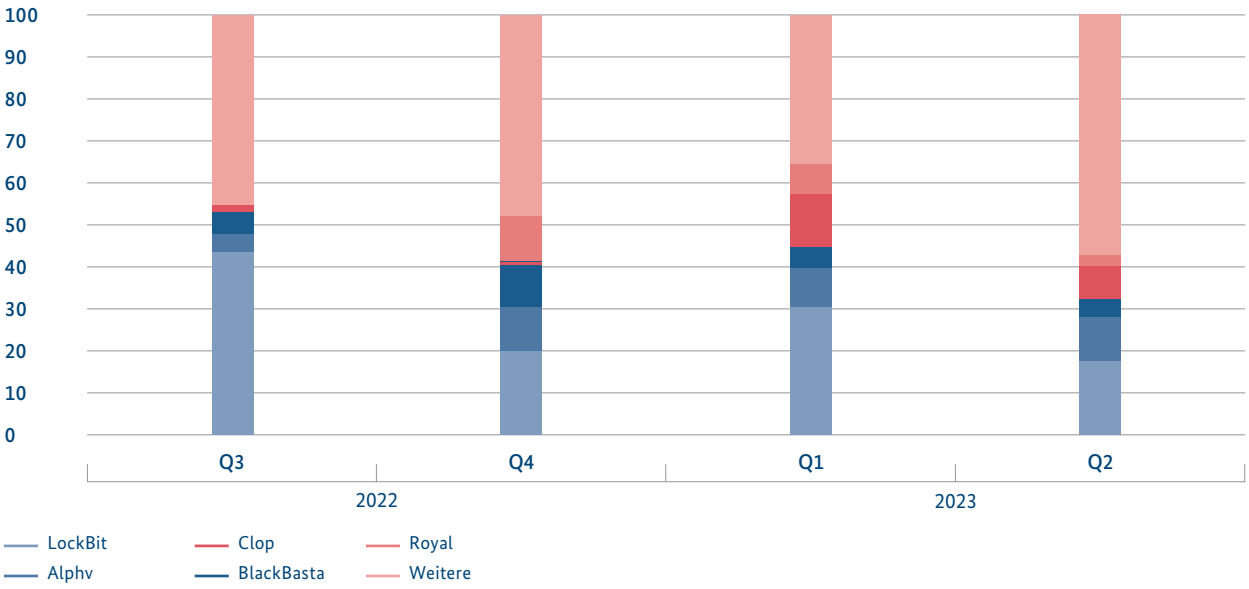


Abbildung 5: Mutmaßliche Opfer weltweit nach Leak-Seiten (Anteile)
Quelle: Leak-Opfer-Statistik des BSI

Die fünf aktivsten Leak-Seiten sind regelmäßig für rund 50 Prozent der mutmaßlichen Opfer verantwortlich. Die *RaaS* LockBit 3.0 ist sowohl bei der Beschränkung auf Deutschland (vgl. Abbildung 4) wie auch bei weltweiter Betrachtung (vgl. Abbildung 5) die aktivste *Ransomware*. Die Leak-Seite von LockBit nannte im Berichtszeitraum insgesamt über 800 weltweit verteilte mutmaßliche Opfer.

Die beiden *RaaS* Black Basta und Royal werden in der IT-Sicherheitscommunity als eine Art Nachfolger der aufgelösten *RaaS* Conti beobachtet. Beide *RaaS* sind erst 2022 in Erscheinung getreten und haben sich schnell unter den Top 5 der aktivsten *Ransomware*-Familien platziert.

Die *RaaS* Alphv (auch bekannt als BlackCat) wurde erstmals im November 2021 beobachtet und zählt mit LockBit zu einer der bedrohlichsten *Ransomware*-Familien. Im Jahr 2023 nahm die cyberkriminelle Gruppe Vice Society Platz 5 der Rangliste ein. Bemerkenswert an Vice Society ist, dass diese Gruppe keine eigene *Ransomware* entwickelte, sondern die *Ransomware* anderer *RaaS* verwendet.

Neben den oben beschriebenen Lösegeld- und Schweigegeld-Erpressung flankieren Angreifer die Verhandlungen mit dem Opfer häufig durch zusätzliche Erpressungsmethoden, um den Zahlungsdruck zu erhöhen. Verglichen mit vergangenen Berichtszeiträumen sind diese weiteren im Folgenden beschriebenen Erpressungsmethoden weitestgehend unverändert geblieben (vgl. Die Lage der IT-Sicherheit in Deutschland 2022). Lediglich die Angreifer hinter der *RaaS* Alphv versuchten im aktuellen Berichtszeitraum in Einzelfällen eine neue Erpressungsmethode. Dabei stellten die Angreifer Daten der Betroffenen über das offene Internet in durchsuchbarer Form auf einer Webseite zur Verfügung. Dies erlaubte jeder Nutzerin und jedem Nutzer des Internets Zugriff auf die Daten. Eine Ausbreitung und Übernahme dieser Methode durch andere Angreifer ist möglich, konnte bislang jedoch noch nicht durch das BSI beobachtet werden.

Erregung öffentlicher Aufmerksamkeit: Einige Angreifer gehen aktiv auf Kundinnen und Kunden des Opfers oder die Öffentlichkeit zu, um zusätzlichen Druck auszuüben. Dies geht über die Veröffentlichung von Opferinformationen auf dafür eingerichteten Leak-Seiten hinaus. Beispielsweise wenden sich Angreifer per E-Mail an Kundinnen und Kunden oder Mitarbeitende eines Opfers und informieren diese darüber, dass aufgrund eines nicht gezahlten Schweigegelds sensible Daten über sie öffentlich wurden. Insbesondere bei einem intransparenten Umgang des Opfers mit dem Datenleak kann dies den Ruf des Opfers langfristig schädigen. Eine pflichtgemäße Meldung an zuständige Datenschutz- oder Regulierungsbehörden kann die negativen Auswirkungen begrenzen (vgl. Kapitel *Erkenntnisse zur Gefährdungslage in der Gesellschaft*, Seite 51).

Verkauf oder Veröffentlichung sensibler Daten: Ist der Betroffene nicht bereit zu zahlen, versteigern oder verkaufen einige Angreifer erbeutete Daten an Dritte. Mit diesen Daten können die Käufer ihrerseits das Opfer erpressen. Dies gilt insbesondere dann, wenn es sich um wertvolle Geschäftsgeheimnisse oder kompromittierende Informationen über Einzelpersonen handelt. An wen solche Daten letztendlich versteigert werden, lässt sich in der Regel nicht mehr feststellen. Finden die Angreifer keinen Käufer, so veröffentlichen sie die Daten auf einer dafür vorgesehenen Leak-Seite. Daten, die einmal abgeflossen sind, gelten selbst im Fall einer erfolgten Schweigegeld- oder Lösegeldzahlung grundsätzlich dauerhaft als kompromittiert.

Abseits der Kombination dieser Erpressungsmethode mit *Ransomware* im Rahmen der *Double Extortion* beobachtet das BSI auch Leak-Seiten von Angreifern, die ihre Opfer ohne den Einsatz von *Ransomware* erpressen. Dabei kompromittieren die Angreifer die Opfer auf dieselbe Weise wie bei einem *Ransomware*-Angriff, verzichten jedoch auf den Einsatz von *Ransomware*. Das BSI nimmt an, dass die Angreifer dadurch schneller von der initialen Infektion zur Erpressung eines Schweigegelds übergehen können.

Androhen einer Meldung bei der zuständigen Datenschutz- oder Regulierungsbehörde: Im Zusammenhang mit einem Cyberangriff können Betroffene gegen die Datenschutz-Grundverordnung oder andere Regulierungen verstoßen, wenn sie beispielsweise ihren Meldepflichten nicht nachkommen oder nachweisbar ist, dass sensible Daten zum Beispiel auf schlecht abgesicherten Webservern lagen. Solche Sorgfaltspflicht- oder Meldepflichtverletzungen seitens der Opfer nutzen einige Angreifer als Druckmittel zweiter Ordnung. Sie drohen, die Regulierungsbehörden über den Verstoß zu informieren. Da der Angriff sowie kompromittierte Daten auch über andere Wege öffentlich werden können, sollten Betroffene Gesetzesverstöße vermeiden, indem sie frühzeitig und pflichtgemäß eine Meldung abgeben.

Einsatz von *DDoS-Angriffen* in der Verhandlungsphase: Einzelne Angreifer setzen während der Verhandlung eines Lösegelds zusätzlich *DDoS-Angriffe* ein, um das Opfer weiter unter Druck zu setzen. Diese Angriffe können zusätzliche Incident-Response-Maßnahmen erfordern und damit auch die Reaktion auf den *Ransomware*-Angriff behindern.

4.1.4 — Maßnahmen

Lösegeldzahlungen bieten grundsätzlich keine Garantie für die Freigabe verschlüsselter Daten. Sie tragen zudem dazu bei, dass sich kriminelle Organisationen und Schattenwirtschaften professionalisieren und wachsen. Daher empfiehlt das BSI, auf Lösegeldzahlungen zu verzichten. Wichtiger ist es, wirksame Vorkehrungen gegen *Ransomware*-Angriffe zu treffen.

4.1.4.1 — Schutzmaßnahmen nach Angriffsphasen

Ein *Ransomware*-Angriff besteht aus mehreren Schritten (vgl. Kapitel *Angriffsablauf*, Seite 15). Für jede Phase eines solchen Angriffs sind Gegenmaßnahmen möglich, um das Eindringen in Netzwerke oder das Verschlüsseln von Daten zu verhindern und möglichen Schaden zu begrenzen. Diese Maßnahmen werden der jeweiligen Angriffsphase zugeordnet dargestellt.

Angriffsphase 1 – Einbruch

Die drei häufigsten Einfallsvektoren von *Ransomware*-Gruppen sind *Malware-Spam* oder Links auf schadcodebehaftete Server, die Ausnutzung von Schwachstellen sowie der Zugriff über schlecht abgesicherte externe Zugänge. Für jedes dieser Einfallstore existieren wirksame Maßnahmen.

Gegenmaßnahme *Malware-Spam*: E-Mails und Sensibilisierung
Empfangene E-Mails sollten grundsätzlich als „Nur-Text“ oder „reiner Text“ codiert angezeigt werden. Dies kann durch die Endnutzerin und den Endnutzer oder die Systemadministratorin oder den Systemadministrator entsprechend eingerichtet werden. Im Gegensatz zur Darstellung als „HTML-Mail“ werden in der Darstellung als Nur-Text-Mails keine eventuell enthaltenen Makros oder versteckten Befehle ausgegeben. Zudem lassen sich Webadressen nicht mehr verschleiern. In einer HTML-codierten Mail könnte zum Beispiel ein Link mit der Bezeichnung „www.bsi.de“ in Wahrheit auf eine schadcodebehaftete Webseite verweisen. Ist eine Nur-Text-Codierung nicht möglich oder nicht erwünscht, sollte zumindest die Ausführung aktiver Inhalte in HTML-Mails unterdrückt werden, damit *maliziöse* Skripte nicht mehr ausgeführt werden können.

Mitarbeitende sollten im Rahmen von Sensibilisierungsmaßnahmen praxisnah bzgl. der Risiken im Umgang mit E-Mails geschult werden. Das gilt besonders für Mitarbeitende aus Behörden- und Unternehmensbereichen, die ein hohes Aufkommen an externer E-Mail-Kommunikation (etwa in der Personalabteilung oder im Marketing) zu bewältigen haben.

Gegenmaßnahme Schwachstellen: *Patches* und Updates
Um Infektionen zu vermeiden, die auf der Ausnutzung von Schwachstellen beruhen, für die es bereits Sicherheitsupdates gibt, sollten diese Updates nach der Bereitstellung durch den Softwareanbieter unverzüglich in die IT-Systeme eingespielt werden – über die zentrale Softwareverteilung des Netzwerks idealerweise auch in alle Desktop-Computer und Notebooks, die zum Firmennetzwerk gehören. Updates, die Schwachstellen von hoher Kritikalität schließen oder sich auf besonders exponierte Software wie Firewalls oder Webserver beziehen (oder beides), sollten priorisiert behandelt werden.

Gegenmaßnahme Remote-Zugang: Multifaktor-*Authentifizierung* (MFA)
Häufig versuchen Cyberkriminelle, *Ransomware* über kompromittierte Remote-Zugänge auf Systemen zu installieren. Daher sollte auch der Zugriff von außen abgesichert werden – normalerweise über Virtual Private Networks (*VPN*s) in Kombination mit einer Multifaktor-*Authentifizierung*.

Angriffsphase 2 – Rechteerweiterung

Gegenmaßnahme: Administrator-Accounts absichern
Grundsätzlich sollten mit privilegierten Accounts nur Administratorentätigkeiten durchgeführt werden. Das Lesen von E-Mails oder das Surfen im Internet gehören nicht dazu. Administratorinnen und Administratoren sollten sich für solche Tätigkeiten, die keine erweiterten Zugriffsrechte erfordern, auch zusätzliche Nutzerkonten mit begrenzten Rechten anlegen. Privilegierte Konten sollten immer über eine Multifaktor-*Authentifizierung* geschützt sein. Zudem sollten für die Administration von Clients keine Domänen-Administrationskonten verwendet werden.

Angriffsphase 3 – Ausbreitung

Gegenmaßnahme: Netzwerk segmentieren
Eine saubere Netzwerksegmentierung hilft, Schäden zu begrenzen, da eine eventuell eingeschleuste *Ransomware* zunächst nur die Systeme im jeweiligen Segment erreichen kann. Auch dafür ist die sichere Verwendung von Administrator-Accounts notwendig.

Angriffsphase 4 – Datenabfluss

Gegenmaßnahme: Anomalie-Detektion
Durch eine Anomalie-Detektion im Netzwerk ist es möglich, zeitnah einen potenziell unerwünschten Datenabfluss zu erkennen. Hierfür ist es nötig, den regulär anfallenden Netzwerkverkehr sehr gut zu kennen. Auf Basis dieses Normalzustands können dann Schwellenwerte gewählt werden, bei deren Über- oder Unterschreitung das System anschlägt. Auch können hierbei die Zeitzone und der Standort berücksichtigt werden. Außerhalb der regulären Arbeitszeiten für einen Betriebsstandort sollten die Schwellenwerte anders sein als während des regulären Betriebs.

Angriffsphase 5 – Verschlüsselung

Gegenmaßnahme: *Backups* und Datensicherung
*Backup*s sind der beste Schutz vor den Auswirkungen einer Verschlüsselung durch *Ransomware*, denn sie gewährleisten die unmittelbare Verfügbarkeit von Daten auch für diesen Fall. Dafür müssen die Daten aber in einem Offline-*Backup* gesichert werden, das nach einem *Backup* von den übrigen Systemen des Netzwerkes getrennt wird. Erst dann sind sie vor Angriffen und Verschlüsselung geschützt. Zu einem *Backup* gehören immer auch die Planung und Vorbereitung des Wiederanlaufs und der Wiederherstellung der Daten. Dies sollte regelmäßig getestet werden, um Komplikationen und Herausforderungen bei der Wiederherstellung bereits vor einem Ernstfall zu erkennen.

Angriffsphase 6 – Incident Response

Gegenmaßnahme: Notfallplan
Für das Worst-Case-Szenario eines erfolgreichen Angriffs, bei dem alle Systeme im Netzwerk verschlüsselt wurden, sollte eine Notfallplanung für Notbetrieb und Wiederaufbau existieren. Die Prozesse zur Reaktion und Wiederherstellung geschäftskritischer Systeme sollten in regelmäßigen Abständen geübt werden. Insbesondere müssen vorab die geschäftskritischen Systeme identifiziert werden und alternative Kommunikationsmöglichkeiten außerhalb des kompromittierten Netzwerks vorbereitet sein. Telefonnummern und Daten von wichtigen Kontaktpersonen sollten offline in Papierform vorgehalten werden.

4.1.4.2 — Unterstützung durch das BSI

Das BSI kann im Rahmen seines gesetzlichen Auftrags bestimmte Betroffene bei der Bewältigung von IT-Sicherheitsvorfällen unterstützen. Die gesetzlich definierten Zielgruppen des BSI sind

- die Betreiber von Kritischen Infrastrukturen (gemäß BSI-Kritisverordnung – BSI-KritisV),
- Institutionen der Bundesverwaltung / Stellen des Bundes,
- Unternehmen im besonderen öffentlichen Interesse.

In begründeten Einzelfällen kann das BSI auch bei solchen Institutionen tätig werden, die nicht zu den drei genannten Zielgruppen zählen. Ein begründeter Einzelfall liegt insbesondere dann vor, wenn es sich um einen Angriff von besonderer technischer Qualität handelt, die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems von besonderem öffentlichem Interesse ist oder eine wichtige Stelle eines Landes betroffen ist.

Die Vorfallsbearbeitung im BSI wird federführend durch die Fachreferate des *CERT-Bund* durchgeführt. Dabei wird im Bedarfsfall auch auf die gesamte Expertise des BSI zurückgegriffen. Dazu zählen Expertinnen und Experten aus den Bereichen Forensik und *Malware*-Reverse-Analyse, Incident Response (Mobile Incident Response Team (MIRT)), Cybersicherheit in Industrieanlagen, Detektion (Bundes Security Operations Center, BSOC) und Betriebssysteme sowie Penetrationstesterinnen und -tester.

Über das im BSI angesiedelte Nationale Cyber-Abwehrzentrum (Cyber-AZ) können bei Bedarf auch weitere Sicherheitsbehörden zum Austausch, zur Bewertung oder zur Bearbeitung von Cybersicherheitsvorfällen hinzugezogen werden.

Das Nationale IT-Lagezentrum führt zusammen mit dem *CERT-Bund* eine Erstbewertung einer Vorfallsmeldung durch. Dazu wird in der Regel eine sogenannte Triage-Besprechung mit den Betroffenen durchgeführt. In dieser Besprechung werden ein gemeinsames Verständnis des Vorfalls erarbeitet sowie mögliche Maßnahmen diskutiert. Darauf aufbauend werden dann die geeigneten weiteren Maßnahmen vereinbart.

Das BSI bietet eine Vielzahl an Produkten und Dokumenten an, die Betroffenen sowohl präventiv als auch im Rahmen der Vorfallsbearbeitung reaktiv zur Verfügung gestellt werden können. Dazu zählen zum Beispiel Dokumente zur Prävention, Detektion und Reaktion bei APT-Vorfällen, Hilfsdokumente für die Vorfallsbearbeitung bei schweren IT-Sicherheitsvorfällen wie *Ransomware*-Vorfällen und viele mehr.

Weitere Informationen und Hilfsdokumente:[c]

Das BSI kann Behörden und Unternehmen zudem hinsichtlich des koordinierten und strukturierten Vorgehens bei Sicherheitsvorfällen, der Umsetzung von geeigneten Maßnahmen, der Durchführung eines angemessenen IT-Krisenmanagements und der passenden Krisenkommunikation beraten.

In besonders herausgehobenen Fällen kann das BSI einen Vor-Ort-Einsatz mit einem Mobile Incident Response Team (MIRT) durchführen. Das MIRT kann das Opfer in einer Vielzahl von Bereichen unterstützen, so zum Beispiel bei der Erstbewertung, bei der Grobanalyse und Abschätzung der Konsequenzen sowie bei der Sichtung von Protokolldaten und Alarmen. Darüber hinaus kann das BSI auch im Rahmen der technischen Beweissicherung tätig werden, wie zum Beispiel bei der Erstellung von Festplatten-Images oder der Aufzeichnung von Netzwerkverkehr sowie bei der technischen Analyse im Backoffice, und das lokale Betriebspersonal bei der Bereinigung beratend unterstützen. Weiterhin können Empfehlungen zur Härtung der Systeme gegen Cyberangriffe gegeben werden.

Das BSI kann Opfer nicht nur mit der eigenen Expertise unterstützen, sondern auch bei der Suche nach geeigneten Incident-Response-Dienstleistern helfen. Hierfür hat das BSI eine entsprechende Liste qualifizierter Dienstleister veröffentlicht. Alle darauf befindlichen Dienstleister wurden anhand der vom BSI festgelegten Kriterien auf ihre Kompetenz beim Umgang mit schwerwiegenden IT-Sicherheitsvorfällen überprüft und konnten sich entsprechend qualifizieren.

Die Liste der qualifizierten Dienstleister finden Sie hier:[d]

4.2 — *Advanced Persistent Threats* und Bedrohungen im Kontext des Ukraine-Kriegs

Advanced Persistent Threats (APT) unterscheiden sich von anderen Bedrohungen der Cybersicherheit durch die Motivation und die Vorgehensweise der Angreifer. Während zum Beispiel Schadprogramme von kriminellen Angreifern in der Regel massenhaft und ungezielt verteilt werden (vgl. Kapitel *Ransomware*, Seite 14), sind APT-Angriffe oft langfristig und mit großem Aufwand geplante Angriffe auf einzelne ausgewählte, herausgehobene Ziele. APT-Angriffe dienen nicht der kriminellen Gewinnerzielung, sondern der Beschaffung von Informationen über das Ziel und gegebenenfalls der Sabotage.

Beobachtungen aus Cyberoperationen in der Ukraine

Im aktuellen Berichtszeitraum gab es eine Reihe von Entwicklungen, die die APT-Bedrohungslage prägten. So entstand durch den russischen Angriffskrieg auf die Ukraine erstmalig die Situation, dass ein Staat mit ausgeprägten Cyberfähigkeiten in einem bewaffneten Konflikt mit einem anderen hoch digitalisierten Staat stand. Zu beobachten war in diesem Zusammenhang eine große Bandbreite an Phänomenen im Cyberraum, darunter Cyberspionage, Hacktivismus, Desinformation einschließlich Veröffentlichung gestohlener Daten sowie Cybersabotage. Dies ermöglichte erstmals einen empirischen Blick auf die Rolle von Cyberfähigkeiten in einem Krieg zwischen einem Aggressor und einem Partnerstaat Deutschlands.

Cybersabotage: Für die Bedrohungslage ist stets relevant, welche Arten von Zielen angegriffen werden. So haben sich die Angreifer in der Ukraine bei der Cybersabotage nicht auf Kritische Infrastrukturen im engeren Sinne beschränkt. Stattdessen wurden in der Ukraine vergleichsweise breitflächig in verschiedenen Sektoren und Branchen Sabotageakte durchgeführt. Zum Einsatz kam dabei *Wiper*-Schadsoftware, die Daten löscht. Diese Schadprogramme waren für Sabotage in normalen Büronetzen ausgelegt. Nur in einem Fall wurden Spezial-Schadprogramme wie Industroyer2 für Prozesssteuerungsanlagen entdeckt, und zwar im ukrainischen Energiesektor, konkret bei Angriffsversuchen auf Umspannwerke in der Ukraine. Der Angriffsversuch auf die Umspannwerke ereignete sich erst einige Monate nach Kriegsbeginn. Dagegen wurde als eines der ersten Ziele – nämlich am Tag des Überfalls – ein Satelliten-Kommunikationsbetreiber angegriffen, der laut Medienberichten Dienste für das ukrainische Militär erbrachte (vgl. Die Lage der IT-Sicherheit in Deutschland 2022). Seitdem liegen kaum Berichte über Cyberangriffe auf militärische Systeme vor, was allerdings auf eine unvollständige Informationslage zurückzuführen sein dürfte.

Cyberspionage: Eine weitere wesentliche Erkenntnis ist, dass die Cybersabotage gegen ukrainische Ziele auf wenige Angreifergruppen beschränkt war. Es waren im Berichtszeitraum zwar weitere Gruppen in der Ukraine aktiv, die jedoch größtenteils auf Informationsbeschaffung zielten. Diese Arbeitsteilung dürfte weniger technische Gründe als vielmehr organisatorische oder strategische Gründe gehabt haben.

Um *Malware* überhaupt einsetzen zu können, werden *Angriffsvektoren* benötigt. Mehrere öffentlich dokumentierte Fälle belegen, dass in der Anfangszeit des Kriegs von den Angreifern kompromittierte Netzwerkzugänge genutzt wurden, die bereits vor dem Krieg bestanden. Es wurden keine technisch neuen *Angriffsvektoren* wie zum Beispiel neue Schwachstellen oder neue Supply-Chain-Angriffe beobachtet.

Hacktivismus und Desinformationskampagnen in Deutschland und anderen westlichen Staaten

Ein Phänomen, das im Zusammenhang mit dem russischen Angriffskrieg gegen die Ukraine in Deutschland größere Medienaufmerksamkeit erhielt, ist prorussischer *DDoS*-Hacktivismus, der allerdings nur begrenzte Schadwirkung entfaltete (vgl. zum *DDoS*-Hacktivismus Kapitel *Distributed Denial of Service*, Seite 28). Proukrainischen Hacktivismus gab es in wenigen Fällen, vor allem zu Beginn des Kriegs, als ein deutsches Unternehmen mit Verbindungen nach Russland kompromittiert wurde (vgl. Die Lage der IT-Sicherheit in Deutschland 2022).

Anders als *DDoS*-Hacktivisten, die lediglich mit begrenzter Schadwirkung Internetdienste vorübergehend beeinträchtigen können, dringen Cyberspione oder -saboteure tief in IT-Netze ein, um Daten zu vernichten oder zu leaken. Dies ist ein Vorgehen, das zukünftig weiteres Potenzial für Angreifer bietet, denn je nach Sensibilität der gestohlenen Daten können diese in Desinformationskampagnen genutzt werden, um die öffentliche Meinung zu beeinflussen. Das wachsende Gruppengeflecht von Hacktivisten wird es zudem in Zukunft auch staatlich gesteuerten Angreifergruppen zunehmend ermöglichen, sich als Hacktivisten auszugeben.

Weiterhin waren Operationen zu beobachten, bei denen durch *Phishing*- oder *Malware*-Einsatz gewonnene Infor-

mationen für Desinformation genutzt wurden. Während dies in osteuropäischen Staaten wie Polen und im Baltikum für die Gruppe Ghostwriter bereits vor dem Krieg bekannt war, hat die Gruppe Callisto seit Beginn des Ukraine-Kriegs solche Operationen Berichten von Sicherheitsbehörden und Sicherheitsfirmen zufolge auch in Großbritannien durchgeführt. Aufgrund des heterogenen IT-Sicherheitsniveaus bei deutschen politischen Einrichtungen und Medien könnten solche Fälle von Datenleaks auch in Deutschland auftreten.

Jenseits des Kriegs in der Ukraine gab es weitere Entwicklungen im Cyberraum, die die Anstrengungen von Angreifergruppen zeigten, ihre Angriffe zu verschleiern und zu optimieren.

Anonymisierungsnetze als Dienstleistung für APT-Gruppen

Prägnant ist die Etablierung mehrerer *Botnetze* aus Routern, *IoT*-Geräten und Virtual-Private-Servern, die von APT-Gruppen für unbefugte Zugriffe aus dem Internet (Scans, *Exploit*-Anwendung und *Webshell*-Zugriffe) betrieben werden. Diese *Botnetze* dienen der Anonymisierung des Angriffsverkehrs, vergleichbar mit legitimen Proxy-Serversystemen. Damit verstetigt sich eine Entwicklung, die bereits im vergangenen Berichtszeitraum beobachtet wurde: Es werden zunehmend Server angegriffen, die direkt aus dem Internet erreichbar sind. Es werden also nicht mehr nur Angriffsmails versandt, sondern vermehrt bestehende Schwachstellen in Webservern, Firewalls oder *VPN*-Servern ausgenutzt. Um diese Systeme auszukundschaften und dann zu kompromittieren, benötigen die Angreifer anonymisierte Internetverbindungen, die sie über die neu geschaffenen *Botnetze* selbst ermöglichen.

Überblick über relevante APT-Gruppen

Für deutsche Ziele stellten im Berichtszeitraum mindestens die in Tabelle 1 benannten APT-Gruppen eine Bedrohung dar. Die Gruppen sind in der Regel vor allem gegen Ziele in den angegebenen Sektoren aktiv. Institutionen, die bereits Basis-IT-Sicherheitsmaßnahmen umgesetzt haben, sollten Berichte über die folgenden Gruppen priorisiert auswerten. Die aufgeführten typischen Angriffstechniken beziehen sich allerdings auf die erste Phase eines Angriffs und sind daher nicht vollständig. Zudem agieren manche der Gruppen sehr vielseitig, sodass auch andere Techniken in der initialen Angriffsphase zum Einsatz kommen können.

APT-Gruppe	Bevorzugte Ziele	Bevorzugte Techniken
APT15 | VixenPanda | Mirage | Ke3chang	Regierungseinrichtungen | NGOs	*Exploits* gegen aus dem Internet erreichbare Systeme
APT27 | Emissary Panda | LuckyMouse	Energie | Telekommunikation | Pharma	*Exploits* gegen aus dem Internet erreichbare Systeme
APT28 | FancyBear | Sofacy	Regierungseinrichtungen | Militär | Medien | NGOs	*Exploits* gegen aus dem Internet erreichbare Systeme
APT29 | Nobelium | DiplomaticOrbiter	Regierungseinrichtungen	Mails mit Archivdaten als Anhang, die LNK-Dateien enthalten
APT31 | JudgementPanda | ZIRCONIUM	Regierungseinrichtungen | NGOs	*Exploits* gegen aus dem Internet erreichbare Systeme; Bruteforcing
Ghostwriter bzw. Untergruppe UNC1151	Politik | NGOs | Medien	Mails mit Links auf *Phishing*-Seite
Kimsuky | VelvetChollima	Rüstung | Kanzleien	Word-Dokumente, die makrobehaftete Remote Templates nachladen; *Social Engineering*
Lazarus | SilentChollima	Rüstung | Luftfahrt	Mails mit Archivdaten als Anhang, die trojanisierte Anwendungen enthalten; *Social Engineering*
MustangPanda (oder VertigoPanda)	Regierungseinrichtungen	Mails mit Archivdaten als Anhang, die LNK-Dateien enthalten
Snake | VenomousBear | Turla	Regierungseinrichtungen | Export	*Exploits* gegen aus dem Internet erreichbare Systeme
UNC2589	Logistik	Mails mit makrobehafteten Dokumenten im Anhang

Tabelle 1: Für Deutschland relevante APT-Gruppen
Quelle: BSI

Supply-Chain-Angriff infolge eines anderen Supply-Chain-Angriffs

Sachverhalt

In einem spektakulären Einzelfall gelang einer APT-Gruppe ein Supply-Chain-Angriff, der durch einen vorhergehenden erfolgreichen Supply-Chain-Angriff ermöglicht wurde. Am 29. März 2023 berichteten mehrere IT-Sicherheitsunternehmen, dass Detektionen und Logdateien bei ihren Kunden auf einen Supply-Chain-Angriff hindeuten, der auf einen Anbieter im Bereich Voice-over-IP-Kommunikation (VoIP-Kommunikation) für Geschäftskunden mit mehreren Hunderttausend Kunden zielte. Es stellte sich heraus, dass mehrere vom Hersteller signierte Installationspakete einer VoIP-Software für Windows und MacOS eine manipulierte Softwarebibliothek enthielten und ausführten. Diese versuchte in mehreren Schritten, einen Command-und-Control-Server zu kontaktieren und weiteren Schadcode herunterzuladen. Diese Installationspakete waren offiziell vom Hersteller bereitgestellt und signiert, sodass von einem Supply-Chain-Angriff, also von einer erfolgreichen Kompromittierung des Herstellers, ausgegangen werden konnte. Der CEO des Anbieters bestätigte in der Folge in einem Forenbeitrag die Medienberichte und den erfolgreichen Angriff auf das eigene Unternehmen.

Eine mit der Untersuchung des Vorfalls beauftragte Sicherheitsfirma fand Folgendes heraus: Der ursprüngliche Angriffsvektor für die Kompromittierung des Anbieters für VoIP-Kommunikation war die Installation einer anderen legitimen Software für Finanz-Transaktionen. Diese Finanz-Software, die ein Schadprogramm enthielt, hatte der Anbieter von der Webseite ihres Herstellers heruntergeladen. Es hatte also bereits ein Angriff auf den Hersteller der Finanz-Transaktionssoftware stattgefunden, sodass es zu einer Verkettung von Supply-Chain-Angriffen kam: Zuerst wurde das Unternehmen für Finanz-Software angegriffen und dessen legitime Software um ein Schadprogramm ergänzt. Diese legitime, aber schadprogrammbehaftete Software wurde dann bei dem Anbieter für VoIP-Kommunikation installiert, wodurch wiederum dessen Software um ein Schadprogramm ergänzt wurde, was Ende März 2023 bei dessen Kunden detektiert wurde.

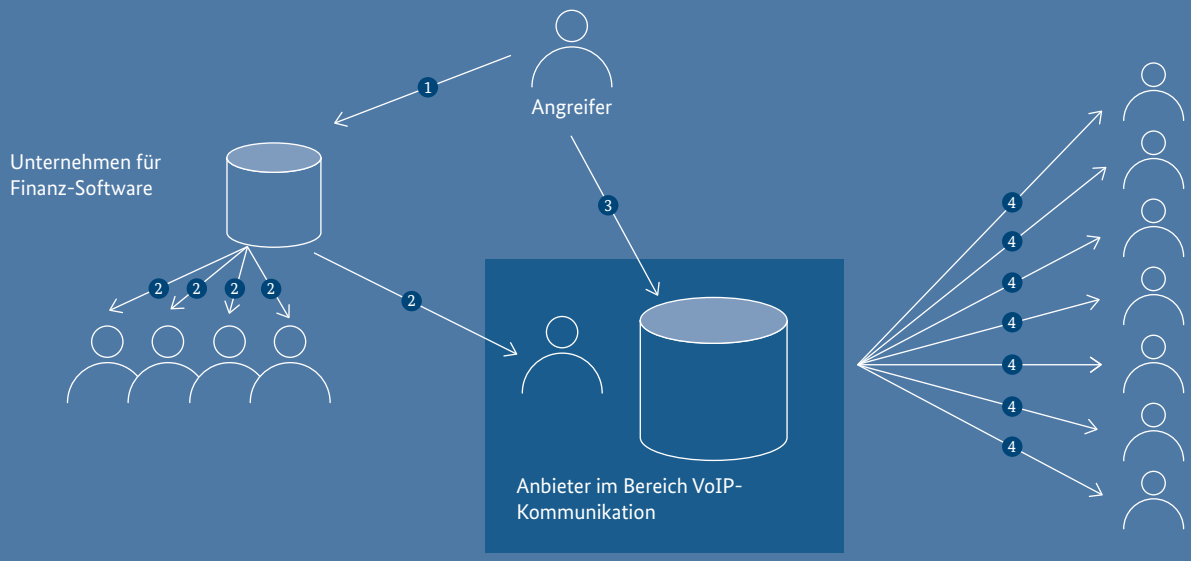


Abbildung 6: Supply-Chain-Angriff infolge eines Supply-Chain-Angriffs

1. Angreifer infiltriert Hersteller einer Software für Finanztransaktionen und kompromittiert legitime Software.
2. Opfer laden kompromittierte Software für Finanztransaktionen herunter, darunter ein Mitarbeiter eines Anbieters von VoIP-Software.
3. Angreifer kompromittiert VoIP-Software, um den Angriff auf eine Vielzahl potenzieller weiterer Opfer ausweiten zu können.
4. Weitere Opfer laden die kompromittierte VoIP-Software herunter.

Bewertung
Ein Supply-Chain-Angriff hat das Potenzial, eine Vielzahl von Opfern gleichzeitig zu kompromittieren. Maßnahmen wie die Signierung von Softwarepaketen und der Download von offiziellen Webseiten greifen hier nicht, da der Angreifer in der Lage ist, sein Schadprogramm bereits im Produktionsprozess der Software zu verankern, sodass dieses wie offizieller Programmcode signiert und bereitgestellt wird.

Die mehreren Hunderttausend Kunden im vorliegenden Fall zeigen eindrucksvoll das Potenzial eines solchen Angriffs. Möglich wären hier Ransomware-Angriffe oder Spionage bei den Kunden, wobei die tatsächliche Motivation hinter dem beschriebenen Fall bisher unklar ist. Hervorzuheben ist die Verkettung verschiedener Supply-Chain-Angriffe wie in diesem Fall: Sie zeigt, dass Angreifer willens und in der Lage sind, Zugänge sehr detailliert zu analysieren, über einen längeren Zeitraum zu beobachten und abzuwägen, ob diese Zugänge systematisch und mit hohem Aufwand für Folgeangriffe genutzt werden können.

Laut öffentlicher Berichterstattung wird der Angriff dem Subcluster „Labyrinth Chollima" zugeordnet, einem Teil der häufig als Lazarus bezeichneten APT-Gruppen.

Reaktion
Nach Bekanntwerden des Angriffs hat der Anbieter für VoIP-Kommunikation die Deinstallation der betroffenen Softwareversionen empfohlen und bereinigte Installationspakete bereitgestellt. Das BSI hat seine Zielgruppen ebenfalls gewarnt. Weiterhin wurde die Infrastruktur zum Nachladen weiterer Schadsoftware schnell blockiert, sodass die Infektionskette in diesem Fall frühzeitig unterbrochen werden konnte. Im Nachgang ist der Hersteller transparent mit dem Vorfall umgegangen und hat über den Stand der Untersuchungen und deren Ergebnisse informiert.

4.3 — Distributed Denial of Service

Denial-of-Service-Angriffe (*DoS*-Angriffe) sind Angriffe auf die Verfügbarkeit von Internetdiensten. Häufig sind Webseiten Ziel solcher Angriffe. Die zugehörigen Webserver werden dabei so mit Anfragen überflutet, dass die Webseiten nicht mehr erreichbar sind. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem Distributed-Denial-of-Service-Angriff (*DDoS-Angriff*).

Angreifer verfolgen mit *DDoS-Angriffen* unterschiedliche Ziele. Zum einen kann es sich auch um eine in den Cyberraum übertragene Form der Schutzgelderpressung handeln. Angreifer fordern dabei Geld vom Opfer, um die Angriffe zu stoppen. Auch im Rahmen eines *Ransomware*-Vorfalls kann *DDoS* eingesetzt werden, um den Druck auf das Opfer zu erhöhen und ein Lösegeld für verschlüsselte Daten zu erpressen. Zum anderen können Angreifer *DDoS-Angriffe* auch nutzen, um Institutionen direkt zu schaden. Gründe können zum Beispiel Wettbewerb unter konkurrierenden Unternehmen oder Aktivismus sein (zum Beispiel durch sogenannte *Script-Kiddies*). Ein *DDoS*-Angriff kann weiterhin auch genutzt werden, um von einem anderen, anspruchsvolleren Angriff wie etwa *Ransomware* (vgl. Kapitel *Ransomware*, Seite 14) oder APT (vgl. Kapitel *Advanced Persistent Threats und Bedrohungen im Kontext des Ukraine-Kriegs*, Seite 25) abzulenken. Im Rahmen des russischen Angriffskriegs gegen die Ukraine kam es darüber hinaus international auch zu politisch motivierten *DDoS-Angriffen*, die unter das Phänomen des Hacktivismus fallen.

Die Folgen eines *DDoS*-Angriffs sind zum einen finanzielle Schäden für Dienstleister oder Onlineshops, wenn diese nicht erreichbar sind. Zum anderen können Imageschäden und gegebenenfalls Unsicherheit in der Bevölkerung folgen, wenn im Fall von Hacktivismus kritische Dienstleistungen und Webseiten beispielsweise von Banken oder der Polizei in ihrer Verfügbarkeit beeinträchtigt werden.

Die Anzahl der bekannt gewordenen *DDoS-Angriffe* in Deutschland wird durch einen Index gemessen (vgl.

Bekannt gewordene *DDoS-Angriffe* (Messzahl) in Deutschland
2021=100

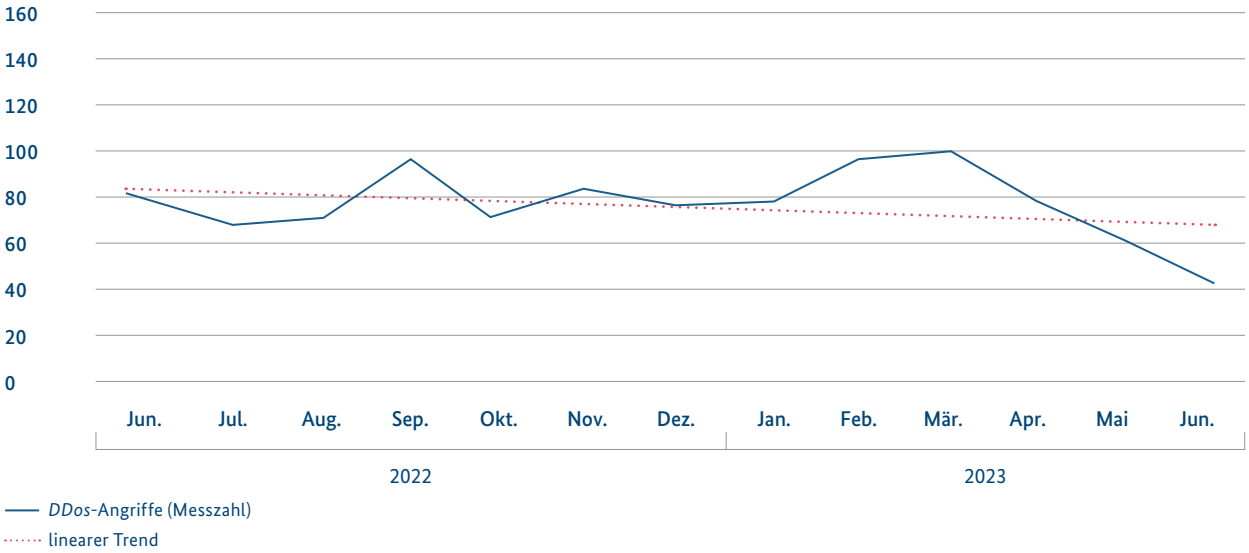


Abbildung 7: Bekannt gewordene *DDoS-Angriffe* (Messzahl) in Deutschland (2021=100)
Quelle: *DDoS*-Statistik des BSI

Abbildung 7). Ein Index von beispielsweise 95 Punkten im Februar 2023 bedeutet, dass die Anzahl der *DDoS-Angriffe* in Deutschland im Februar 0,95-mal so hoch war wie im Jahresdurchschnitt 2021.

Der Indikator zeigt im September 2022 sowie im Frühjahr 2023 *DDoS-Angriffe* prorussischer Hacktivisten in Deutschland an, die insgesamt nur geringe Schadwirkungen entfalteten und auch zahlenmäßig hinter den Häufigkeiten von kriminellen *DDoS-Angriffe*n in früheren Berichtszeiträumen zurückblieben. Im Gegensatz zu *Ransomware*- oder APT-Angriffen können Angreifer mit *DDoS* keine Netzwerke hacken oder kapern, sondern lediglich Internetdienste vorübergehend beeinträchtigen. Es ist daher davon auszugehen, dass das Interesse des *DDoS*-Hacktivismus in Deutschland nicht darin bestand, tatsächlich umfangreichen materiellen Schaden anzurichten. Vielmehr dürfte das Ziel der Angreifer darin bestanden haben, gesellschaftliche Verunsicherung zu schüren und das Vertrauen in die Fähigkeiten des Staates zum Schutz und zur Versorgung der Bevölkerung zu beschädigen.

Im Gegensatz zum vergangenen Berichtszeitraum war im aktuellen Berichtszeitraum keine Steigerung von *DDoS-Angriffe*n an absatzstarken Aktionstagen wie dem Black Friday, dem Cyber Monday oder auch dem Vorweihnachtsgeschäft zu erkennen. Insgesamt ist in der zweiten Jahreshälfte 2022 die Anzahl der *DDoS-Angriffe* im Vergleich zur ersten Jahreshälfte 2022 deutlich zurückgegangen. Nach den hacktivistischen Kampagnen im ersten Quartal 2023 setzte sich im zweiten Quartal 2023 der schon länger zu beobachtende rückläufige Trend cyberkrimineller *DDoS-Angriffe* fort.

Im Dezember 2022 gelang den Strafverfolgungsbehörden ein Schlag gegen *DDoS*-as-a-Service-Angebote: Europol berichtete über die Abschaltung von etwa 50 Webseiten, die Dienste für gezielte *DDoS-Angriffe* anboten. Einer dieser Dienste soll für über 30 Millionen *DDoS-Angriffe* weltweit verantwortlich gewesen sein. Mehrere Administratoren der Webseiten konnten festgenommen werden. An der Aktion waren Behörden aus den USA, dem Vereinigten Königreich, den Niederlanden, Deutschland und Polen beteiligt.[1]

Informationen zu *DDoS*-Prävention und -Mitigation sowie eine Liste qualifizierter Dienstleister für *DDoS*-Mitigation finden Sie hier:[e]

DDoS-Hacktivismus

Sachverhalt
Im Zuge des russischen Angriffskriegs gegen die Ukraine formierten sich verschiedene Gruppierungen prorussischer Hacktivisten, die DDoS-Angriffe auch gegen deutsche Ziele durchführten. Im Sommer 2022 machte so die Hacktivisten-Gruppe Killnet von sich reden (vgl. Die Lage der IT-Sicherheit in Deutschland 2022). Zudem rief die Gruppe NoName057 das Projekt „DDoSia" ins Leben. Dabei handelt es sich um ein Botnetz, das gezielt für hacktivistische Angriffe aufgebaut wurde. Im Herbst 2022 begannen die Anbieter von DDoSia mit der Anwerbung von Affiliates, die das Botnetz für Angriffe auf Internetdienste westlicher Behörden verwenden sollten. Potenziellen Affiliates wurde eine Geldprämie in Aussicht gestellt.

Die verschiedenen Hacktivisten-Gruppen zeichnen für zahlreiche DDoS-Angriffe auch in Deutschland verantwortlich; darunter auf Webseiten und Internetportale von Flughäfen, Polizeien und Landesregierungen. Kennzeichnend für die Angriffe ist, dass die Gruppierungen diese jeweils vorher öffentlichkeitswirksam auf ihren Social-Media-Kanälen ankündigten. Auf der Zielliste des DDoSia-Projekts befanden sich beispielsweise Webdienste mehrere Landespolizeien und Institutionen der Bundesländer. Aufgeführt wurden dabei Webseiten der Polizeien in Brandenburg, NRW, Niedersachsen, Bremen, Hessen, Mecklenburg-Vorpommern, Rheinland-Pfalz sowie Landesdomains des Saarlands oder Sachsen-Anhalts. Darüber hinaus wurden auch Webseiten von Bundesbehörden sowie die Webseite www.ukraine-wiederaufbauen.de angegriffen.

Bewertung
Die genannten Angriffe entfalteten nur begrenzte Schadwirkung. Grund dafür ist, dass DDoS-Angriffe generell keine tiefere Infiltration von Netzwerken oder nachhaltige Schäden ermöglichen, wie sie etwa durch Datenverschlüsselung entstehen. Sie können aber zu kurzzeitigen Ausfällen oder verlangsamtem Aufruf von Webseiten für einen begrenzten Zeitraum führen. Solche Angriffe lassen sich durch die Aktivierung entsprechender DDoS-Schutzmechanismen wirksam mitigieren.

Es ist daher davon auszugehen, dass das Ziel der Angreifer darin bestand, gesellschaftliche Verunsicherung zu schüren und das Vertrauen in demokratische Institutionen sowie in die Fähigkeiten des Staates zum Schutz und zur Versorgung der Bevölkerung zu beschädigen.

Reaktion
Das BSI informierte die zuständigen Landes-CERTs über die Erkenntnisse und stand während der gesamten Zeit im direkten Austausch mit den Landes-CERTs.

4.4 — *Spam* und *Phishing*

Eine unerwünschte E-Mail bezeichnet man im Allgemeinen als *Spam*. Häufig wird *Spam* über kompromittierte oder angemietete Server versandt. Gleichermaßen können gestohlene E-Mail-Adressen hierfür ausgenutzt werden, die ursprünglich einem legitimen Account gehörten. Hinzu kommt, dass weitere mit dem Internet verbundene Systeme infiziert werden können, um diese für *Spam*-Dienstleistungen zu missbrauchen. Beispielsweise können *IoT*-Geräte und Geräte zur privaten Heimautomatisierung als Teile eines *Botnet*zes zusammengeschaltet und missbraucht werden.

Spam lässt sich in unterschiedliche Kategorien aufteilen. Dabei wird unterschieden zwischen unerwünschtem, aber im Grunde unschädlichem Werbe-*Spam* (28 %) und schädlichen Cyberangriffen, darunter Erpressungs- (34 %) und Betrugsmails (32 %). Wesentliches Unterscheidungsmerkmal ist, dass im Rahmen erpresserischer Nachrichten gedroht wird, vermeintliches oder tatsächliches Wissen über das Opfer weiterzugeben, und auf diesem Weg ein Schweigegeld gefordert wird. Das geschieht meistens unabhängig davon, ob ein echtes Erpressungspotenzial in Form von Informationen vorliegt. Demgegenüber wird beim Betrug ein Handlungsbedarf im Namen einer Institution oder Person vorgetäuscht, ohne dabei ein Schweigegeld zu erpressen. Ziel dabei ist es, sensible persönliche Daten abzufangen, um diese weiterzuverkaufen oder für eigene kriminelle Tätigkeiten zu verwenden.

Im Bereich der E-Mails mit betrügerischem Hintergrund nehmen *Phishing*-Mails den größten Anteil ein (84 %).

Spam im Berichtszeitraum nach Art des _Spam_
Anteile in %

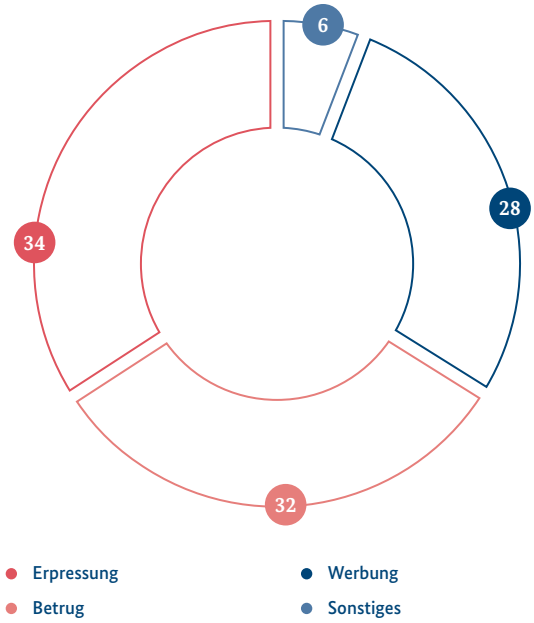


Abbildung 8: *Spam* im Berichtszeitraum nach Art des *Spam*
Quelle: E-Mail-Verkehrsstatistik des BSI

Diese Nachrichten zielen darauf ab, das Opfer mittels Social-Engineering-Techniken dazu zu bringen, seine Identitäts- beziehungsweise Authentisierungsdaten offenzulegen.

Weitere Angriffsvariationen lassen sich anhand des für den Angriff gewählten Kanals unterscheiden. Hier sind insbesondere Smishing (*Phishing* per SMS) und Vishing (Voice *Phishing*) hervorzuheben. Smishing zeigt sich in dem Versand von zahllosen SMS oder Kurznachrichten per Messenger an eine Vielzahl von Rufnummern, beispielsweise mit angeblichen Lieferbenachrichtigungen oder Anleitungen zum Download einer Sprachnachricht. Bei diesem Verfahren ist das Ziel meist, die Empfängerin oder den Empfänger zum Klicken auf einen Link zu verleiten, hinter dem sich schädliche Apps oder *maliziöse* Webseiten befinden. Dagegen wird beim Vishing die Zielperson telefonisch kontaktiert und mithilfe eines Gesprächsskriptes dazu verleitet, Informationen preiszugeben oder eine Zahlung zu tätigen. Weitverbreitete und noch immer aktuelle Inhalte der Telefonate sind gefälschte Anrufe von angeblichen IT-Supports oder Behörden, bei denen den Opfern suggeriert wird, sie müssten eine Zahlung durchführen oder persönliche Daten zur Überprüfung freigeben.

Schwerpunkt- und Beobachtungsthemen im Bereich _Phishing_ und _Spam_

Wie an den geschilderten *Phishing*-Techniken deutlich wird, nutzen Kriminelle meist bestimmte Themen aus, mit denen sie ihre Opfer erreichen wollen. Den meisten Betrugsversuchen lässt sich eine monetäre Motivation zuschreiben. Das führt dazu, dass vor allem im Bereich Finance-*Phishing* der größte Anteil an versendeten *Spam*-Nachrichten zu finden ist. Hierbei werden *Phishing*-E-Mails verschickt, die mit entsprechendem Corporate Design vorgeben, von bekannten Banken oder Finanzdienstleistern zu stammen. Ziel ist es, bei Verbraucherinnen und Verbrauchern einen vermeintlichen Handlungsbedarf zu suggerieren. Angeblich drohende Kontensperrung, notwendige Verifikation des Onlinebankings oder ausstehende Zahlungen sind dabei nur einige wenige Beispiele, mit denen Betroffene dazu gebracht werden sollen, ihre Zahlungs- und Accountdaten preiszugeben. Ergänzend dazu beobachtet das BSI *Phishing*-Kampagnen rund um die Themen Krypto-Wallets und FinTechs.

Gesellschaftliche Krisensituationen und Großereignisse im Berichtszeitraum boten den Kriminellen weitere Möglichkeiten für *Phishing* und Scam. Die angespannte Situation auf dem Energiemarkt im Winter 2022/23 sowie die von der Regierung beschlossenen Entlastungspakete führten zu *Phishing*-Nachrichten mit Betreffzeilen wie „Energiepauschale jetzt sichern!“ und „Wir überweisen Ihre Energiepauschale“. Angreifer gaben sich hier als Energieanbieter oder Teil der Regierung selbst aus und wollten die finanzielle Notsituation von Verbraucherinnen und Verbrauchern ausnutzen. Daneben trat vermehrt Charity-Scam im Namen von Hilfsorganisationen auf, die zum Beispiel Hilfeleistungen im Kontext des Kriegs in der Ukraine sowie des Erdbebens in der Türkei und Syrien versprachen. Hier sollte bei Verbraucherinnen und Verbrauchern das Gefühl einer emotionalen Betroffenheit geweckt werden, um im Rahmen von gefälschten Spendenaufrufen über Social Media oder E-Mail Geld einzutreiben.

Die Nutzung von großen KI-Sprachmodellen zur Verbesserung der Qualität von *Phishing*- und Scam-Angriffen ist eine weitere und zunehmende Herausforderung (vgl. Kapitel *Große KI-Sprachmodelle*, Seite 40). Durch den technologischen Fortschritt und die zunehmende Verfügbarkeit von KI-Systemen besteht die Gefahr, dass diese missbraucht werden. Dies führt zum Beispiel dazu, dass *Phishing*-Nachrichten authentischer gestaltet werden. Außerdem wird Sprache besser imitiert und klingt menschlicher. Auch der Einsatz von Chatbots, die

Gesprächsabläufe authentischer imitieren können, verleitet zur Preisgabe von Informationen und Daten.

4.5 — Angriffe im Kontext Kryptografie

Kryptografische Mechanismen sind wichtige Bausteine für die Umsetzung von Sicherheitsfunktionen in IT-Produkten. Dem Stand der Technik entsprechende Kryptoalgorithmen liefern hierfür grundsätzlich ausgezeichnete Sicherheitsgarantien. Das BSI empfiehlt in der Technischen Richtlinie TR-02102 eine Reihe kryptografischer Verfahren und Protokolle, die aufgrund eingehender mathematischer Kryptoanalyse gemeinhin als sicher angesehen werden.

Die Technische Richtlinie TR-02102:[f]

Dagegen können folgende Aspekte dazu führen, dass das theoretische Sicherheitsniveau in der Praxis reduziert ist:

- Schwächen in kryptografischen Mechanismen oder Protokollen
- Implementierungsfehler
- unzureichend abgesicherte Seitenkanäle
- Schwächen in der Zufallszahlen- und Schlüsselerzeugung
- nicht ausreichend geschütztes Schlüsselmaterial

Die klassische Anwendung der Kryptografie ist der Schutz der Vertraulichkeit und Integrität von Daten, zum Beispiel wenn diese über offene Netzwerke wie das Internet übertragen werden. Dafür stehen verschiedene kryptografische Mechanismen und Protokolle zur Verfügung, für die gemeinhin angenommen wird, dass ein Angreifer mit Zugriff auf den Netzwerkverkehr weder die geheimen Schlüssel in Erfahrung bringen noch die ausgetauschten Daten entschlüsseln oder unbemerkt manipulieren kann. Um die Wirksamkeit kryptografischer Mechanismen und Protokolle zu gewährleisten, müssen zum einen geeignete Verfahren ausgewählt und korrekt implementiert werden. Zum anderen muss sichergestellt sein, dass das an der Netzwerkschnittstelle beobachtbare Verhalten (z. B. Antwortzeiten eines Servers) keine Informationen über verarbeitete Geheimnisse preisgibt.

Bei der Absicherung von Kryptosystemen, die selbst Angreifern in räumlicher Nähe standhalten sollen, müssen weitere Seitenkanäle (z. B. Stromverbrauch oder elektromagnetische Abstrahlung der Geräte) berücksichtigt werden, über die ebenfalls Geheimnisse abfließen können. Die Seitenkanalanalyse, also die Analyse auf Anfälligkeit für *Seitenkanalangriffe*, ist heute ein eigener Forschungszweig, der neben Gegenmaßnahmen auch neue *Angriffsvektoren* hervorgebracht hat. Der im Info-Kasten HERTZBLEED (Seite 33) beschriebene Angriff nutzt einen neuartigen Seitenkanal in modernen Prozessoren aus, bei dem Unterschiede im Stromverbrauch zu unterschiedlichen Laufzeiten führen. Dieser Angriff demonstriert, dass Seitenkanäle, die eigentlich einen physischen Zugriff voraussetzen, in manchen Situationen auch durch einen entfernten Angreifer ausgenutzt werden können.

Eine wesentliche Voraussetzung für den sicheren Einsatz von Kryptografie ist die Erzeugung von echten Zufallszahlen, die gewisse Gütekriterien erfüllen müssen. Zufallszahlen werden unter anderem für die Schlüsselerzeugung benötigt. Für kryptografische Anwendungen dürfen Zufallszahlen nicht vorhersagbar sein und keine ausnutzbaren statistischen Defekte aufweisen. Um Angriffen durch schwache Zufallszahlen vorzubeugen, definiert das BSI in den Anwendungshinweisen und Interpretationen zum Schema AIS 20 und AIS 31 Funktionalitätsklassen von Zufallszahlengeneratoren für verschiedene Einsatzzwecke. Ein neuer Entwurf der mathematisch-technischen Anlage der AIS 20/31 wurde im September 2022 veröffentlicht.

Die Sicherheitsgarantien vieler heute eingesetzter Kryptoalgorithmen gelten allerdings nicht mehr, sobald ein hinreichend leistungsstarker Quantencomputer zur Verfügung steht. Das Kapitel Quantentechnologien (Seite 74) zeigt Möglichkeiten auf, dieser Bedrohung zu begegnen, und stellt die Aktivitäten des BSI in diesem Bereich dar.

5. — Schwachstellen

Um Computersysteme infiltrieren zu können, benötigen Angreifer Schwachstellen in der IT-Infrastruktur, die für einen Angriff ausgenutzt werden können. Ein Schadprogramm, das eine Schwachstelle ausnutzt, um einen Cyberangriff durchzuführen, wird als *Exploit* bezeichnet. *Exploits* werden zum Beispiel von Cyberkriminellen für die Erstinfektion von Systemen und zur Vorbereitung eines *Ransomware*-Angriffs eingesetzt.

HERTZBLEED – Timing-Angriff auf SIKE durch Taktfrequenz-Seitenkanal in Prozessoren

Der Stromverbrauch eines Prozessors hängt im Allgemeinen von den Daten ab, die in den Registern des Prozessors verarbeitet werden. Durch Messungen des Stromverbrauchs können somit Rückschlüsse auf die verarbeiteten Daten gezogen und, im Falle kryptografischer Operationen, auch Erkenntnisse über verarbeitete Geheimnisse gewonnen werden. Um den Stromverbrauch und die Wärmeentwicklung zu reduzieren, passen einige Prozessoren ihre Taktfrequenz dynamisch an. Eine solche Anpassung der Taktfrequenz beeinflusst wiederum die Laufzeit der vom Prozessor durchgeführten Berechnungen. Die Laufzeit einer Berechnung kann dadurch auch von den verarbeiteten Daten abhängen. Dieser neuartige Timing-Seitenkanal wurde im sogenannten HERTZBLEED-Angriff ausgenutzt, der im Juni 2022 veröffentlicht wurde.

In der Publikation von HERTZBLEED[2] wurde die Abhängigkeit der Taktrate von den verarbeiteten Daten beschrieben, systematisch untersucht und experimentell verifiziert. Im Weiteren haben die Forschenden demonstriert, dass ein entfernter Angreifer durch Ausnutzung solcher Timing-Informationen den geheimen Schlüssel des Schlüsselaustauschverfahrens SIKE (Supersingular Isogeny Key Encapsulation) vollständig bestimmen kann. Wohlbemerkt waren die angegriffenen SIKE-Implementierungen dabei gegen bislang bekannte Timing-Angriffe gehärtet.

SIKE galt im Standardisierungsprozess für Post-Quanten-Verfahren des National Institute of Standards and Technology (NIST) lange Zeit als aussichtsreicher Kandidat. Durch einen im Juli 2022 veröffentlichten Angriff von Castryck und Decru[3] wurde SIKE aber letztendlich vollständig kryptoanalytisch gebrochen. Das Kapitel Quantentechnologien (Seite 74) enthält nähere Informationen zur Post-Quanten-Kryptografie und zum NIST-Auswahlprozess.

5.1 — Schwachstellen in Softwareprodukten

Schwachstellen entstehen beispielsweise durch Fehler in der Programmierung, durch schwache Default-Einstellungen von IT-Produkten im Produktivbetrieb oder auch durch fehlkonfigurierte Sicherheitseinstellungen. IT-Systeme werden immer komplexer und die Produktionsbedingungen immer arbeitsteiliger und modularer, sodass Schwachstellen sehr verbreitet sind. Sie können daher auch sowohl in Betriebssystemen und Anwendungen (vgl. Kapitel *Schwachstellen in Softwareprodukten*, Seite 33) als auch in Hardware (vgl. Kapitel *Schwachstellen in Hardwareprodukten*, Seite 39) auftreten. Mit der Ausweitung des *Internet of Things* treten zunehmend auch Schwachstellen in vernetzten Geräten auf (vgl. Kapitel *Schwachstellen in vernetzten Geräten*, Seite 39).

Wenn eine Schwachstelle in einem IT-Produkt entdeckt wird, stellen Hersteller in der Regel Sicherheitsupdates (sog. *Patches*) bereit, um die Schwachstelle zu schließen und deren Ausnutzung für Cyberangriffe zu verhindern. Ein strukturiertes *Patchmanagement* ist daher eine der wichtigsten Präventivmaßnahmen, um den Risiken der Digitalisierung erfolgreich zu begegnen.

Schwachstellen in Softwareprodukten dienen oftmals als erstes Einfallstor zur Kompromittierung von Systemen und ganzen Netzwerken – schließlich sind sie häufig über das Internet ausnutzbar und erlauben den Angreifenden somit maximale Anonymität und Flexibilität aus der Ferne.

Im Berichtszeitraum wurden durchschnittlich täglich 68 neue Schwachstellen bekannt, rund 24 Prozent mehr als im vergangenen Berichtszeitraum. Es wurden also insgesamt knapp 27.000 neue Schwachstellen in jeglicher Art von Softwareprodukten bekannt, von spezialisierten Fachanwendungen über komplexe Serverinfrastrukturen bis hin zu Handy-Apps. Wie schon in den vergangenen Jahren wirkte sich auch im aktuellen Berichtszeitraum die zunehmende Modularisierung und Arbeitsteilung bei der Softwareproduktion auf die Bedrohungslage aus. Denn wenn eine Schwachstelle in einer Softwarekomponente bekannt

wird, die in einer Vielzahl verschiedener Anwendungen eingesetzt wird, kann solch eine einzelne Schwachstelle für Cyberangriffe gegen alle diese Anwendungen ausgenutzt werden.

Die im Berichtszeitraum bekannt gewordenen Schwachstellen unterschieden sich hinsichtlich ihrer Kritikalität sowie hinsichtlich der Schäden, die Angreifer durch Ausnutzung der Schwachstellen bewirken können. Für die Quantifizierung der Schadwirkungen wird im Folgenden die Common Weakness Enumeration (CWE-Klassifikation) herangezogen, eine von der IT-Sicherheitscommunity gepflegte Auflistung verschiedener Typen von Schwachstellen in Hard- und Software. Die Kritikalität wird anhand des Common Vulnerability Scoring System (*CVSS-Score*) gemessen.

Schadwirkung: Die Ausführung von unautorisierten Programmcodes oder Befehlen ist eine der wichtigsten Schadwirkungen. Rund 47 Prozent der im Berichtszeitraum bekannt gewordenen Schwachstellen eigneten sich dafür. Sie ermöglichten beispielsweise die initiale Erstinfektion bei einem *Ransomware*-Angriff (vgl. Kapitel *Angreifermotivation und Angriffsablauf*, Seite 15). Viele Schwachstellen ermöglichten Angreifern auch, Sicherheitsvorkehrungen zu umgehen (40 %). Mit jeweils 20 Prozent der Schwachstellen konnten Angreifer Speicher sowie Anwendungsdaten manipulieren, um zum Beispiel die erlangten Zugriffsrechte zu erweitern. Und rund 40 Prozent ermöglichten schließlich das Auslesen von Daten. Solche Daten können Angreifer einerseits für Cybererpressungen nutzen (vgl. Kapitel *Schweigegeld-Erpressung mit Datenleaks und weitere Erpressungsmethoden*, Seite 19), andererseits auch an andere Angreifer weiterverkaufen, die diese Daten dann ihrerseits für Cyberangriffe verwenden können. Darüber hinaus konnte jede dritte im Berichtszeitraum bekannt gewordene Schwachstelle für einen *DoS*-Angriff genutzt werden.

Kritikalität: Die Kritikalität einer Schwachstelle ergibt sich jedoch nicht nur aus den möglichen Schadwirkungen, die Angreifer damit erzielen können. In den *CVSS-Score*, einen international anerkannten Industriestandard, mit dem die Kritikalität von Schwachstellen international vergleichbar bewertet wird, fließen auch *Angriffsvektoren* und andere Faktoren ein. Die Kritikalität der bekannt gewordenen Schwachstellen schwankte stark. Gut drei Prozent wiesen niedrige und 45 Prozent mittlere Scoring-Werte auf der zehnstufigen Skala auf (vgl. Abbildung 10). Mit 53 Prozent mehr als die Hälfte wiesen hohe (7–9) oder kritische (9–10) *CVSS-Score*s auf. Der Anteil kritischer Schwachstellen lag bei rund 15 Prozent. Wie im vorigen Berichtszeitraum waren die häufigsten *Angriffsvektoren* Cross-Site Scripting (13 %), Out-of-Bounds Write (8 %) und SQL-Injection (7 %).

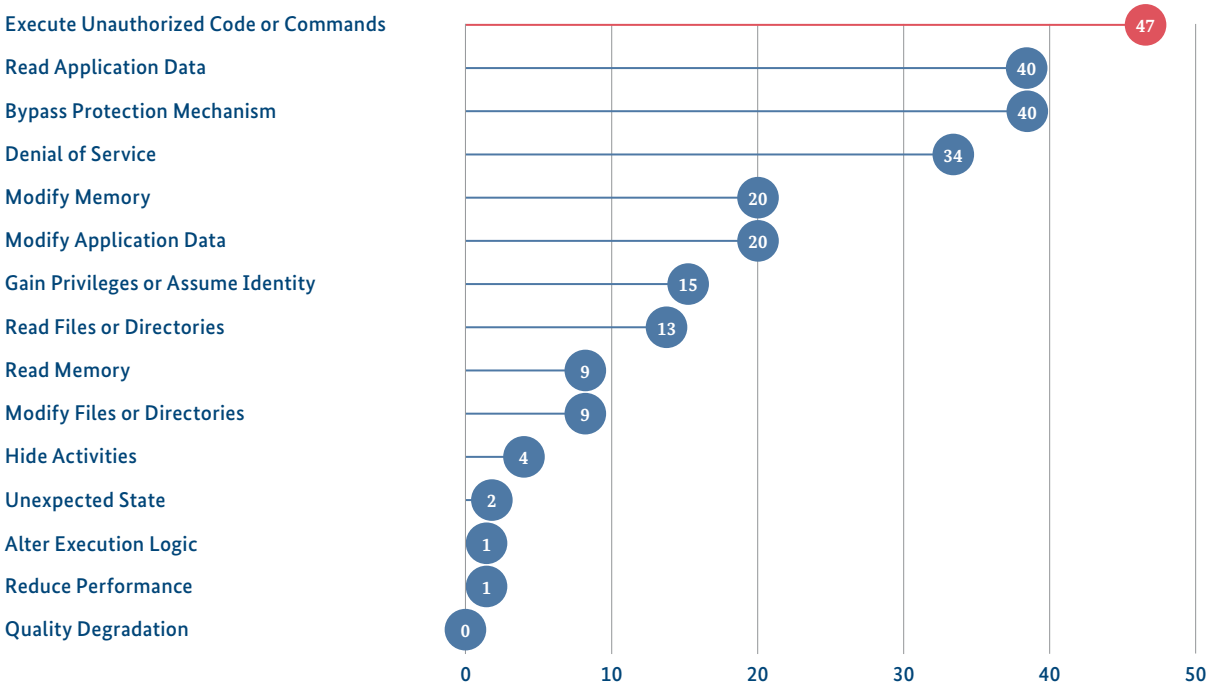
Nicht jede Schwachstelle ist für Angriffe einfach ausnutzbar. Eine Schwachstelle in einer lokalen Anwendung ohne Verbindung zum Internet kann beispielsweise lediglich durch einen lokalen Angreifer ausgenutzt werden. Dagegen können beispielsweise Schwachstellen in Softwareprodukten, die direkt aus dem Internet erreichbar sind, leichter und von einer höheren Anzahl von Cyberkriminellen für Angriffe missbraucht werden. Von den 13.500 Schwachstellen mit hohem oder kritischem *CVSS-Score* im Berichtszeitraum war knapp die Hälfte (49 %) leicht für Cyberangriffe ausnutzbar. Im Cyberraum findet ein ständiger Wettlauf zwischen Sicherheitsforschenden und den verschiedenen Angreifergruppierungen statt: Wer Schwachstellen zuerst entdeckt, kann diese entweder für Cyberangriffe nutzen oder im Darknet anderen Angreifern zum Kauf anbieten oder sie dem Hersteller melden, um die Bereitstellung eines *Patch*es voranzutreiben.

Im Berichtszeitraum hat das BSI monatlich durchschnittlich rund 20 Meldungen von Sicherheitsforschenden über schwachstellenbehaftete Softwareprodukte erhalten und nach dem System des Open Web Application Security Project (OWASP) klassifiziert. Während CWE und CVSS die Schwachstellen selber beschreiben, erlaubt OWASP eine Beschreibung des schwachstellenbehafteten Produkts. Demnach wiesen mit rund 21 Prozent der Meldungen die meisten gemeldeten Produkte im Berichtszeitraum Fehlkonfigurationen auf (Security Misconfiguration, vgl. Abbildung 36). Dazu zählen zum Beispiel eine fehlende Sicherheitshärtung des Produkts, unnötige Features wie etwa offene Ports, Zugriffsrechte oder Services oder auch unveränderte Default Accounts aus der Entwicklungsphase. In rund
18 Prozent der gemeldeten Fälle ermöglichte das schwachstellenbehaftete Produkt Angreifern das Einschleusen von Schadcode (Injection), weil Benutzereingaben von der Software nicht validiert, gefiltert oder bereinigt wurden. An dritter Stelle folgten im Ranking mit 13 Prozent Softwareprodukte ohne funktionierende Zugangskontrollen (Broken Access Control). Sie verletzten das Prinzip der standardmäßigen Verweigerung des Zugangs und erlaubten ohne weitere Zugangskontrolle jeglichem Nutzer den Zugriff, ermöglichten die Umgehung von Zugriffskontrollen oder gewährten authentifizierten Benutzern die Verwendung der Software mit Administratorrechten. Rund 13 Prozent

Bekannt gewordene Schwachstellen nach möglicher Schadwirkung (Top 10)*
Anteile in %

Abbildung 9: Bekannt gewordene Schwachstellen nach Schadwirkung
Quelle: Schwachstellenstatistik des BSI

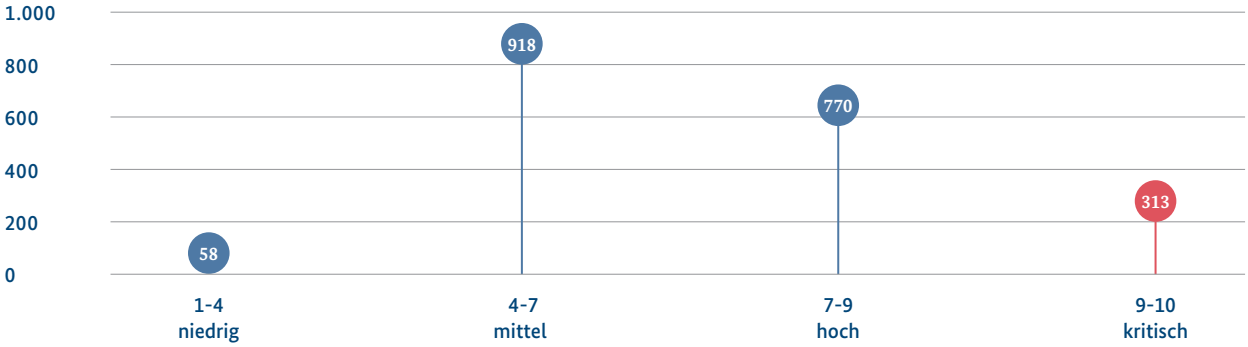
* Mehrfachnennungen möglich



Durchschnittlich monatlich bekannt gewordene Schwachstellen nach dem *CVSS-Score** für Kritikalität

Abbildung 10: Durchschnittlich monatlich bekannt gewordene Schwachstellen nach dem *CVSS-Score* für Kritikalität
Quelle: Schwachstellen-Statistik des BSI

* Risikobewertung nach CVSS-Version 3.1



der gemeldeten Produkte verletzten Security-by-Design-Prinzipien (Insecure Design). Jedes zehnte gemeldete Produkt wies verwundbare oder veraltete Komponenten auf und bei sechs Prozent der gemeldeten Produkte versagten kryptografische Schutzmechanismen (Cryptographic Failures). Weitere Produkte wiesen Schwachstellen bei der Sicherheitsüberwachung auf oder erlaubten die Manipulation von Daten. Mit einem Anteil von sechs Prozent wurden Produkte mit Schwachstellen in den Identifikations- und *Authentifizierungs*systemen noch vergleichsweise selten gemeldet. In diese Kategorie fallen auch Multifaktor-*Authentifizierung*en. Inzwischen sind allerdings Schadprogramme bekannt, die diese Form der Benutzer-*Authentifizierung* umgehen können

(vgl. Vorfall *Identitätsdiebstahl mit Phishing-as-a-Service (PhaaS)*, Seite 54). Es ist daher zu erwarten, dass sich künftig mehr Produkte in dieser Kategorie als schwachstellenbehaftet erweisen werden.

Neben den genannten Schwachstellen in Softwareprodukten erreichten das BSI auch Meldungen über Schwachstellen in Industrial Control Systems (ICS). Industrial Control Systems sind Systeme zur Steuerung industrieller Produktion, zur Automatisierungskontrolle, zur Mensch-Maschine-Interaktion und zu anderem mehr. Im Berichtszeitraum wurden dem BSI insgesamt 24 schwachstellenbehaftete ICS-Systeme gemeldet.

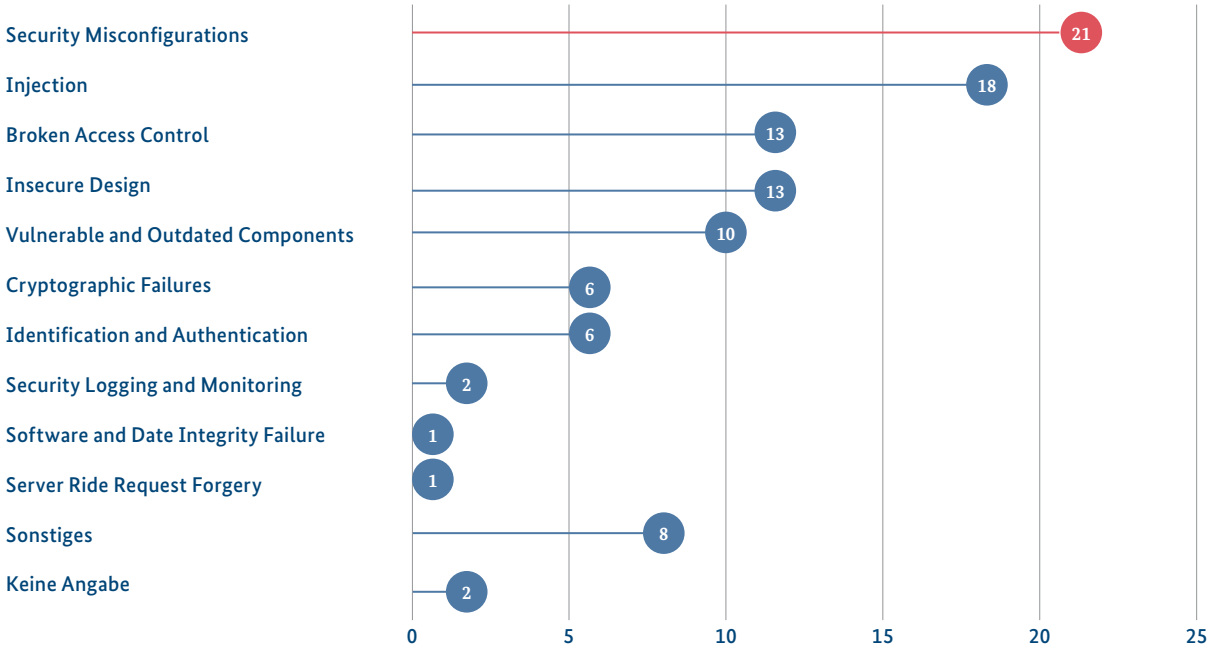
Im Warn- und Informationsdienst (WID) des BSI werden täglich die verschiedenen Quellen zu neuen Schwachstellen in Softwareprodukten gesichtet und die identifizierten Sachverhalte über das Portal des WID veröffentlicht. Zu unterscheiden ist dabei zwischen *Advisories* (umfangreiche Schwachstellen-Informationen, die exklusiv der Bundesverwaltung zur Verfügung gestellt werden) und Kurzinformationen, die Sachverhalte für Organisationen aus anderen Sektoren in gekürzter Form zusammenfassen. Beide Formate können in Behörden, Unternehmen und anderen Institutionen als Grundlage für das *Patchmanagement* genutzt werden, um das Ausrollen von Sicherheitsupdates voranzutreiben. Technische Warnungen für Verbraucherinnen und Verbraucher ergänzen das Angebot.

Im aktuellen Berichtszeitraum wurde das Webangebot erheblich ausgebaut. Auch ist das Portfolio der beobachteten Softwareprodukte deutlich angewachsen, sodass die Zahlen des aktuellen Berichtszeitraums nicht mit früheren Berichtszeiträumen vergleichbar sind.

Die Flut an neu bekannt gewordenen Schwachstellen ist eine tägliche Herausforderung für IT-Sicherheitsverantwortliche. Perspektivisch sieht das BSI durch (Teil-)Automatisierung das Potenzial, Prozesse im *Patchmanagement* weiter zu beschleunigen. Unter anderem ist es denkbar, die Masse der Schwachstellenmeldungen dadurch zu bewältigen, dass alle Meldungen automatisiert nach denjenigen gefiltert werden, die für die eigene Organisation von besonderem Interesse sind. Die technische Grundlage hierfür stellt das Common *Security Advisory* Format (CSAF) dar, an dessen Spezifizierung das BSI beteiligt war. Dieser neue Standard macht *Advisories* maschinenlesbar und somit automatisiert verarbeitbar.

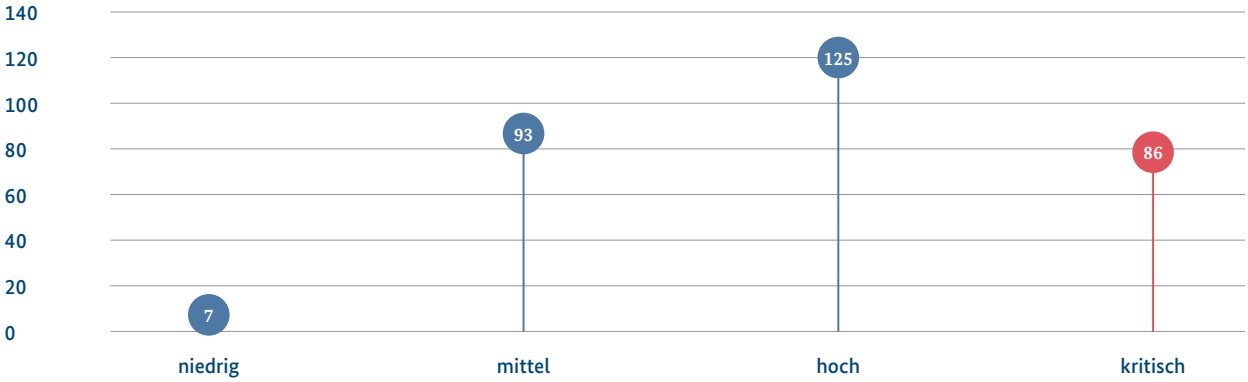
Meldungen über schwachstellenbehaftete Produkte
Anteile in %

Abbildung 11: Meldungen über schwachstellenbehaftete Produkte
Quelle: BSI



Durchschnittliche monatliche WID-Meldungen nach Kritikalität, einschließlich Updates
Anzahl

Abbildung 12: Durchschnittliche monatliche WID-Meldungen nach Kritikalität
Quelle: BSI



Angriffskampagne gegen Schwachstelle in Filesharing-Software GoAnywhere

Sachverhalt
Am 30. Januar 2023 wurde die Zero-Day-Schwachstelle CVE-2023-0669 in dem Produkt GoAnywhere Managed File Transfer (MFT) bekannt. Die Software GoAnywhere MFT wird zum Betrieb eines Filesharing-Servers verwendet und ist daher in der Regel aus dem Internet heraus erreichbar. Die Ausnutzung der Schwachstelle ermöglicht Zugang durch Fernzugriff (Remote Access) und damit die Ausführung von beispielsweise Malware durch einen Angreifer. Am 6. Februar 2023 berichtete ein Sicherheitsforscher öffentlich über die Schwachstelle und veröffentlichte Proof-of-Concept-(PoC-)Code, der die Ausnutzung der Schwachstelle ermöglichte. Kurz nach dieser Veröffentlichung wurde das Framework für Penetrationstesting Metasploit um ein entsprechendes Modul erweitert, womit jeder Angreifer zur Ausnutzung befähigt war. Am 7. Februar 2023 stellte der Hersteller einen Notfallpatch zum Schließen der Schwachstelle zur Verfügung. Seit dem 8. Februar 2023 wurden Ausnutzungsversuche der Schwachstelle beobachtet.

Anfang März 2023 veröffentlichten Angreifer der Ransomware Clop auf ihrer Leak-Seite die Namen mehrerer mutmaßlicher Opfer. Die Angreifer behaupten, 130 Organisationen durch diese Schwachstelle kompromittiert und Daten gestohlen zu haben. Diese mutmaßlichen Opfer wurden anschließend durch die Angreifer um ein Schweigegeld erpresst.

Bewertung
Nach Kenntnislage des BSI setzten die Angreifer in dieser Angriffskampagne keine Ransomware ein. Sie beschränkten sich mutmaßlich auf den Diebstahl von Daten auf den kompromittierten GoAnywhere-Servern. Die Zielauswahl erfolgte wahrscheinlich opportun gegen verwundbare Server.

Dieser Vorfall ähnelt einer Angriffskampagne von Ende Dezember 2020. Dabei nutzte dieselbe cyberkriminelle Gruppe eine Schwachstelle in einer anderen Filesharing-Software aus. Auch in dieser Kampagne setzten die Angreifer keine Ransomware ein, sondern erpressten nur mit gestohlenen Daten.

Reaktion
Um Kompromittierungen wie in diesem Fall zu verhindern, sind aktives Patchmanagement und die Umsetzung präventiver Maßnahmen notwendig. Zudem sollte geprüft werden, ob verwundbare Server bis zur Bereitstellung eines Patches vom Netz genommen werden können.

Angriffskampagne gegen Filesharing-Software MOVEit

Sachverhalt

Am 31. Mai 2023 veröffentlichte der Softwarehersteller Progress Informationen über eine Schwachstelle in seinem Filesharing-Produkt MOVEit und eine aktive Angriffskampagne dagegen. MOVEit-Server werden häufig zum Hochladen von Daten durch externe Nutzer eingesetzt. Angreifer nutzten die Schwachstelle CVE-2023-34362 mindestens seit dem 27. Mai 2023 in einer mehrtägigen Angriffskampagne aus. Ziel der Angreifer war der Diebstahl von Daten vom Filesharing-Server. Der Angriff wurde von mehreren IT-Sicherheitsdienstleistern der Angreifergruppe hinter der Ransomware Clop zugeordnet.

Am 5. Juni 2023 übernahm die Angreifergruppe hinter Clop gegenüber der Nachrichtenwebseite Bleeping Computer die Verantwortung für die Angriffe. Die Angreifer platzierten eine Webshell, welche zum Diebstahl der Daten diente. Diese Webshell wurde von dem IT-Sicherheitsdienstleister Mandiant als Lemurloot bezeichnet.

Seit dem 14. Juni 2023 veröffentlichten die Angreifer auf der Leak-Seite der Ransomware Clop Daten mehrerer Unternehmen. Diese Veröffentlichungen gehen wahrscheinlich auf diese Angriffskampagne zurück. Allerdings können sich auch Opfer darunter befinden, die nicht im Zusammenhang mit der Angriffskampagne gegen MOVEit stehen. Es ist unbekannt, wie viele Organisationen durch diese Angriffskampagne tatsächlich betroffen sind. Aufgrund der Verbreitung von MOVEit waren wahrscheinlich Hunderte Organisationen verwundbar.

Bewertung

Das BSI hat keine Hinweise auf den Einsatz von Ransomware in dieser Angriffskampagne. Verwundbare MOVEit-Server wurden opportun mit dem Ziel des Datendiebstahls angegriffen. Dieser Vorfall ähnelt zwei anderen Angriffskampagnen derselben Gruppe gegen verwundbare Filesharing-Server: auf den GoAnywhere-Server im Januar 2023 (vgl. Vorfall Angriffskampagne gegen Schwachstelle in Filesharing-Software GoAnywhere, Seite 37) und auf die Filesharing-Software des Herstellers Accellion im Dezember 2020.

Diese Angreifergruppe erpresst Opfer in der Regel mit Double Extortion, also der Verschlüsselung mit Ransomware und der Veröffentlichung gestohlener Daten. Die wiederholten Angriffskampagnen gegen Filesharing-Server zeichneten sich jedoch durch den Verzicht auf den Einsatz von Ransomware aus. Es ist auch nicht bekannt, dass die Angreifer den für den Diebstahl etablierten Zugang für einen späteren Ransomware-Angriff wiederverwendeten. Die Angreifer zielten in diesen Kampagnen darauf ab, möglichst viele Server in kurzer Zeit zu kompromittieren und Daten auszuleiten. Denn sobald die Angriffskampagne bekannt wird, können die verwundbaren Server bis zur Bereitstellung eines Patches vom Internet getrennt werden. Es ist daher davon auszugehen, dass die Angreifer gezielt auf ein hohes Angriffstempo bei der Ausnutzung der Schwachstelle setzten.

Abhängig vom Verwendungszweck des MOVEit-Servers können für die betroffene Organisation sensible Informationen gestohlen worden sein.

Reaktion

Das BSI veröffentlichte in Reaktion auf die Angriffskampagne am 1. Juni 2023 eine BSI-IT-Sicherheitswarnung. Die IT-Bedrohungslage wurde zuerst mit 4 / Rot bewertet, da unmittelbarer Handlungsbedarf bestand. Am 2. Juni 2023 wurde die Sicherheitswarnung auf 3 / Orange heruntergestuft, nachdem der Softwarehersteller ein Patch zur Verfügung gestellt hatte.

5.2 — Schwachstellen in Hardwareprodukten

Hardware-Schwachstellen können normalerweise nicht durch Softwarepatches behoben werden, da ihre Ursache in der Herstellungsweise und der Architektur der Produkte begründet ist. Es gibt verschiedene Angriffsmöglichkeiten. Zum einen sind die Funktionsweisen der Transistoren das Ziel, die in integrierten Schaltungen verbaut werden, und somit auch die Mikroarchitektur von Prozessoren. Zum anderen geben im Lebenszyklus eines IT-Produktes auch verschiedene Schritte in der Lieferkette und der Produktion Angriffsmöglichkeiten. Da die Schwachstellen in bereits verbauter Hardware normalerweise nicht einfach behoben werden können, ist der mögliche Nutzen für einen potenziellen Angreifer sehr hoch. Allerdings sind die finanziellen Aufwendungen zur Ausnutzung im Gegensatz zu Schwachstellen in Software ebenfalls höher.

Seitdem 2017 die Angriffe MELTDOWN und SPECTRE bekannt geworden sind, gibt es immer weitere Versionen dieser Angriffe, die sich die spekulativen Ausführungen in modernen Prozessoren zunutze machen. Daher ist weiterhin mit neuen Schwachstellen dieser Angriffsklasse zu rechnen, solange die Mikroarchitektur der Prozessoren nicht grundlegend verändert wird. Jedoch ist die spekulative Ausführung zu einem substanziellen Teil für die Performance der Prozessoren verantwortlich. Eine andere Ausführung würde zu einer erheblichen Verringerung der Rechenleistung führen. Wie auch in den vorangegangenen Jahren dominieren immer noch die aus diesen Angriffen weiterentwickelten Variationen. Im Jahr 2022 wurden etwa die Angriffe Retbleed, SPECTRE-BHB, SQUIP und PACMAN veröffentlicht. Gegen diese Schwachstellen existieren entweder keine Gegenmaßnahmen-, oder diese führen zu großen Leistungsminderungen.

Im Gegensatz zu auf SPECTRE basierenden Angriffen handelt es sich bei der Schwachstelle ÆPIC-Leak um einen echten Fehler in der Mikroarchitektur des Prozessors, bei dem geheime Schlüsseldaten ausgelesen werden können, jedoch nur von Usern mit Administratorrechten.

Neue Kryptoalgorithmen sollten quantensicher sein (Post-Quantum Cryptography, PQC). PQC-Verfahren müssen nicht nur Quantencomputern standhalten, sondern auch hardwarenahen Seitenkanal- und Fehlerangriffen, da sie auf klassischen Plattformen implementiert werden. So wurde zum Beispiel gezeigt, dass Schlüsselmaterial bei einer Hardware-Implementierung des PQC-Kryptoverfahrens CRYSTALS-Kyber mittels Seitenkanalanalyse in Kombination mit neuronalen Netzen ausgelesen werden kann (vgl. auch Kapitel *Post-Quanten-Kryptografie*, Seite 74). Für die zukünftige Verwendung von Hardware-Implementierungen müssen geeignete Gegenmaßnahmen entwickelt werden, damit PQC-Verfahren in Hardwareprodukten sicher implementiert werden können.

Im März 2023 wurden kritische Zero-Day-Schwachstellen in Exynos-Modemchips veröffentlicht, die nicht nur in Smartphones, sondern auch in Fahrzeugen verbaut sind. Diese Schwachstellen ermöglichen es Angreifern, Programme auf den mobilen Geräten auszuführen, ohne dass der Eigentümer davon etwas merkt oder etwas dagegen unternehmen kann. Für einen erfolgreichen Angriff reicht lediglich die Kenntnis der Telefonnummer. Nach derzeitigem Kenntnisstand gibt es jedoch keine breite Ausnutzung dieser Schwachstelle im Feld.

Da die Ausnutzung von Hardware-Schwachstellen im Vergleich zu den zahlreichen Software-Schwachstellen relativ aufwendig ist, ist Hardware seltener Ziel von Cyberangriffen. Wie in mehreren Studien gezeigt wurde, kann die Verwendung von dedizierten Sicherheitselementen oder vollständig logisch separierten Prozessoreinheiten zur Speicherung und Verarbeitung sensibler Daten das Angriffspotenzial stark senken. Ein Kennzeichen für eine gute Sicherheitsfunktionalität in IT-Produkten bietet dabei eine unabhängige Sicherheitsüberprüfung und Zertifizierung, zum Beispiel nach dem ISO-Standard 15408: Common Criteria for IT Security Evaluation.

5.3 — Schwachstellen in vernetzten Geräten

Neben Software und Hardware können auch Geräte und Komponenten des *Internet of Things* Schwachstellen aufweisen. Mit dem Grad der Vernetzung und der Komplexität der Produkte nimmt die digitale Angriffsfläche im *IoT*-Bereich stetig zu. Jede zusätzliche Schnittstelle und jeder zusätzliche Controller bietet potenzielle *Angriffsvektoren*. Insbesondere in modernen Fahrzeugen ist eine Vielzahl von Steuergeräten verbaut, die untereinander vernetzt sind. Zudem steigt der ohnehin große Softwareumfang durch die zusätzlichen Funktionalitäten weiter an, was typischerweise auch eine höhere Anzahl an

Schwachstellen nach sich zieht. Im Fall einer App- oder *Cloud*-Anbindung und einer gezielten Manipulation ist es für einen Angreifer daher prinzipiell möglich, aus der Ferne essenzielle Funktionen zu stören oder zu deaktivieren.

Die große Angriffsfläche, die das *IoT* bietet, erfordert einen aktiven Schutz, insbesondere durch Maßnahmen der Hersteller wie Sicherheitskonzepte und Penetrationstests. Die Schwachstellen, die die *Angriffsvektoren* ermöglichen, sind vielfältig: Zunächst sind viele ursprünglich konventionelle Produkte auf dem Markt, die seit Generationen existieren und mit der Zeit immer weiter digitalisiert und vernetzt wurden. In diesem Rahmen wurden zusätzliche Schnittstellen implementiert. Das ursprüngliche Produkt erforderte mangels Vernetzung keine Cybersicherheitsmaßnahmen. Inzwischen ist jedoch in den meisten Fällen ein grundlegendes Sicherheitskonzept zum wirkungsvollen Schutz erforderlich, das bereits beim Design des Produktes berücksichtigt werden muss (Security by design). Beispielsweise sind viele Komponenten nicht auf einen Schutz durch eine Transportverschlüsselung ausgelegt und enthalten keine Firewalls, die vor unberechtigtem Zugriff schützen. Häufig ist es durch Hardwarebeschränkungen und Abwärtskompatibilität nicht möglich, solche Maßnahmen im Nachhinein wirkungsvoll zu implementieren.

Eine weitere Ursache ist die fehlende Erfahrung von Herstellern im Umgang mit Cybersicherheit und potenziellen Schwachstellen. Da bei konventionellen, nicht vernetzten Produkten keine IT-Sicherheitsmaßnahmen notwendig waren, gibt es bei vielen Herstellern bisher weder Strukturen noch Fachwissen, um digitalen Angriffen auf ihre Produkte entgegenzuwirken. Durch das gestiegene Bewusstsein für Cybersicherheitsfragen und besonders durch neue regulatorische Rahmenbedingungen wie etwa Typgenehmigungsvorschriften zur Cybersicherheit in Fahrzeugen hat sich die Situation hier in jüngster Zeit geändert. Automobilhersteller beispielsweise sind verpflichtet, geeignete Prozesse zum Management der Cybersicherheit in der Produktion und zur Behebung von Schwachstellen zu etablieren.

Schwachstellen im Bereich Automotive

Im Berichtszeitraum wurden neue Schwachstellen im Bereich Automotive bekannt. Der Sicherheitsforscher Sam Curry konnte zeigen[4], dass mangelhaft abgesicherte Webportale verschiedener Hersteller Angreifern neben Zugriffen auf Hersteller- und Kundendaten aus der Ferne auch Zugriff auf Fahrzeugfunktionen erlaubten. Das Manipulieren von Webanfragen ermöglichte Angreifern beispielsweise, sich im Webportal als Händler auszugeben. Händler genießen vonseiten der Hersteller ein besonderes Vertrauen und können Fahrzeuge bestimmten Kunden namentlich zuordnen. Entsprechend konnte ein Angreifer bereits vergebene Fahrzeuge einem eigenen Account zuordnen und Fahrzeugfunktionen fremder Autos über die offizielle App des Herstellers steuern. Auf diese Weise konnte ein betroffenes Fahrzeug aus der Ferne geöffnet oder dessen Motor gestartet werden. In einem weiteren Fall war es möglich, Live-Bilder der Heckkamera zu empfangen. Für eine Manipulation dieser Art war lediglich die Fahrzeugidentifikationsnummer (FIN) nötig, die in einigen Fällen auf der Windschutzscheibe des Fahrzeugs zu finden ist.

Im Falle eines großen nordamerikanischen Telematikbetreibers ermöglichten Schwachstellen die Ausführung von Fahrzeugfunktionen ganzer Flotten. Unter den über 15 Millionen betroffenen Fahrzeugen befanden sich auch Ambulanz- und Polizeifahrzeuge, deren Einsatz durch ein Ausnutzen dieser Schwachstellen behindert worden wäre.

Diese Vorfälle zeigen, dass nicht nur das Fahrzeug an sich und dessen interne Systeme betrachtet werden müssen. Darüber hinaus muss auch das ganze Ökosystem, in dem sich das Fahrzeug bewegt, einschließlich der Vertrauensbeziehungen zwischen verschiedenen Marktakteuren abgesichert werden.

Weitere Informationen zum Bereich Automotive finden Sie im Lagebild Automotive:[5]

6. — Große KI-Sprachmodelle

Die technische Entwicklung großer KI-Sprachmodelle (Large Language Models, LLMs) hat im aktuellen Berichtszeitraum einen Schlüsselmoment erfahren. Mit der Veröffentlichung des Chatbots ChatGPT des von Microsoft unterstützten Unternehmens OpenAI im November 2022 wurde erstmals eine Anwendung basierend auf einem großen KI-Sprachmodell einer breiten Öffentlichkeit zugänglich. Die Fähigkeiten des Modells bei der Erzeugung von Texten haben nicht nur die allgemeine Öffentlichkeit, sondern auch die Fachwelt überrascht. Sowohl technisch als auch bei den Anwen-

dungsfeldern dieses und vergleichbarer Modelle ist seitdem eine dynamische Entwicklung zu beobachten.

6.1 — Technische Entwicklung

Sprachmodelle können inzwischen wesentlich mehr als Texte erstellen, da sie in größere Kontexte eingebunden werden. Über die Integration in verschiedene Anwendungen oder die Verwendung von Plug-ins können diese Modelle auch im Internet agieren, zum Beispiel E-Mails verschicken, Flüge buchen oder bezahlen. In IT-Infrastrukturen in Unternehmen werden Sprachmodelle eingebaut, um vorwiegend repetitive Aufgaben zu übernehmen und Mitarbeitende bei ihrer Arbeit zu unterstützen.

Die Leichtigkeit der Automatisierung und die Variationsbreite der Ergebnisse geht dabei inzwischen weit über bisherige IT-Produkte hinaus. Waren zuvor noch Programmierkenntnisse erforderlich, um beispielsweise eine automatisierte Archivierung zu erstellen, so ist es inzwischen technisch möglich, diese Aufgabe einfach mittels natürlichsprachlicher Eingabe an ein Sprachmodell zu delegieren: „Erstelle bitte jeden Freitag um 16 Uhr eine Exceltabelle mit den Umsatzzahlen der Woche unterteilt nach Bereich und Gebiet. Reichere sie mit einer entsprechenden zweistufigen Kuchengrafik an und maile sie an den Vorstand." Eine solche Aufgabenstellung können LLMs mit Zugriff auf die entsprechenden Unternehmensdaten und Mailserver ohne Weiteres umsetzen. Sprachmodelle prüfen inzwischen Bewerbungen im Hinblick auf die Eignung von Bewerberinnen und Bewerbern auf ausgeschriebene Stellen, erstellen Geschäftsbriefe mit direkten finanziellen Auswirkungen, schließen Buchungen ab oder beauftragen Dienstleister.

Bedeutsam für die Bedrohungs- und Gefährdungslage ist zudem die Nutzung von LLMs durch Programmiererinnen und Programmierer, die sich bei der Entwicklung komplexer IT-Produkte unterstützen lassen. Die inhaltliche Qualität der Ergebnisse wird hier unter Umständen nicht ausreichend durch Menschen gesichert.

Mit den zweifellos großen Chancen von LLMs gehen analog große Risiken einher. Einerseits können solche Modelle als Werkzeuge für Cyberangriffe missbraucht werden, andererseits können sie selbst angegriffen oder als Schwachstelle ausgenutzt werden. Da solche Modelle nicht nur in legalen Anwendungen eingesetzt werden können, sondern auch im cyberkriminellen Kontext, sind erhebliche Skalierungseffekte bei bereits bekannten Cyberbedrohungen zu erwarten. Die folgende Darstellung liefert eine Betrachtung neuer Bedrohungen und Gefährdungen, die sich aus dem Entwicklungsstand großer KI-Sprachmodelle zum Redaktionsschluss dieses Berichts absehen lassen.

6.2. — Neue Bedrohungen

Neue, vormals unbekannte Bedrohungen entstehen im Wesentlichen durch die herausragende Bedeutung der Trainingsdaten einerseits sowie durch den Einsatz der KI in der Software-Entwicklung andererseits. Auf diese neuen Bedrohungen wird im Folgenden eingegangen.

6.2.1 — Trainingsdaten

Die Ausgaben und das Verhalten großer KI-Sprachmodelle hängen wesentlich von den Trainingsdaten ab, die für das Anlernen der KI verwendet wurden. Bei Sprachmodellen, die in einem abgeschlossenen, begrenzten Unternehmenskontext entwickelt und eingesetzt werden, können das die Informationen einzelner Fachbereiche oder Abteilungen sein, gegebenenfalls auch Daten und Infrastruktur-Metadaten des gesamten Unternehmens. Bei LLMs wie GPT-3 oder GPT-4, auf denen Anwendungen wie ChatGPT basieren, kommen dagegen Trainingsdaten aus dem gesamten Internet zum Einsatz. Je mehr und je diverser die Trainingsdaten sind, desto universeller kann das Modell bei der Erledigung von Anfragen und Aufgaben hilfreiche Ausgaben erzeugen. Von den Trainingsdaten können verschiedene Bedrohungen ausgehen.

Schiefe Trainingsdaten: Enthalten Trainingsdaten eine Schiefe, einen sogenannten Bias, kann das Modell unausgewogene Ausgaben liefern. Das kann Aussagen über bestimmte Marken oder Produkte betreffen, aber zum Beispiel auch Bewertungen von Menschen, Institutionen oder politische Tendenzen, wenn Modelle beispielsweise tendenziöse Aussagen aus sozialen Medien übernehmen. Wenn Trainingsdaten manipuliert werden, können zudem Falschnachrichten und Desinformationskampagnen getriggert werden, die die öffentliche Meinung bis hin zum gesellschaftlichen Wertekanon beeinflussen können.

Selbstreferenzialität: Trainiert man LLMs mit den Inhalten des allgemeinen, öffentlichen Internets, so nimmt mit der zunehmenden Menge KI-generierter Inhalte im Internet die Selbstreferenzialität der Sprachmodelle exponentiell zu. Anders gesagt: Je mehr KI-generierte Inhalte im Internet verfügbar sind, desto mehr bestehen auch die Trainingsdaten großer KI-Sprachmodelle aus KI-generierten Inhalten. Falschnachrichten oder Desinformationskampagnen lassen sich dann immer schwerer erkennen, da unterschiedliche, ggf. auch seriös wirkende Quellen durch die Nutzung von Sprachmodellen ähnliche inhaltliche Verzerrungen aufnehmen. Die Art und die Zahl der referenzierten Quellen ist nach längerer Etablierung der unreflektierten Sprachmodellnutzung immer weniger ein Qualitätsmerkmal in Bezug auf die Echtheit oder Korrektheit einer Information, wenn das gleiche Sprachmodell an vielen Stellen eingesetzt wird.

Automatisiertes *Social Engineering*: Sprachmodelle können auf menschliche Reaktionen Antworten generieren (zunächst in Textform, aber in Zukunft vermutlich auch als Ton, Bild oder Video) und gewinnen durch diesen Dialogcharakter an Glaubwürdigkeit in einer Gesellschaft, die nicht schnell und umfassend aufgeklärt wird. Es besteht die Gefahr, dass dies in einem automatisierten *Social Engineering* mündet, da als erfolgreich erkannte Textangriffe einer beschleunigten Weiterverbreitung unterliegen, weil sie ohne menschliche Interaktion gestreut werden können.

Schwachstellen „lernen“ und finden: Sprachmodelle werden zunehmend genutzt, um Programmcode in den verschiedensten Programmiersprachen zu generieren und dadurch Programmiererinnen und Programmierer bei ihrer täglichen Arbeit zu unterstützen. Enthalten Trainingsdaten für Programmcode beabsichtigt oder unbeabsichtigt Schwachstellen oder schlechten Code, so lernt das Modell diese mit und kann sie in generiertem Code reproduzieren. Dieser kann unter Umständen ungeprüft in neue IT-Produkte übernommen werden und damit zur Vervielfältigung von Schwachstellen beitragen.

LLMs können zudem helfen, im Internet nach bestehenden Schwachstellen in Programmcode und in Unternehmensnetzwerken zu suchen und den nötigen *Exploit* für die Ausnutzung einer identifizierten Schwachstelle zu finden und zu erstellen. Kenntnisse über entsprechende Werkzeuge, die bisher erforderlich waren, sind dann nur noch in reduzierter Form nötig.

6.2.2 — Fehlerhaft erzeugter Code

Große KI-Sprachmodelle machen Fehler. Insbesondere bei der Nutzung im Rahmen der Entwicklung von IT-Produkten stellt dies eine Bedrohung dar. Das betrifft zum einen die oben genannten gelernten Schwachstellen und schlechten Codes, zum anderen jedoch insbesondere auch die Anwendungsbedingungen von Sprachmodellen. Die Bedrohung, die sich aus einem in einer Unternehmensinfrastruktur eingebauten Sprachmodell ergibt, hängt wesentlich davon ab, auf welche Daten und Dienste das Modell zugreifen darf. Die Ausgaben, die es produziert, können von den Entwicklerinnen und Entwicklern des Modells nicht mehr im Einzelnen nachvollzogen werden. Diese können faktisch nicht mehr kontrollieren, was das KI-Sprachmodell in einem bestimmten Anwendungskontext tun wird.

Je nach erteilten Zugriffsrechten kann ein Modell ganz unterschiedlich auf eine gestellte Aufgabe oder eine Anfrage reagieren. Security-by-Design als Basisanforderung an die Sicherheit von IT-Produkten ist für Sprachmodelle daher kaum erfüllbar. Da es für LLMs kein Design gibt (die KI designt sich gleichsam selbst), kann es auch keine Security-by-Design geben. Eine große Herausforderung besteht daher darin, überhaupt allgemeingültige Sicherheitskriterien im Zusammenhang mit KI-Sprachmodellen – unabhängig von einem konkreten Anwendungsfall – anzugeben.

6.3 — Neue Gefährdungen – die KI als Angriffsfläche

Die Bandbreite möglicher Anwendungen für ein Sprachmodell in einem Unternehmen steigt mit der Menge der verwendeten Unternehmensdaten und der Menge der Zugriffsrechte des Softwaresystems, in welches das Sprachmodell integriert ist. Je mehr Informationen ein Modell über das Unternehmen verarbeiten kann und je mehr Zugriffsrechte das entsprechende System hat, desto besser wird es Mitarbeitende bei ihren täglichen Aufgaben unterstützen können. Die Reichweite der Zugriffsrechte, die einem solchen System gewährt werden, sollte jedoch einer gründlichen Risikoabwägung unterzogen werden. Zumindest die folgenden Risiken sollten dabei beachtet werden.

Rekonstruktion von Trainingsdaten: Sprachmodelle können prinzipiell sämtliche gelernten Informationen aus den Trainingsdaten in Ausgaben reproduzieren, selbst wenn ihr Training auf die Vermeidung bestimmter Ausgaben abzielte. Angreifer können dieses Verhalten umgehen, um ein Modell für Angriffe zu missbrauchen. So hat sich beispielsweise gezeigt, dass häufig Trainingsdaten im gelenkten Dialog oder mittels gezielter Anfragen, die dem Modell einen bestimmten Kontext suggerieren, rekonstruiert werden können. Beispielsweise konnten dem Modell Hassbotschaften oder Anleitungen zum Bombenbau als Antwort entlockt werden, wenn man vorgab, diese Informationen als Grundlage für einen warnenden Artikel zu benötigen und damit Gutes zu tun. Selbst wenn es inzwischen durch erneutes Training der Modelle schwieriger wird, explizite Äußerungen zu extrahieren, können immer noch abstrakte Beschreibungen schädlicher Ideen zurückgegeben werden und so für deren Verbreitung sorgen oder als Ideengeber oder Recherchehelfer fungieren. Wenn die Trainingsdaten sensible Unternehmensinformationen enthalten, wird die grundsätzliche sprachliche Manipulierbarkeit eines Sprachmodells auf diese Weise schnell zu einer Schwachstelle, die für Datenleaks ausgenutzt werden kann. Ein wirksames Rechte-Management, das verschiedenen Nutzerinnen und Nutzern unterschiedliche Zugriffs- und Informationsrechte gewährt, war zum Redaktionsschluss des vorliegenden Berichts nicht möglich. Es werden stets die gesamten Trainingsdaten herangezogen.

Sammlung von Unternehmensinformationen in einer einzigen, schwer abzusichernden Anwendung: Ein mit weitreichenden Zugriffsrechten und einem KI-Sprachmodell ausgestattetes System weiß unter Umständen mehr über ein Unternehmen als jede oder jeder menschliche Beschäftigte und kann Aktionen hochautomatisiert ausführen. Mehr noch: Die Gründe für bestimmte Aktionen oder Ausgaben eines Modells sind für Mitarbeitende und selbst für IT-Sicherheitsverantwortliche, Administratorinnen und Administratoren in Unternehmen schwer durchschaubar und teilweise sogar gänzlich unbekannt. Aus diesem Grund sind aktuelle Kriterien für ein wirksames IT-Sicherheitsmanagement, wie sie auch für andere IT-Produkte gelten, nur bedingt auf Softwaresysteme anwendbar, die mit großen Datenmengen und KI-Sprachmodellen arbeiten.

Möglicher Missbrauch des Modells: Die Nützlichkeit von Sprachmodellen ergibt sich wesentlich aus der Steuerbarkeit mittels natürlicher Sprache. Ziel der aktuellen Modellentwicklung ist es, Befehle und auch komplexe Aktionen nicht mehr programmieren zu müssen, sondern als natürlichsprachliche Arbeitsanweisungen, sogenannte Prompts, an das Modell zu delegieren. Das Finden der richtigen Anweisungen wird „Prompt Engineering" genannt. Dieses Konzept ermöglicht jedoch auch sogenannte „Prompt Injections". Das sind Eingaben in manipulativer oder krimineller Absicht. So können Angreifer mittels eines spezifischen Dialogaufbaus ein Modell beispielsweise sukzessive dazu bringen, eine bestimmte schädliche Aktion auszuführen oder Daten wie etwa Identitätsdaten herauszugeben.

Darüber hinaus können diese *maliziö*sen Eingaben in ein ansonsten nicht als *Malware* agierendes Sprachmodell („Adversarial Attacks") in bestimmten Angriffsszenarien auch über zweistufige *Angriffsvektoren* ausgeführt werden. So können Angreifer Textabschnitte in Webseiten verstecken, die zwar für den Menschen nicht sichtbar sind, für ein KI-Sprachmodell aber ausführbare Befehle wie etwa zum Herunterladen von Schadcode enthalten. Bekommt ein harmloses Auskunftssystem, das solche Seiten mit einem KI-Sprachmodell analysiert, diesen versteckten Input und ist aufgrund seiner technischen Fähigkeiten und Berechtigungen in der Lage, als Agent zu handeln, kann Schadsoftware ins System der Nutzerin oder des Nutzers gelangen. Bei dieser Art von Angriff, bei dem eine andere Person als der Nutzende selbst eine Anweisung an das Sprachmodell übergibt, spricht man von sogenannten „Indirect Prompt Injections".

Auch Angreifer, die auf konventionelle Art in ein Unternehmensnetzwerk eingebrochen sind, können mit der entsprechenden Berechtigung ein im Unternehmensnetz befindliches Sprachmodell entsprechend missbrauchen.

6.4. — Systemische Bedrohungsveränderung

Neben ganz neuen Bedrohungen der Cybersicherheit bringen KI-Sprachmodelle auch eine Veränderung bereits bekannter Bedrohungen hervor. Dies betrifft zum einen Skalierungseffekte, die durch die enorme Performanz der KI entstehen. Dies betrifft jedoch auch die informationstechnischen Infrastrukturen insgesamt bzw. die KI als Agent, also als gleichsam handelnden Akteur innerhalb dieser Infrastrukturen. Zur Manipulation der „Schwach-

stelle Mensch“ durch *Social Engineering* kommt nunmehr die Manipulation der „Schwachstelle KI“ durch Prompt Engineering hinzu.

6.4.1 — Skalierungseffekte bekannter Bedrohungen

Neben den genannten neuen Bedrohungen und Gefährdungen werden große KI-Sprachmodelle wahrscheinlich Skalierungseffekte bei bekannten Cyberbedrohungen bewirken.

Spam, Phishing, Social Engineering

Durch die Sprachmodelle sind mehr *Spam*- und *Phishing*-Mails zu erwarten, die weniger Rechtschreib- und Grammatikfehler enthalten und somit schwerer zu erkennen sind. Da LLMs nicht nur qualitativ hochwertige Texte verfassen, sondern auch entsprechende Vorlagen in Wortwahl und Sprachstil überzeugend imitieren können, werden Social-Engineering-Angriffe wie Spear-*Phishing* und *CEO-Fraud* personalisierbar und damit weiter an Überzeugungskraft gewinnen. Diese Entwicklung kann durch die ebenfalls rasante Entwicklung im Bereich KI-generierter Bild-, Audio- und Videoformate zusätzlich verschärft werden. Verfahren, mit deren Hilfe Fälschungen von Stimmen erstellt werden können, haben sich in den letzten Jahren sowohl in ihrer Qualität, als auch in ihrer Verfügbarkeit und Zugänglichkeit signifikant verbessert. So ist es beispielsweise für Laien möglich, gefälschte Audiobeispiele von bekannten Politikern zu erstellen, die insbesondere in Bezug auf deren Klangfarbe nicht mehr vom Original zu unterscheiden sind (siehe auch Kapitel *KI für autonomes Fahren und mediale Identitäten*, S. 73). Die zunehmende Echtzeitfähigkeit dieser *Deepfakes* genannten Manipulationen bewirkt beispielsweise, dass man in Onlinemeetings in absehbarer Zeit nicht mehr sicher sein kann, ob man mit der realen Person, einem Angreifer oder sogar dem Avatar eines Chatbots spricht.

Schadprogramme

Große KI-Sprachmodelle, die auf Code-Beispielen trainiert wurden, sind grundsätzlich in der Lage, Programmcode zu erzeugen. Das schließt Schadprogramme ein. Zwar bemühen sich Entwickler, KI darauf zu trainieren, keine Hilfestellung für strafbare Handlungen zu geben. Mittels Prompt Engineering lassen sich derartig antrainierte Skrupel eines Modells jedoch potenziell umgehen. Neben einer rascheren Neuproduktion von Schadsoftware ist daher künftig mit schnelleren Veränderungen bestehender Schadprogramme zu rechnen, was deren Detektion erschwert. Erwartet werden muss eine schnellere und bessere Weiterentwicklung von Angriffswerkzeugen jeglicher Art: vom *Information Stealer* über das *DDoS-Botnetz* bis hin zu den einzelnen Modulen eines komplexen *Ransomware*-Angriffs. Insbesondere die Möglichkeiten der Codegenerierung dürften die Zugangsvoraussetzungen zu cyberkriminellen Aktivitäten wie zumindest rudimentäre Programmier- und Systemkenntnisse deutlich senken. Die Zahl der Personen mit krimineller Energie, die zum Erzeugen von Schadprogrammen fähig sind, wird durch diese geringeren fachlichen Anforderungen vermutlich steigen.

***Ransomware* und APT**

Im Zusammenhang mit komplexen Cyberangriffen dürften Sprachmodelle insbesondere einen Einfluss darauf haben, wie Angreifer sich in einem infiltrierten Unternehmensnetzwerk ausbreiten, wie sie dort Daten sammeln und wie sie ihre Zugriffsrechte erweitern können. Während sich Angreifer in herkömmlichen Unternehmensnetzwerken vergleichsweise mühsam von System zu System vorarbeiten müssen, finden sie künftig möglicherweise ein KI-Sprachmodell mit umfangreichem Wissen über das Unternehmen und weitreichenden Zugriffsrechten vor, welches verhältnismäßig leicht manipuliert und für Angriffe missbraucht werden kann. Derartige Modelle dürften nicht nur für cyberkriminelle Angreifer ein attraktives Angriffsmittel darstellen, sondern ebenso für Zwecke der Cyberspionage und Cybersabotage nutzbar sein.

Effekte

Durch die Skalierung dieser grundsätzlich bekannten Bedrohungen entstehen neue Dynamiken. Die Zahl der potenziellen Angreifer kann sich durch die Leichtigkeit des Zugangs deutlich erhöhen unabhängig davon, ob es sich um staatliche Akteure, finanziell motivierte Angreifer, Innentäter, durch Spieltrieb motivierte *Script-Kiddies* oder sogar leichtfertige Sicherheitsforscher handelt. Selbst wenn die Nutzung von KI-Elementen auch auf der Verteidigerseite für eine deutlich gestiegene Aufklärungsrate sorgt, kann sich eine negative Bilanz einstellen. Die Kapazitäten der Strafverfolgungsbehörden werden möglicherweise stark ausgelastet und insbesondere in Richtung der weniger kenntnisreichen KI-gestützten Angreifer umgelenkt, weil diese leichter zu ermitteln sind. Sie fehlen dann für die Verfolgung kennt-

nisreicher Angreifer. Wie sich die Angreifer-Verteidiger-Dynamik bei beidseitigem Gebrauch aktueller KI-Sprachmodelle entwickeln wird, ist nicht vorhersagbar. Die Vermutung liegt nah, dass die Seite, die die Technologie zuerst nutzt, größere Chancen hat. Bei der aktuell hohen Entwicklungsgeschwindigkeit reicht auch ein kleinerer zeitlicher Vorsprung für einen essenziellen Vorteil.

6.4.2 — Schwachstellen, Unschärfe und Agentennetzwerke

Durch ihren Black-Box-Charakter stellen große KI-Sprachmodelle eine Schwachstelle an sich dar. Das Prompt Engineering als Mittel zur Ausnutzung von Schwachstellen eines Modells hat keine klar definierten Grenzen. Es handelt sich nicht um eine technische Fehlleistung wie einen *Stack Overflow*, der überprüft und verhindert werden kann. Auch gibt es aktuell keine Möglichkeit, einen Prompt als Schadcode zu identifizieren, weil der Input syntaktisch nicht überprüft werden kann, sondern semantisch überprüft werden müsste. Eine natürlichsprachliche Prompt-Injection ist daher nur unscharf und damit unsicher abzuwehren, weil der semantische Inhalt durch sehr viele verschiedene Formulierungen übermittelt oder auch anders kontextualisiert werden kann.

Dadurch wird das Schwachstellenmanagement von KI-Sprachmodellen zu einer Aufgabe mit unscharfem Ziel. Es muss nicht nur ein bestimmter Text unterbunden werden, sondern auch alle semantischen Äquivalente. Schwachstellenmanagement verschiebt sich daher von einer technischen auf eine wenig greifbare, weil semantische Ebene. Solche Schwachstellen können deshalb auch nicht mehr eindeutig klassifiziert werden. Beispielsweise kann ein Prompt, der in einem System als schadhaft erkannt wird, trotz Schließen der Schwachstelle in diesem System in einem anderen System noch wirksam sein, weil auch verschiedene Systeme aufgrund gleicher Trainingsgrundlagen unscharfe Überlappungen aufweisen. Damit wird der Unterschied zwischen einer Zero-Day-Schwachstelle und einer bekannten öffentlichen Schwachstelle ebenfalls unschärfer, was das Vorgehen für IT-Sicherheitsverantwortliche grundsätzlich infrage stellt.

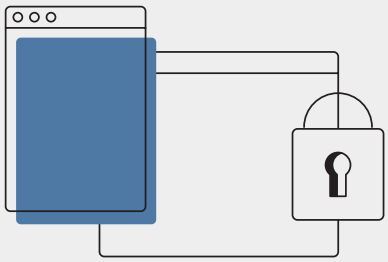
Berücksichtigt man diese Unschärfe, gewinnt zudem eine weitere Entwicklung an Relevanz. Aktuell werden Sprachmodelle nicht nur für die Ausgabe von Text, den Menschen lesen sollen, in IT-Systeme integriert. Von großer Bedeutung sind Agentensysteme, in denen die Ausgaben von KI-Sprachmodellen in (elektronische) Handlungen umgesetzt werden. Hier kommt es entscheidend darauf an, ob für diese Handlungen weiterhin Menschen Verantwortung tragen. Damit dies der Fall ist, dürfen diese Systeme nur unter menschlicher Kontrolle handeln können. Dazu gehören Abfragen wie „Jetzt kostenpflichtig kaufen/buchen?“ oder „Wollen Sie diese persönlichen Daten wirklich an den Anbieter XY/in den *Cloud*speicher übermitteln?“. Solche Sicherheitsabfragen stehen jedoch dem Trend entgegen, Funktionalitäten in die *Cloud* zu verlagern und sie zu kompletten Agentennetzwerken auszubauen. Verbindet man die Unschärfe einzelner Schwachstellen mit der Vielzahl an künftig beteiligten externen Komponenten, die potenziell selbst KI-Komponenten mit Schwachstellen enthalten, wird die Größe der Aufgabe deutlich, solche Strukturen zu schützen. Vor diesem Hintergrund entwickelt das BSI gemeinsam mit nationalen und internationalen Partnern Kriterien für einen sicheren Betrieb von KI-Sprachmodellen und KI-Systemen allgemein (vgl. Kapitel *Künstliche Intelligenz*, Seite 71).

Die Lage der IT-Sicherheit in Deutschland 2023
im Überblick

Ransomware

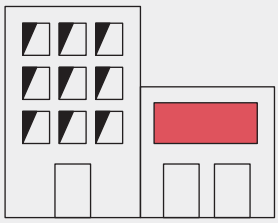
ist weiterhin die größte Bedrohung.

2 **Ransomware-Angriffe** auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.



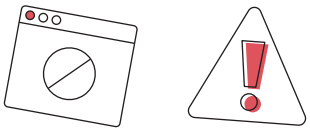
68 erfolgreiche **Ransomware-Angriffe auf Unternehmen** wurden bekannt.

15 davon richteten sich gegen **IT-Dienstleister**.

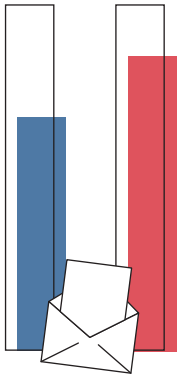


Mehr als **2.000** **Schwachstellen** in Softwareprodukten **(15 % davon kritisch)** wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %.**

Eine Viertelmillion
neue **Schadprogramm-Varianten** wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.



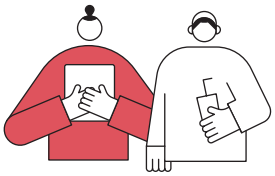
66%
aller **Spam-Mails** im Berichtszeitraum waren Cyberangriffe:
34 % Erpressungsmails,
32 % Betrugsmails



84%
aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.

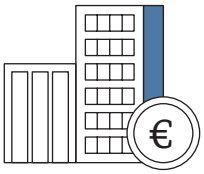
Top-3-Bedrohungen je Zielgruppe:

Gesellschaft



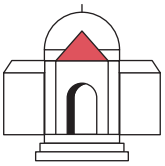
Identitätsdiebstahl
Sextortion
Phishing

Wirtschaft

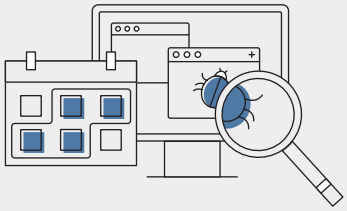


Ransomware
Abhängigkeit innerhalb der IT-Supply-Chain
Schwachstellen, offene oder falsch konfigurierte Onlineserver

Staat und Verwaltung



Ransomware
APT
Schwachstellen, offene oder falsch konfigurierte Onlineserver



Rund **21.000** **infizierte Systeme** wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.

Durchschnittlich rund **775** **E-Mails mit Schadprogrammen** wurden an jedem Tag im Berichtszeitraum in deutschen Regierungsnetzen abgefangen.

370 **Webseiten** wurden im Durchschnitt an jedem Tag des Berichtszeitraums für den Zugriff aus den Regierungsnetzen gesperrt. **Der Grund:** Die Seiten enthielten Schadprogramme.

6.220
2022

5.100
2021

7.120
Teilnehmer hatte die **Allianz für Cyber-Sicherheit** im Jahr 2023.

Deutschland
Digital•Sicher•BSI•

13 Monate Cybersicherheit im Überblick

Juni 22

- *Ransomware*-Angriff auf alle Rathäuser eines Landkreises sowie mehrere kommunale Betriebe einer angrenzenden kreisfreien Großstadt
- Neue Technische Richtlinien zur Sicherheit in Telekommunikations-Infrastrukturen, Sicherheit von Digitalen Gesundheitsanwendungen und für Hersteller mobiler Finanzanwendungen
- Gegenseitige Anerkennung von IT-Sicherheitszertifikaten zwischen ANSSI und BSI
- Zweiter Bericht zum Digitalen Verbraucherschutz 2021 erscheint.

Juli 22

- Neues Zertifizierungsprogramm für Komponenten der 5G-Telekommunikationsnetze
- Saarland wird zweite Pilotregion des Cyber-Sicherheitsnetzwerks (CSN).
- Erste Prüfstelle für Programm *NESAS CCS-GI* anerkannt
- BSI stellt Tool zum Telementrie-Monitoring für Windows 10 zur Verfügung.

Angriffe auf albanische Regierungsinstitutionen mit der *Ransomware* GoneXML und dem *Wiper* ZeroShred

August 22

- Industrie- und Handelskammern nach Cyberangriff deutschlandweit offline
- *Ransomware*-Angriffe auf höhere staatliche Einrichtungen in Montenegro
- BSI warnt vor Einsatz unsicherer Funktürschlösser der Marke ABUS.
- BSI startet in Sachsen-Anhalt virtuelle Roadshow für Kommunen.

September 22

- Verstärkte *DDoS-Angriffe* durch Hacktivisten-*Botnetz*-Projekt „DDoSia“
- *Ransomware*-Angriffe auf höhere staatliche Einrichtungen in Bosnien-Herzegowina
- 10 Jahre Allianz für Cyber-Sicherheit (ACS)
- BSI veröffentlicht Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung.

Oktober 22

- Einsatz der *Ransomware* Prestige unter anderem gegen Unternehmen in Polen
- BSI und Cybersicherheitsbehörde von Singapur erkennen gegenseitig Cybersicherheitskennzeichen an.
- BSI bestätigt Sicherheitseigenschaften von Betriebssystemen von iPhone und iPad.
- Erstes regionales Forum des Cyber-Sicherheitsnetzwerks (CSN) im Rhein-Main-Gebiet durchgeführt

November 22

- CSAF als internationaler Standard aufgenommen
- Digitalbaromenter 2022 von BSI und Polizei

Dezember 22

- Abschaltung von etwa 50 Webseiten, die Dienste für gezielte *DDoS-Angriffe* anboten
- BSI und ANSSI veröffentlichen Publikation zur Sicherheitszertifizierung von IT-Produkten.
- BSI und Hessen unterzeichnen Kooperationsvereinbarung.
- BSI und ZF entwickeln Sicherheitscheck für Künstliche Intelligenz im Automobil.

Januar 23

- Weltweiter *Ransomware*-Angriff auf ESXi-Server
- Cybersicherheit und digitale Souveränität – 5G/6G-Projekte gestartet

Februar 23

- Angriffskampagne gegen Schwachstelle in Filesharing-Software GoAnywhere
- Cyberangriffe auf IT-Dienstleister
- EU-Richtlinien NIS 2 und CER treten in Kraft.
- BSI veröffentlicht Betaversion des TLS-Testtools „TaSK“.

Verstärkte Angriffe durch *DDoS*-Hacktivisten

März 23

- Supply-Chain-Angriff infolge eines anderen Supply-Chain-Angriffs auf mehrere 100.000 Geschäftskunden
- Angriff gegen Filesharing-Software GoAnywhere
- Kritische Zero-Day-Schwachstellen in Exynos-Modemchips veröffentlicht
- BSI und Rheinland-Pfalz unterzeichnen Kooperationsvereinbarung.

April 23

- Empfehlungen an IT-Hersteller gemeinsam mit internationalen Partnerbehörden
- BSI bietet Zertifizierungen nach neustem Common-Criteria-Prüfstand an.
- BSI veröffentlicht Studie zu Hardware-Angriffen auf Mikrocontroller.
- BSI entwickelt mit Partnern den Standard-Sicherheitscheck DIN-SPEC für KMU.

Mai 23

- Einschätzung der Cyber-Sicherheitslage in Deutschland nach dem russischen Angriff auf die Ukraine
- BSI erteilt erste IT-Sicherheitskennzeichen für Breitbandrouter.
- Veröffentlichung von Whitepaper zur Bestandsaufnahme zur Prüfbarkeit von KI-Systemen

Juni 23

- Internationale Cyber-Sicherheitsbehörden nehmen Ramsomware LockBit unter die Lupe.
- Neuer BSI-Standard 200-4 verhilft mit Business Continuity Management zu ganzheitlicher *Resilienz*.
- BSI und kommunale Spitzenverbände starten Pilotprojekt für bessere IT-Absicherung in Kommunen.
- BSI veröffentlicht neue technische Richtlinie zur Informationssicherheit für Satelliten.

Im gesamten Berichtszeitraum:

- 27 *Ransomware*-Angriffe auf Kommunalverwaltungen und kommunale Betriebe
- 23 *Ransomware*-Angriffe auf Bildungs- und Forschungseinrichtungen
- Cyberangriffe auf 15 IT-Dienstleister mit Auswirkungen auf deren Kunden in öffentlicher Verwaltung, Wirtschaft, Gesellschaft

Gefährdungslage

Teil B: Erkenntnisse zur Gefährdungslage in der Gesellschaft

7. — Erkenntnisse zur Gefährdungslage in der Gesellschaft

Menschen in Deutschland leben digital wie nie. Ob Onlineshopping oder Onlinebanking, Nachrichtenkonsum und Information im Netz oder Zeitvertreib in sozialen Medien: Die Digitalisierung hat weitreichende Auswirkungen in zahlreiche Bereiche der Gesellschaft hinein. Das BSI arbeitet mit gezielten Angeboten für Verbraucherinnen und Verbraucher daran, seinen gesetzlichen Auftrag zum digitalen Verbraucherschutz zu erfüllen und Menschen Unterstützung bei der sicheren Nutzung digitaler Angebote zu bieten. Dabei stehen Prävention, Detektion und Reaktion im Mittelpunkt. Im Berichtszeitraum hat das BSI dem Thema Identitätsdaten besondere Aufmerksamkeit gewidmet. Neben Maßnahmen der Verbraucherinnen und Verbraucher, um ihre persönlichen Daten vor Missbrauch zu schützen, stehen insbesondere die Hersteller und Anbieter digitaler Dienste in der Verantwortung.

7.1 — Missbräuchliche Nutzung von Identitätsdaten

Für Verbraucherinnen und Verbraucher war im Berichtszeitraum das Thema Datenleaks prägend. In vielen Fällen standen diese in Verbindung mit *Ransomware*-Angriffen, bei denen Cyberkriminelle große Datenmengen von Organisationen exfiltrierten, um später mit deren Veröffentlichung zu drohen, sofern keine Löse- oder Schweigegeldzahlung erfolgt (vgl. Kapitel *Ransomware*, Seite 14). Betroffen waren sowohl Unternehmen als auch Institutionen des öffentlichen Sektors, wie zum Beispiel Kommunalverwaltungen und Bildungseinrichtungen. Ein erfolgreicher *Ransomware*-Angriff bedeutet einerseits ein enormes Schadenspotenzial für das Angriffsopfer, andererseits wirkt sich dies negativ auf Verbraucherinnen und Verbraucher aus. Während die Angriffsopfer mit der Wiederherstellung der betroffenen informationstechnischen Systeme beschäftigt sind, sehen sich Verbraucherinnen und Verbraucher mit der Veröffentlichung ihrer teils sensiblen Daten konfrontiert, die häufig Adress-, Bezahl- und/oder Login-Daten umfassen. Erfolgreiche Angriffe mittels *Ransomware* bedeuten für Verbraucherinnen und Verbraucher zudem erhebliche Verfügbarkeitseinschränkungen bis hin zum Ausfall von Behörden- und Unternehmensdienstleistungen. Insbesondere die Beeinträchtigung oder der Ausfall von kritischen Dienstleistungen, wie zum Beispiel ausbleibenden Zahlungen von Sozialleistungen oder Elterngeld, hat gravierende Auswirkungen.

Die infolge eines *Ransomware*-Angriffs erbeuteten Identitätsdaten ermöglichen es den Angreifern, zusätzlichen Druck auf die Angriffsopfer auszuüben, indem sie drohen, die Daten auf dafür eingerichteten Leak-Seiten im Darknet zu veröffentlichen. Einige Angreifer gingen einen Schritt weiter und erstellten dedizierte Webseiten, auf denen von einem Datenleak betroffene Verbraucherinnen und Verbraucher überprüfen konnten, ob ihre Daten gestohlen wurden. Da diese Webseiten im Clear Web, also im öffentlichen Internet, gehostet werden, sind diese von Suchmaschinen indexierbar und können zu Suchergebnissen hinzugefügt werden. Daher ist ein transparenter Umgang, ausgehend von dem Angriffsopfer bis hin zu den potenziell von einem Datenleak betroffenen Verbraucherinnen und Verbrauchern, essenziell, um durch zeitnahe Information und Hilfestellung die negativen Auswirkungen zu begrenzen.

Neben Organisationen waren auch Verbraucherinnen und Verbraucher unmittelbar von Angriffen mittels *Ransomware* betroffen. Cyberkriminelle erpressten, wenn auch vergleichsweise geringe Summen Lösegeld mit *Ransomware*-Angriffen auf private Endgeräte wie beispielsweise Netzwerkspeichergeräte *(NAS)*. Die betroffenen Verbraucherinnen und Verbraucher hatten infolgedessen keinen Zugriff mehr auf ihre privaten Daten.

Neben Angriffen mittels *Ransomware* stellten auch sogenannte *Information Stealer* eine Bedrohung für die Datensicherheit von Verbraucherinnen und Verbrauchern dar. Während bei *Ransomware*-Angriffen die Betroffenen selbst das Ziel sind, da von diesen Lösegeld für die Entschlüsselung ihrer Daten verlangt wird, steht bei Angriffen mittels *Information Stealern* der Handel mit gestohlenen Identitätsdaten im Vordergrund. *Information*

Stealer sind Schadprogramme, die es Cyberkriminellen ermöglichen, auf infizierten Geräten unbemerkt an unterschiedliche Arten persönlicher Daten, wie beispielsweise Login-Daten für verschiedene Onlinedienste, zu gelangen. Die gestohlenen Daten umfassen auch Cookies und biometrische Daten, wie zum Beispiel Fingerabdrücke. Die entwendeten Anmeldeinformationen bieten Cyberkriminelle anschließend auf Marktplätzen im Darknet zum Verkauf an. Auf einem der größten Untergrundmarktplätze für Identitätsdaten boten Cyberkriminelle Interessenten ein Browser-*Plug-in* an, über das es möglich war, die gestohlenen Anmeldeinformationen direkt im Webbrowser zu importieren. Dadurch konnte die digitale Identität einer anderen Person mit wenigen Klicks angenommen werden.

Datenleaks aufgrund von Schwachstellen

Datenleaks waren auch auf mangelnde Schutzmaßnahmen für Login-Daten bei Onlinediensten oder Schwachstellen in IT-Produkten, wie zum Beispiel im Onlineshopping, zurückzuführen. So gelang es verschiedenen Angreifern unter anderem, Onlineshops zu kompromittieren und dabei Daten wie Kundennamen, Rechnungs- und Lieferadressen, Telefonnummern, Bestelldetails und auch Zahlungsdaten zu stehlen. Schwachstellen in der von den Onlineshops verwendeten Shop-Software stellen dabei ein großes Risiko für die Sicherheit von Verbraucherdaten dar. Im Berichtszeitraum traten beispielsweise Schwachstellen in Shop-Softwareprodukten auf, die unberechtigte Datenbankzugriffe ermöglichten, durch Zugriff auf den SQL-Manager die Einsicht in abgeschottete Daten erlaubten oder bei Ausnutzung zu einem Cross-Site-Scripting-Angriff führen konnten. Dabei schleusen Angreifer Schadcode in Webformulare oder URLs ein und lassen die Benutzerin oder den Benutzer diesen unbemerkt ausführen.

Im Rahmen einer BSI-Studie zur IT-Sicherheit von Verbraucherdaten im Onlineshopping[5] ergab eine Schwachstellenanalyse von zehn zufällig ausgewählten Shop-Softwareprodukten eine Vielzahl von Schwachstellen mit teilweise gravierenden Auswirkungen auf die Datensicherheit von Verbraucherinnen und Verbrauchern. Nahezu alle getesteten Produkte wiesen eine unzureichende Passwortrichtlinie auf, wodurch ein angemessener Schutz von Kundenkonten nicht gegeben war. Darüber hinaus wies die Hälfte der getesteten Shop-Softwareprodukte JavaScript-Bibliotheken von Drittanbietern auf, die verwundbar durch bekannte Schwachstellen sind und somit ein unkalkulierbares Sicherheitsrisiko darstellen. Die geschilderten Fälle verdeutlichen, dass unzureichende IT-Sicherheitsmaßnahmen das Risiko für Verbraucherinnen und Verbraucher erhöhen, Opfer eines Datenleaks zu werden. Eine ebenfalls im Rahmen der Studie durchgeführte repräsentative Befragung ergab, dass rund ein Viertel der Befragten bereits von einem Datenleak im Onlineshopping betroffen war. Weiterhin gaben 68 Prozent der Befragten an, dass sie generell Bedenken beim Onlineshopping haben.

Angriffe auf Kundendatenbanken bei Onlinediensten oder der Diebstahl von Identitätsdaten infolge von *Malware* liegen meist außerhalb des Einflussbereichs der von einem Datenleak betroffenen Verbraucherinnen und Verbraucher. Derartige Sicherheitsvorfälle mit darauffolgender Veröffentlichung sensibler persönlicher Daten unterminieren daher in besonderer Weise das Vertrauen in die Nutzung digitaler Dienste sowie in die Digitalisierung insgesamt. Zudem können die entwendeten Daten für weitere Angriffe gegen Verbraucherinnen und Verbraucher genutzt werden. Der unbefugte Zugriff und die Veröffentlichung persönlicher Daten stellen daher ein hohes Risiko für Verbraucherinnen und Verbraucher dar.

7.2 — Handlungsfelder: Hersteller und Anbieter in der Verantwortung

Die Erkenntnisse zur aktuellen Gefährdungslage in der Gesellschaft machen deutlich, dass neben der Sensibilisierung und Aufklärung von Verbraucherinnen und Verbrauchern insbesondere das verantwortungsvolle Handeln der Hersteller und Anbieter entscheidend für einen wirksamen Digitalen Verbraucherschutz ist. Besonders deutlich wird dies beim Schutz vor drohenden Datenleaks (vgl. Kapitel *Spam und Phishing*, Seite 30), da die Auswirkungen für alle Beteiligten vielfältig und zugleich gravierend sein können. Bei der hersteller- und anbieterseitigen Datenverarbeitung wie auch -speicherung sind daher geeignete technisch-organisatorische Maßnahmen umzusetzen, um

- die Privatsphäre und sensible Kundendaten zu schützen,
- finanzielle Schäden sowohl aufseiten der Verbraucherinnen und Verbraucher (z. B. durch gestohlene Onlinebanking-Zugänge) als auch aufseiten der Hersteller und Anbieter (Bußgelder, Schadenersatzforderungen) zu vermeiden,
- die Reputation des Anbieters zu schützen,
- Vertrauen und langfristige Kundenzufriedenheit zu fördern.

Zu den Maßnahmen gehören unter anderem der Einsatz effektiver Verschlüsselungstechnologien, die regelmäßige Überprüfung und Stresstests der IT-Infrastruktur, die Schulung der Mitarbeitenden im Umgang mit sensiblen Daten sowie die transparente und schnelle Kundenkommunikation im Falle eines Datenabflusses.

Die skizzierten Anforderungen verdeutlichen die Komplexität sowie die Wirkungsmechanismen von IT-Sicherheitsfragen und setzen für Erfolg versprechende Antworten ein tiefes organisatorisches Verständnis für den verantwortungsbewussten Umgang mit digitalen Technologien voraus. Das als Corporate Digital Responsibility (CDR) bezeichnete Denken und Handeln erfordert dabei eine proaktive Herangehensweise, die sich unter anderem im „Security-by-Design"-Ansatz widerspiegelt. Dieser steht für die Berücksichtigung von IT-Sicherheitsaspekten in allen Phasen des Hard- und Softwareentwicklungsprozesses, von der Konzeption bis hin zur Implementierung und zum Betrieb. Durch die frühzeitige Identifikation und Berücksichtigung von Sicherheitsanforderungen können sowohl potenzielle Schwachstellen als auch hohe (monetäre) Aufwendungen für spätere Fehlerbehebungen minimiert werden.

Ein weiterer wichtiger Baustein in der verantwortungsvollen Entwicklung digitaler Alltagstechnologien ist die einfache, barrierefreie und intuitive Gestaltung von Sicherheitsfunktionen (Usable Security) in Geräten und Onlineanwendungen. Deren nutzerfreundliche und zugleich nutzergerechte Ausgestaltung erhöht die Bereitschaft der Verbraucherinnen und Verbraucher, sie zu aktivieren und durchgehend zu nutzen. Positive Nutzungserlebnisse (User Experience) von IT-Sicherheitsmechanismen erhöhen zudem deren Akzeptanz. Usable Security spielt damit auch eine wichtige unterstützende Rolle beim wirksamen Schutz vor *Spam* und *Phishing* im Verbraucheralltag (vgl. Kapitel *Spam und Phishing*, Seite 30).

All diese Anstrengungen zur Verbesserung der IT-Sicherheitseigenschaften von Geräten, Anwendungen und Diensten sollten für Verbraucherinnen und Verbraucher noch transparenter und sichtbarer werden. Klare Kennzeichnungen wie das IT-Sicherheitskennzeichen des BSI sind hierfür ein wirksames Instrument. Das BSI sieht hier die Notwendigkeit, noch stärker gestaltend tätig zu werden, um Informationssicherheit im digitalen privaten Alltag zu fördern.


Volksbanken
Raiffeisenbanken

um die Auswirkungen der gestiegenen Energiepreise für die Verbraucher abzumildern, wird im September ein Pauschalbetrag von 300 Euro an alle Erwerbstätigen ausbezahlt. Dies ist ein Beschluss der Bundesregierung und Inhalt des Entlastungspakets 2022, welches die durch den Ukraine-Krieg entstandene Energiekosten-Explosion etwas abfedern soll.

Wer erhält die Energiepauschale?

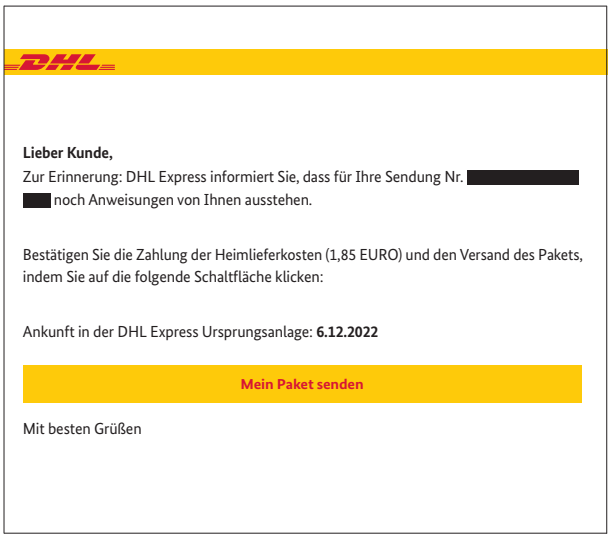
- **Steuerpflichtige** mit Einkünften aus Gewinneinkunftsarten (§ 13, § 15 oder § 18 des Einkommensteuergesetzes) und
- **Arbeitnehmerinnen und Arbeitnehmer**, die Arbeitslohn aus einem gegenwärtigen Dienstverhältnis beziehen und in die Steuerklassen I bis V eingereiht sind oder als **geringfügig Beschäftigte** pauschal besteuert werden.

Um Ihre Identät sowie den Anspruch auf eine Auszahlung feststellen zu können, benötigen wir eine Bestätigung Ihrer bereits angegeben Daten bei der Erstellung Ihres Girokontos in einer unserer Filialien.

Geben Sie noch heute Ihre aktuellen Daten auf unserer Homapege an und erhalten Sie innerhalb der nächsten vier Wochen Ihre Auszahlung der Energiepauschale. Dies können Sie ganz bequem von zu Hause aus erledigen, anbei finden Sie einen Direktlink zu den geforderten ...

Zur Homepage

Abbildung 13: Beispiel einer *Phishing*-Mail im Namen von Banken
Quelle: *Phishing*-Radar vom 09. September 2022[6]


DHL

Lieber Kunde,

Zur Erinnerung: DHL Express informiert Sie, dass für Ihre Sendung Nr. [redacted] noch Anweisungen von Ihnen ausstehen.

Bestätigen Sie die Zahlung der Heimlieferkosten (1,85 EURO) und den Versand des Pakets, indem Sie auf die folgende Schaltfläche klicken:

Ankunft in der DHL Express Ursprungsanlage: **6.12.2022**

Mein Paket senden

Mit besten Grüßen

Abbildung 14: Beispiel einer *Phishing*-Mail im Namen eines Paketversanddienstleisters
Quelle: *Phishing*-Radar vom 02. Dezember 2022[7]

Identitätsdiebstahl mit Phishing-as-a-Service (PhaaS)

Sachverhalt

Es gibt inzwischen eine Vielzahl an PhaaS-Anbietern, die einen unterschiedlichen Umfang an Services für Angreifer anbieten: von der Erstellung und dem Versand von Phishing-E-Mails über die Verwaltung von Weiterleitungswebseiten und den endgültigen Köderseiten bis hin zu technischem Support und Schritt-für-Schritt-Tutorials. Häufig gibt es schon fertige Phishing-Seiten für bekannte Webseiten wie unter anderem Google, Microsoft, LinkedIn, iCloud, Facebook, Twitter, Yahoo, WordPress und Dropbox. Daneben gibt es auch Angebote, auf Anfrage individuelle Phishing-Seiten für spezielle Angriffszwecke zu erstellen.

Gängig sind Phishing-Proxy-Services, die als Man-in-the-Middle (MITM) zwischen Opfer und der Login-Seite eines Unternehmens agieren. In der Regel können sie Zugangsdaten und Cookies stehlen und somit beispielsweise auch Multifaktor-Authentifizierung umgehen.
Ein Beispiel für einen Phishing-Proxy-Service ist EvilProxy. Besorgniserregend ist, dass EvilProxy neben den Phishing-Login-Seiten für Google, Microsoft & Co. auch Phishing-Login-Seiten für den Python Package Index (offizielles Softwareverzeichnis für die Programmiersprache Python), npmjs (von über 11 Millionen Entwicklern weltweit genutzter JavaScript Package Manager) und GitHub (Softwareentwickler-Plattform) anbietet. Eine Kompromittierung solcher Seiten könnte zu Supply-Chain-Angriffen durch bösartig modifizierte oder geklonte Code-Repositories führen und beispielsweise legitime Software mit Information Stealern infizieren, die Zugangsdaten stehlen.

Bewertung

Phishing bleibt weiterhin ein verlässlicher Vektor für Angreifer, um initialen Zugang zu IT-Netzen zu erhalten. Durch die zuvor genannten PhaaS-Angebote können auch weniger fortschrittliche Angreifer mit geringen Ressourcen Phishing-Angriffe durchführen, was einen deutlichen Einfluss auf die weitere Entwicklung von Phishing haben wird. Darüber hinaus sind Phishing-Aktivitäten vielfältiger geworden und beinhalten Angriffe über Social Media, SMS und Voice-Calls.

Reaktion

Das BSI warnt Nutzerinnen und Nutzer über seine Social-Media-Kanäle.

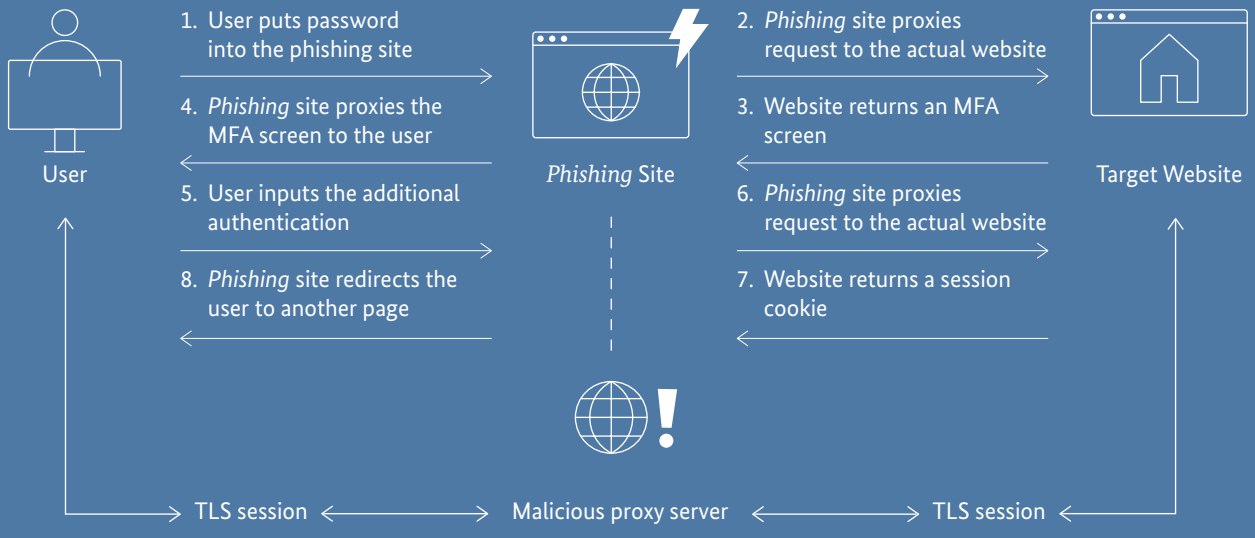


Abbildung 15: Umgehung von Multifaktor-*Authentifizierung*

8. – Erkenntnisse zur Gefährdungslage in der Wirtschaft

Mit einem Blick auf die Cybersicherheitslage in der Wirtschaft zeigt sich, dass ein großer Teil der deutschen Unternehmen die Bedeutung von Cybersicherheit erkannt hat. In einer Umfrage des TÜV-Verbandes aus 2023 gaben 95 Prozent der befragten Unternehmen an, dass Cybersicherheit ein Muss für den Schutz der Unternehmensdaten ist. Ebenso sehen sie 80 Prozent der Unternehmen als Grundvoraussetzung für einen reibungslosen Geschäftsablauf an[8]. Dies spiegelt sich auch in konkreten Maßnahmen wider. Seit 2020 sind die Ausgaben für das IT-Sicherheitsbudget in Unternehmen kontinuierlich gestiegen. Das Statistische Bundesamt geht von einer jährlichen Wachstumsrate von 10,5 Prozent aus[9]. 2022 wurde mit rund 7,8 Milliarden Euro so viel wie noch nie in Cybersicherheit investiert.

Gleichwohl sind weitere Schritte hin zu mehr Cybersicherheit dringend notwendig. Nach Schätzungen des Digitalverbandes Bitkom haben deutsche Unternehmen im Jahr 2022 einen Schaden von 203 Milliarden Euro[10] durch Cyberangriffe erlitten. Nahezu jedes deutsche Unternehmen sei dabei schon einmal von einem Angriff betroffen gewesen. Angesichts dieser Verluste ist eine Ausweitung der Cybersicherheitsmaßnahmen unerlässlich, auch wenn viele Unternehmen eine kontinuierliche Umsetzung von Cybersicherheitsmaßnahmen im laufenden Betrieb noch immer als Hemmnis empfinden[11].

Gestiegene Bedrohungslage

Die Corona-Pandemie hat einerseits die Digitalisierung in deutschen Unternehmen stark beschleunigt, andererseits neue Angriffsflächen geschaffen. Zudem erleben viele Unternehmen den russischen Angriffskrieg auf die Ukraine und die sich verändernde globale Sicherheitsarchitektur als große Herausforderungen. Obwohl diese Unsicherheit besteht, kann das BSI, wie bereits im Kapitel *Advanced Persistent Threats* und Bedrohungen im Kontext des Ukraine-Kriegs (Seite 25) beleuchtet wurde, aufgrund der vorliegenden Erkenntnisse keine gesteigerte Bedrohung im Kontext des Ukraine-Kriegs auf deutsche Unternehmen feststellen.

Wirklich angespannt wird die Bedrohungslage für Unternehmen durch finanziell motivierte Cyberangriffe. Die größte Bedrohung für Wirtschaftsunternehmen besteht nach wie vor durch *Ransomware* und *Ransomware* as a Service (vgl. Kapitel *Ransomware*, Seite 14). Es zeigt sich eine fortschreitende Professionalisierung, gekoppelt mit einer Eskalationsspirale an Maßnahmen, um Druck auf die erpressten Unternehmen auszuüben. Längst wird das betroffene System nicht nur verschlüsselt. Es ist mittlerweile gängige Praxis, dass die Täter im nächsten Schritt dem betroffenen Unternehmen und im dritten Schritt (Triple Extortion) auch dessen Kunden mit der Veröffentlichung der Daten drohen. Damit werden Unbeteiligte, deren Systeme nicht betroffen waren, ebenfalls zu Opfern.

Unter den bekannt gewordenen *Ransomware*-Opfern stachen im aktuellen Berichtszeitraum IT-Dienstleister hervor. Von den insgesamt 68 bekannt gewordenen Opfern von *Ransomware*-Angriffen waren 15 IT-Dienstleister. Für Angreifer stellen IT-Dienstleister hochattraktive Opfer dar, da über deren Dienstleistungen oder Kundenbeziehungen potenziell eine Vielzahl weiterer Opfer angegriffen und erpressbar gemacht werden kann (vgl. Vorfall *Cyberangriffe auf IT-Dienstleister*, Seite 57).

Cybercrime-Schattenwirtschaft

Die Angriffe auf Wirtschaftsunternehmen sind breit gestreut. Einerseits werden nach wie vor umsatzstarke Großunternehmen angegriffen. Gleichzeitig werden *Ransomware*-Angriffe aufgrund der niedrigen Kosten durch *RaaS* auch zum Massengeschäft. Dabei gehen die Kriminellen den Weg des geringsten Wiederstandes, sodass jetzt zunehmend die kleinen und mittleren Unternehmen (KMU), aber auch Kommunen, Universitäten und Forschungseinrichtungen stärker betroffen sind.

Das BSI beobachtet in dieser Professionalisierung den Aufbau einer Cybercrime-Schattenwirtschaft (siehe auch Kapitel *Ransomware*, Seite 14). Unternehmen stehen keinem einzelnen Angreifer, sondern einer arbeitsteiligen und effizient aufgestellten Angreiferindustrie gegenüber.

Gleichzeitig führt die zunehmende Spezialisierung auch zu einer neuen Stufe der Bedrohung. Mit gut gemachten Angriffen wird eine höchstmögliche Zahl von Unternehmensnetzwerken erreichbar – mittlerweile sogar ohne dass der *Angriffsvektor* im betroffenen Unternehmen war. Diese neue Bedrohungsqualität wird beispielsweise anhand des Sicherheitsvorfalls bei einem Anbieter von VoIP-Software im März 2023 deutlich. Hier waren durch einen doppelten Lieferkettenangriff potenziell rund 600.000 Unternehmen über eine mit einem gültigen 3CX-Zertifikat signierte Anwendung bedroht (vgl. Vorfall *Cyberangriffe auf IT-Dienstleister,* Seite 57).

Bekannt gewordene *Ransomware*-Opfer in Deutschland im Berichtszeitraum nach Art des Opfers
Anzahl

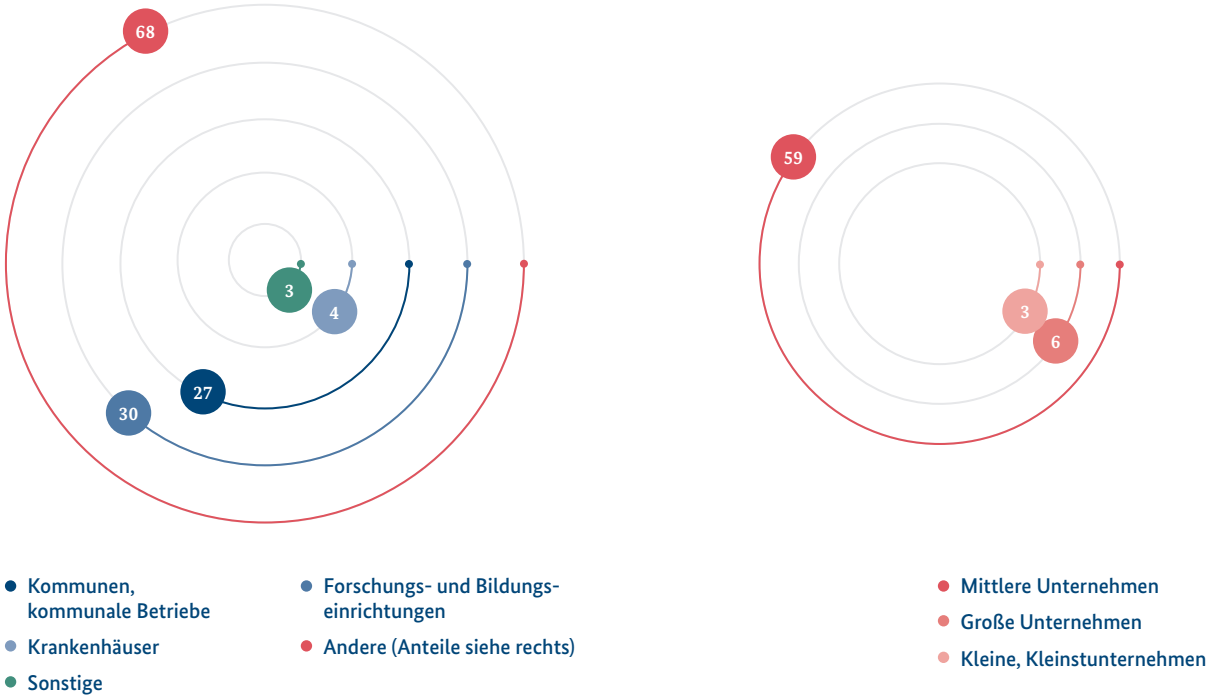


Abbildung 16: Bekannt gewordene *Ransomware*-Opfer in Deutschland
Quelle: *Ransomware*-Opfer-Statistik des BSI

Ein starker Schutzschild: Cyberresilienz

Um sich in dieser Bedrohungslage gut aufzustellen, ist es notwendig, dass Unternehmen jetzt in ihre Cyberresilienz investieren. Dazu gehören technische und organisatorische Maßnahmen wie regelmäßige Sicherheitsupdates, *Backups* und Schulungen der Mitarbeitenden. Während große Unternehmen hier in der Regel gut aufgestellt sind, haben KMU meist noch dringenden Nachholbedarf. So geben beispielsweise laut einer Umfrage der DIHK nur 61 Prozent der Kleinstunternehmen an, regelmäßig *Backups* zu machen (vgl. Kapitel *Besondere Situation von KMU in Deutschland*, Seite 64). Wenn es um das Erstellen von Notfallplänen geht, haben sowohl große als auch kleinere Unternehmen noch Nachholbedarf. Weniger als ein Drittel der Unternehmen verfügt über einen schriftlich fixierten Notfallplan. Das BSI bietet hier für die Zielgruppe KMU mit dem „Maßnahmenkatalog Notfallmanagement“ und einem Einseiter einen leichten Einstieg in das Notfallmanagement.

Ebenso wichtig wie Maßnahmen zur Steigerung der *Resilienz* ist auch das regelmäßige Einüben der getroffenen Maßnahmen. Ein *Backup* ist nur dann hilfreich, wenn es auch wieder eingespielt werden kann. Ein weiterer wesentlicher Faktor sind der Austausch und die Kommunikation über Sicherheitsvorfälle. Immer mehr Unternehmen gehen transparent mit einem Vorfall um und informieren die Öffentlichkeit und ihre Kundinnen und Kunden. Dies trägt dazu bei, dass potenzielle Schwachstellen schneller behoben und Schäden von weiteren Unternehmen abgewendet werden können.

Das BSI bietet mit seinen Angeboten für die Wirtschaft und dem Netzwerk der Allianz für Cybersicherheit zahlreiche Unterstützungs-angebote, damit Unternehmen resilienter werden und einen starken Schutzschild für mehr Cybersicherheit aufbauen können.

Den Maßnahmenkatalog des BSI für Unternehmen finden Sie hier:[h]

Weiterführende Informationen für Unternehmen finden Sie hier:[i]

Cyberangriffe auf IT-Dienstleister

Sachverhalt
Im Berichtszeitraum wurden mehrere Ransomware-Angriffe auf deutsche IT-Dienstleister bekannt. Betroffen waren neben den IT-Dienstleistern selbst häufig auch deren Kunden, sowohl in der öffentlichen Verwaltung als auch in Wirtschaft und Gesellschaft. So wurden neben verschiedenen Kommunalverwaltungen beispielsweise auch soziale und gemeinnützige Einrichtungen beeinträchtigt.

Die Arbeitsfähigkeit der betroffenen IT-Dienstleister wurde durch die Angriffe eingeschränkt. Für Kunden entwickelte Software konnte entweder nicht weiterentwickelt oder nicht ausgeliefert werden. Zudem wurde die Arbeitsfähigkeit der Kunden der betroffenen Dienstleister ebenfalls teilweise stark eingeschränkt.

Bewertung
IT-Dienstleister stellen für Cyberkriminelle besonders interessante Ziele dar, da Angriffe auf einen einzelnen Dienstleister Schadwirkungen bei zahlreichen Opfern zur Folge haben können und der Erpressungsdruck damit vergleichsweise hoch ist. Das BSI empfiehlt grundsätzlich, keine Lösegelder oder Schweigegelder zu zahlen.

Industrie- und Handelskammern nach Cyberangriff deutschlandweit offline

Sachverhalt
Der IT-Dienstleister der Industrie- und Handelskammern entdeckte am 3. August 2022 ein auffälliges Verhalten in den bei ihm gehosteten IT-Systemen. Das IHK Cyber Emergency Response Team (IHK-CERT) hat diese Anomalien untersucht. In Zusammenarbeit mit externen IT-Sicherheitsfachleuten wurde entschieden, die Systeme aus Sicherheitsgründen herunterzufahren, um größeren Schaden durch Diebstahl von Daten oder die mögliche Verschlüsselung von Daten zu verhindern.

Dies hatte zur Folge, dass die Verbindung aller 79 Industrie- und Handelskammern in Deutschland zum Internet getrennt wurde und deren Dienste nicht mehr zur Verfügung standen. Dadurch waren Webseiten offline und die Mitarbeitenden weder telefonisch noch per E-Mail erreichbar. Auch interne Anwendungen funktionierten nicht oder nur mit Einschränkungen.

Bewertung
Der Cyberangriff wurde höchstwahrscheinlich von professionellen Angreifern ausgeführt. Deren Vorgehensweise deutet auf Spionage- oder Sabotage-Ziele hin, auch wenn sich eine finanziell ausgerichtete Motivation der Angreifer nicht ausschließen lässt.

Reaktion
Um das Risiko weiterer Angriffe und möglicher Kompromittierungen zu verringern, wurden sämtliche Anwendungen und IT-Systeme erst nach einer intensiven Prüfung schrittweise wieder hochgefahren. Einzelne Kammern und verschiedene Dienstleistungen der Organisation waren auch Monate später noch beeinträchtigt.

8.1 — Gefährdungslage Kritischer Infrastrukturen

Kritische Infrastrukturen sind Organisationen mit wichtiger Bedeutung für das Gemeinwesen. Die Betreiber Kritischer Infrastrukturen erbringen für die Bevölkerung kritische Dienstleistungen wie die Versorgung mit Strom, Wasser oder Lebensmitteln. Zu den kritischen Dienstleistungen zählen darüber hinaus unter anderem der öffentliche Nahverkehr, die Bargeldversorgung und die medizinische Versorgung. Kritische Infrastrukturen bilden eine entscheidende Grundlage für das Funktionieren unserer Gesellschaft. Dennoch erkennt man ihre Bedeutung gelegentlich erst, wenn es zu Störungen kommt.

„Kritische Infrastrukturen sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“ (KRITIS-Definition der Bundesressorts)

Alle kritischen Dienstleistungen sind ganz besonders von einer störungsfrei arbeitenden IT abhängig. Daher sieht das BSI-Gesetz (BSIG) für KRITIS-Betreiber Maßnahmen zur Prävention (§ 8a BSIG) und zur Bewältigung (§ 8b BSIG) von IT-Sicherheitsvorfällen oder IT-Störungen vor.

Bedrohung und Bewältigung

Bei Betreibern Kritischer Infrastrukturen können erfolgreiche Angriffe auf die IT-Infrastruktur nicht nur zu Schäden beim Unternehmen selbst führen, sondern sie wirken sich auch auf die Versorgung der Bevölkerung mit kritischen Dienstleistungen und damit auf die Daseinsvorsorge aus. Umso wichtiger ist es, dass Betreiber und staatliche Stellen zusammenarbeiten, um Angriffe zu verhindern oder Auswirkungen zu mildern.

Betreiber Kritischer Infrastrukturen im Sinne des BSIG sind verpflichtet, Vorfälle dem BSI zu melden. So meldete zum Beispiel ein Klinikum im Mai 2023 einen Vorfall und arbeitete zudem mit dem zuständigen Landeskriminalamt zusammen, um die Lage zu bewältigen. Es wäre aber wünschenswert, dass sich auch Betreiber Kritischer Infrastrukturen, die wegen der Unterschreitung der Schwellenwerte laut BSI-KritisV nicht unter die Regelungen des BSIG fallen, bei entsprechenden Vorfällen an staatliche Stellen wenden. Der hierfür notwendige Vertrauensaufbau kann insbesondere in der öffentlich-privaten Kooperation UP KRITIS (vgl. Kapitel *Nicht regulierte KRITIS-Wirtschaft: UP KRITIS*, Seite 60) erfolgen und Vorteile für alle Seiten bieten. Das BSI ist grundsätzlich für alle Betreiber Kritischer Infrastrukturen ansprechbar und rät dazu, den Kontakt zu staatlichen Stellen bereits zu suchen, bevor etwas passiert. So lässt sich im Fall der Fälle einfacher und vertrauensvoller zusammenarbeiten und ein schwerer IT-Vorfall gemeinsam bewältigen, bevor er sich zur Krise ausweitet.

Die Lage im Sektor Gesundheit

Die Auswertung von Vorfallsmeldungen aus dem Bereich medizinische Versorgung zeigt eine hohe Bereitschaft der Betreiber, ihre Vorfälle an das BSI zu melden. Die Meldungen sind für die Erstellung eines detaillierten Lagebilds durch das BSI entscheidend und bilden die Basis für zielgruppenorientierte Warn- und Informationsmeldungen, die das BSI den regulierten Betreibern Kritischer Infrastrukturen und den Teilnehmern des *UP KRITIS* zur Verfügung stellt.

Hierzu werden die Meldungen durch das BSI sanitarisiert, das heißt, schutzbedürftige Informationen werden aus einer Meldung entfernt, während die für andere Betreiber relevanten Informationen bestehen bleiben.

Fast die Hälfte der eingegangenen Meldungen aus dem Sektor Gesundheit zeigten einen Ausfall oder eine Beeinträchtigung der durch den Betreiber erbrachten kritischen Dienstleistung an. Als Grund für die Störungen wurde in den meisten Fällen technisches Versagen angegeben. Dies korreliert mit den in den turnusmäßigen Nachweisen gemäß § 8a Abs. 3 BSIG festgestellten Mängeln: Die meisten Mängel im Sektor Gesundheit betreffen den Bereich „Technische Informationssicherheit“.

In etwa 20 Prozent der Meldungen aus dem KRITIS-Sektor Gesundheit spielten Angriffe eine Rolle. Bei diesen lässt sich ein zunehmender Fokus auf die Dienstleister der Betreiber als Einfallstor feststellen: Anstatt KRITIS-Betreiber und Behörden direkt anzugreifen, zielen diese sogenannten Supply-Chain-Angriffe auf Anbieter, Lieferanten und damit auf die etablierten Lieferketten ab. Indem Produkte bereits bei den Herstellern oder Drittanbietern kompromittiert werden, beschränkt sich der mögliche Schaden nicht nur auf das angegriffene Unternehmen selbst, sondern betrifft alle in der Wertschöpfungskette nachgelagerten Unternehmen. Dieser Multiplikatoreffekt macht Supply-Chain-Angriffe für Kriminelle besonders lukrativ, was das vermehrte Auf-

treten solcher Attacken erklären kann. Der beschriebene Trend ist nicht auf den Sektor Gesundheit beschränkt. Auch Betreiber in anderen Sektoren sind grundsätzlich Angriffen auf Lieferketten ausgesetzt, mit denen zahlreiche etablierte Maßnahmen der Prävention umgangen werden können.

In Prüfungen nach § 8a Abs. 4 BSIG hat das BSI mehrfach festgestellt, dass die Beziehungen zwischen Betreibern und Dienstleistern so gestaltet sind, dass die Betreiber ihrer Verantwortung in Bezug auf einen angemessenen IT-Schutz nicht ausreichend nachkommen können. Denn auch bei Auslagerung von IT-Dienstleistungen verbleibt die Sicherheitsverantwortung beim KRITIS-Betreiber. Auch eine Risikobewertung der Dienstleisterbeziehung findet häufig nicht statt. So ist manchmal unklar, wer welchen Teil der Betreiberverantwortung übernimmt und ob die getroffenen Maßnahmen tatsächlich ausreichen.

Gesetzliche Verpflichtung zum Einsatz von Systemen zur Angriffserkennung

Betreiber Kritischer Infrastrukturen sind verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen. Mit dem *IT-Sicherheitsgesetz 2.0* wurde für KRITIS-Betreiber im Mai 2021 ausdrücklich der Einsatz von Systemen zur Angriffserkennung im BSIG vorgeschrieben (§ 8a Abs. 1a BSIG). Diese Systeme stellen eine effektive Maßnahme zur Erkennung von Cyberangriffen dar und unterstützen insbesondere die Schadensreduktion. Die Betreiber mussten die Einführung eines Systems zur Angriffserkennung erstmalig bis zum 1. Mai 2023 gegenüber dem BSI nachweisen. Die gesetzliche Verpflichtung betrifft aber nicht nur KRITIS-Betreiber, die die Schwellenwerte der BSI-KritisV überschreiten, sondern über § 11 Abs. 1d Energiewirtschaftsgesetz (EnWG) auch alle Strom- und Gasnetzbetreiber.

Insbesondere gegen die Bedrohung durch *Ransomware* bietet ein effektives System zur Angriffserkennung zusätzlichen Schutz. Solche Systeme ermöglichen es, einen Angreifer zu entdecken, der bereits im Netzwerk ist, aber noch nicht mit der Verschlüsselung begonnen hat. Zudem ermöglicht ein frühzeitiges Erkennen, die gewonnenen Erkenntnisse über den Angreifer oder den *Angriffsvektor* mit anderen Einrichtungen zu teilen und so zum kollektiven Schutz beizutragen.

Neue EU-Richtlinien zum Schutz Kritischer Infrastrukturen und weiterer kritischer Einrichtungen

Am 16. Januar 2023 sind zwei Richtlinien der EU in Kraft getreten:

- die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union mit Fokus auf IT-Sicherheit (NIS-2-Richtlinie, Network Information Security)[12]
- die Richtlinie über die *Resilienz* kritischer Einrichtungen mit Fokus auf physische Sicherheit (CER-Richtlinie, Critical Entities Resilience)[13]

Diese Richtlinien müssen in den Mitgliedsstaaten bis zum 17. Oktober 2024 in nationales Recht umgesetzt werden. Beide Richtlinien haben unter anderem zum Ziel, dass kritische Einrichtungen einheitlich besser vor Cyberangriffen, Sabotage und Naturgefahren geschützt werden. Hierbei wird auch in Deutschland der Kreis der durch gesetzliche Regulierung erfassten Einrichtungen erheblich ausgeweitet. Dies wird nicht nur bei den betroffenen Unternehmen zu verstärkten Investitionen in die Cybersicherheit führen, sondern auch für das BSI als Aufsichtsbehörde zahlreiche zusätzliche Aufgaben mit sich bringen.

Zahl der regulierten Unternehmen wird stark ansteigen

Derzeit sind Anforderungen an die Cybersicherheit Kritischer Infrastrukturen in Deutschland in erster Linie durch das BSI-Gesetz mit der zugehörigen BSI-KritisV festgelegt. Durch die beiden EU-Richtlinien werden zukünftig sowohl der Kreis der regulierten Unternehmen als auch die Anforderungen an diese erweitert. Für die EU werden harmonisierte Vorgaben zum Schutz von wichtigen, besonders wichtigen und kritischen Einrichtungen vor Cybersicherheits- und physischen Bedrohungen verpflichtend. Die von den Richtlinien erfassten Sektoren sind zu einem Großteil mit denen des § 2 Abs. 10 BSIG in Verbindung mit der BSI-KritisV identisch (vgl. Tabelle 2).

NIS-2-Richtlinie – Stärkung der Cybersicherheit der wichtigen und besonders wichtigen Einrichtungen

Durch ihren Fokus ist die NIS-2-Richtlinie für die IT-Sicherheit und deren regulatorischen Rahmen von besonderer Bedeutung. Sie ist die Fortentwicklung der ersten NIS-Richtlinie, die im August 2016 in Kraft getreten ist. Angesichts der gestiegenen Bedrohung, insbesondere durch Cyberangriffe, die mit der stark zunehmenden

KRITIS nach nat. KRITIS-Strategie	KRITIS gemäß §2 (10) BSIG	NIS-2-Richtlinie	CER-Richtlinie
Energie	Energie	Energie	Energie
Transport und Verkehr	Transport und Verkehr	Verkehr	Verkehr
Finanz- und Versicherungswesen	Finanz- und Versicherungswesen	Bankwesen und Finanzmarktinfrastrukturen	Bankwesen und Finanzmarktinfrastrukturen
Gesundheit	Gesundheit	Gesundheit	Gesundheit
Wasser	Wasser	Wasser	Wasser
Informationstechnik und Telekommunikation	Informationstechnik und Telekommunikation	Digitale Infrastruktur, Verwaltung von IKT-Diensten	Digitale Infrastruktur
Ernährung	Ernährung	–	Ernährung
Siedlungsabfallentsorgung	Siedlungsabfallentsorgung	–	–
Medien und Kultur	–	–	–
–	–	Weltraum	Weltraum
Staat und Verwaltung	–	Öffentliche Verwaltung	Öffentliche Verwaltung

Tabelle 2: KRITIS-Sektoren nach der nationalen KRITIS-Strategie, dem BSI-Gesetz und den aktuellen EU-Richtlinien
Quelle: BSI

Digitalisierung in allen Bereichen der Wirtschaft und bei staatlichen Einrichtungen einhergehen, weitet die NIS-2-Richtlinie Vorgaben zur Cybersicherheit auf mehr Sektoren und mehr Unternehmen aus. Sie legt Sicherheitsanforderungen für eine deutlich größere Zahl von Unternehmen fest, als bisher durch die BSI-KritisV erfasst wurden, und erweitert den Handlungsrahmen zur Durchsetzung der gesetzlichen Anforderungen. Zusätzlich werden Teilen der öffentlichen Verwaltung entsprechende Pflichten auferlegt.

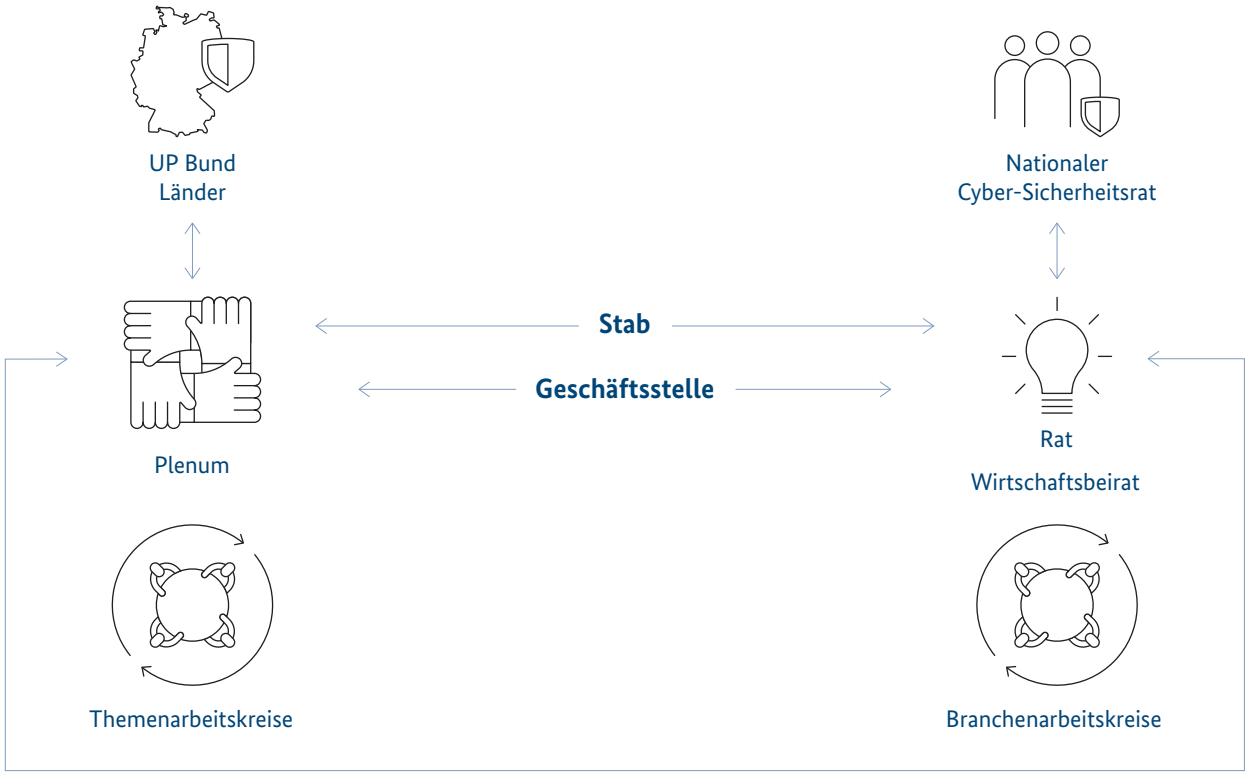
Ein wichtiges Merkmal in der NIS-2-Richtlinie ist die Unterscheidung zwischen wichtigen und besonders wichtigen Einrichtungen. Für besonders wichtige Einrichtungen gelten im Hinblick auf den Umfang der staatlichen Aufsicht schärfere Vorschriften als für wichtige Einrichtungen. Die Anzahl Letzterer ist dafür deutlich größer. Die heute bereits nach BSIG regulierten Kritischen Infrastrukturen gehören in aller Regel zu den besonders wichtigen Einrichtungen im Sinne der NIS-2-Richtlinie. Die in der NIS-2-Richtlinie adressierten Sektoren gehen jedoch über die KRITIS-Sektoren aus dem BSIG hinaus. Für wichtige und besonders wichtige Einrichtungen, einschließlich bisheriger Betreiber Kritischer Infrastrukturen, ist daher mit veränderten Pflichten und Anforderungen aus der Umsetzung der NIS-2-Richtlinie in nationales Recht zu rechnen.

8.1.1 — Kooperation zwischen Staat und KRITIS-Wirtschaft: *UP KRITIS*

Im *UP KRITIS* arbeiten KRITIS-Betreiber, deren Fachverbände und die zuständigen Behörden zusammen, um die Kritischen Infrastrukturen in Deutschland zu schützen. Teilnehmer im *UP KRITIS* können alle Betreiber Kritischer Infrastrukturen werden, auch wenn im Einzelfall die jeweiligen Schwellenwerte der BSI-KritisV nicht erreicht werden. Es nehmen mehr als 900 Organisationen am *UP KRITIS* teil (Stand: Juni 2023). Der fachliche Aus-

Gremien des *UP KRITIS*

Abbildung 17: Gremien des *UP KRITIS*



tausch erfolgt insbesondere in Themen- und Branchenarbeitskreisen. Die Selbstverwaltung des *UP KRITIS* geschieht über folgende Gremien:

- Rat – arbeitet auf politischer Ebene, besteht aus hochrangigen Personen aus den KRITIS-Sektoren sowie aus den Behörden Bundesministerium des Innern und für Heimat (BMI), Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BKK) und BSI,
- Plenum – in dieses Gremium entsenden alle Branchen- und Themenarbeitskreise einen Sprecher,
- Stab – der Arbeitskreis des Plenums, dessen Mitglieder im Plenum bestimmt werden,
- Geschäftsstelle – diese liegt im BSI und bearbeitet insbesondere Anmeldungen und übernimmt andere administrative Aufgaben.

Das BSI nimmt an den meisten Arbeitskreisen, dem Plenum, dem Stab und dem Rat des *UP KRITIS* teil (vgl. auch Abbildung 17: Gremien des *UP KRITIS).*

Im Berichtszeitraum gab es unter anderem folgende Entwicklungen im *UP KRITIS*:

- Der Themenarbeitskreis „Anforderungen an Lieferanten und Hersteller“ hat ein Papier mit Empfehlungen zu Entwicklung und Bereitstellung von in Kritischen Infrastrukturen eingesetzten Produkten veröffentlicht.
- Der Themenarbeitskreis „Auswirkungen Ukraine-Krise“ wurde umbenannt in „Auswirkungen aktueller Krisen und Ereignisse“.
- Der *UP KRITIS* hat folgende Gesetzesvorhaben begleitet: Änderungsverordnung zur BSI-KritisV, die NIS-2-Richtlinie, die CER-Richtlinie und das KRITIS-Dachgesetz. Es fanden erste Aktivitäten statt, um den *UP KRITIS* für das Inkrafttreten der neuen Gesetze umzugestalten.

Weiterführende Informationen finden Sie hier:[j]

8.1.2 — Anbieter digitaler Dienste

Im Zusammenhang mit dem russischen Angriffskrieg gegen die Ukraine ist auch die Cybersicherheit der Anbieter digitaler Dienste stärker in den Fokus gerückt. Zu ihnen zählen Online-Marktplätze, Online-Suchmaschinen und *Cloud*-Computing-Dienste. Diese werden nach § 8c BSIG reguliert.

Da bisher noch keine Registrierungspflicht für die Anbieter digitaler Dienste bestand, war es für regulierende Behörden wie das BSI in vielen Fällen schwierig, die Anbieter zu identifizieren und einen Kontakt zu etablieren, damit diese (analog zu den Betreibern Kritischer Infrastrukturen) BSI-Produkte, wie zum Beispiel Sicherheitswarnungen, erhalten.

Mit der Überarbeitung der NIS-Richtlinie wurde eine Registrierungspflicht für die Anbieter digitaler Dienste eingeführt. Hierdurch sollen eine bessere Sichtbarkeit von Sicherheitsvorfällen und der unmittelbare Kontakt zu den Anbietern in diesem Bereich gewährleistet werden.

Mit der NIS-2-Richtlinie werden darüber hinaus die *Cloud*-Computing-Dienste den besonders wichtigen Einrichtungen zugeordnet und unterliegen denselben Pflichten wie Betreiber Kritischer Infrastrukturen. Zusätzlich sind die Social-Media-Plattformen als neue Kategorie in den Kreis der Anbieter digitaler Dienste aufgenommen worden.

8.1.3 — Statistiken

Meldungen nach KRITIS-Sektoren (§ 8b Abs. 4 BSIG)

Mit dem IT-Sicherheitsgesetz wurde im Jahr 2015 in § 8b Abs. 4 BSIG eine Meldepflicht für Betreiber Kritischer Infrastrukturen eingeführt. Die Meldepflicht gilt für Störungen, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben oder führen können.

Im Berichtszeitraum gingen beim BSI 490 entsprechende Meldungen ein, die Verteilung auf die KRITIS-Sektoren zeigt Tabelle 3. Ein hohes Meldeaufkommen ist nicht zwangsläufig ein Indikator für den Stand der Informationssicherheit des jeweiligen Sektors. Betreiber Kritischer Infrastrukturen melden zum Teil auch Vorkommen, die unterhalb der gesetzlichen Meldeschwelle liegen, und tragen dadurch zum Lagebild bei. Die Anzahl der Meldungen entspricht nicht der Anzahl der Vorfälle, die gemeldet worden sind. Vorfälle, die über einen längeren Zeitraum andauern, beinhalten in der Regel eine Initialmeldung, ein oder mehrere aktualisierende Meldungen und eine Abschlussmeldung.

Sektor	Meldung
Energie:	99
Informationstechnik und Telekommunikation:	81
Transport und Verkehr:	111
Gesundheit:	132
Wasser:	16
Ernährung:	9
Finanz- und Versicherungswesen:	61
Siedlungsabfallentsorgung (neuer Sektor):	0
Gesamt:	490

Tabelle 3: Meldungszahlen nach KRITIS-Sektoren im Berichtszeitraum
Quelle: BSI

Reifegrade der Managementsysteme für Informationssicherheit und Geschäftskontinuität bei KRITIS-Betreibern

Betreiber Kritischer Infrastrukturen sind nach § 8a Abs. 3 BSIG gesetzlich verpflichtet, alle zwei Jahre gegenüber dem BSI nachzuweisen, dass ihre IT-Sicherheit auf dem aktuellen Stand der Technik ist. Diese Nachweise enthalten eine Einschätzung der prüfenden Stelle zur Wirksamkeit der Managementsysteme für Informationssicherheit (ISMS) und Geschäftskontinuität (Business Continuity Management System, BCMS) beim geprüften Betreiber. Dies geschieht mittels eines Reifegradmodells, das es ermöglicht, den Fortschritt von ISMS und BCMS im Hinblick auf die Sicherstellung der kritischen Dienstleistung nachvollziehbar über Prüfzyklen hinweg zu dokumentieren, ohne sich dabei auf Einzelmaßnahmen zu fokussieren.

Die Einteilung in Reifegrade orientiert sich an klassischen Reifegradmodellen. Eine Reifegradbestimmung nach wissenschaftlichen Methoden wird vom BSI jedoch nicht gefordert. Der attestierte Reifegrad stellt eine potenzielle Kennzahl zur Steuerung in einer Institution dar.

Die Orientierungshilfe zu Nachweisen gemäß § 8a Abs. 3 BSIG beschreibt folgende Reifegrade für ISMS und BCMS[14]:

ISMS-Reifegrad

Reifegrad 1 Ein ISMS ist zwar geplant, aber bisher nicht etabliert.
Reifegrad 2 Ein ISMS ist weitestgehend etabliert.
Reifegrad 3 Ein ISMS ist etabliert und dokumentiert.
Reifegrad 4 Zusätzlich zum Reifegrad 3 wurde das ISMS regelmäßig auf Effektivität überprüft.
Reifegrad 5 Zusätzlich zum Reifegrad 4 wurde das ISMS regelmäßig verbessert.

BCMS-Reifegrad

Reifegrad 1 Ein BCMS ist zwar geplant, aber bisher nicht etabliert.
Reifegrad 2 Ein BCMS ist weitestgehend etabliert.
Reifegrad 3 Ein BCMS ist etabliert und dokumentiert.
Reifegrad 4 Zusätzlich zum Reifegrad 3 wurde das BCMS regelmäßig überprüft und beübt.
Reifegrad 5 Zusätzlich zum Reifegrad 4 wurde das BCMS regelmäßig verbessert.

Die Reifegrade sind in den verschiedenen Sektoren Kritischer Infrastrukturen unterschiedlich ausgeprägt, was sich auch an den in den Nachweisen enthaltenen Mängeln der Managementsysteme ablesen lässt. Die erheblichen Unterschiede unter anderem in der Größe der Anlagen, der Abhängigkeit von IT und den Anforderungen verschiedener Aufsichtsregime führen jedoch dazu, dass eine Vergleichbarkeit über Sektorgrenzen hinaus regelmäßig nicht gegeben ist.

Sektor	ISMS-Reifegrad laut jeweils letztem vorliegenden Nachweis					BCMS-Reifegrad laut jeweils letztem vorliegenden Nachweis				
	Reifegrad					Reifegrad				
	1	2	3	4	5	1	2	3	4	5
Wasser	0	6	15	27	24	1	13	27	17	14
Energie	2	7	27	23	25	2	20	34	15	13
Transport und Verkehr	6	13	27	7	7	9	18	16	11	6
Finanz- und Versicherungswesen	1	5	33	19	29	1	24	19	23	20
IT und TK	0	5	6	9	11	3	6	7	7	8
Ernährung	0	8	20	5	9	4	8	20	6	4
Gesundheit	14	88	59	26	12	34	79	49	24	13
Insgesamt	23	132	187	116	117	54	168	172	103	78

Tabelle 4: ISMS-Reifegrade und BCMS-Reifegrade nach Sektoren
Quelle: BSI

BSI beobachtet fortwährend die Sicherheitslage der Kritischen Infrastrukturen in Deutschland

Die staatlichen und privatwirtschaftlichen Betreiber Kritischer Infrastrukturen tragen im Hinblick auf die Versorgung der Bevölkerung mit zum Teil lebensnotwendigen Dienstleistungen ein hohes Maß an Verantwortung für einen sicheren und störungsfreien Betrieb. Durch den russischen Angriffskrieg gegen die Ukraine steht die Sicherheit der Kritischen Infrastrukturen in Deutschland weiterhin im Fokus.

Auch im dritten Nachweiszyklus erreichen das BSI noch Nachweise mit Reifegraden 1 und 2. Durch die Überwachung der betreiberseitigen Mängelbeseitigung im Rahmen der Nachweisführung wirkt das BSI darauf hin, dass sich diese Situation kurzfristig verbessert, hin zu etablierten Managementsystemen. Auffällig ist darüber hinaus, dass trotz der Krisen, insbesondere der COVID-19-Pandemie und des Kriegs in der Ukraine, die BCMS-Reifegrade noch hinter den ISMS-Reifegraden zurückbleiben. Hier sieht das BSI dringenden Handlungsbedarf.

8.2 — Besondere Situation von KMU in Deutschland

2,6 Millionen kleine (weniger als 50 Mitarbeitende) und mittlere Unternehmen (50 bis 249 Mitarbeitende) in Deutschland stehen vor den Herausforderungen der Digitalisierung und damit einhergehend der Cybersicherheit. Dieser Teilbereich von Unternehmen, der zahlenmäßig 99,4 Prozent der deutschen Wirtschaftsunternehmen ausmacht, gliedert sich wie folgt auf:

Gerade die Kleinst- (weniger als zehn Mitarbeitende) und die kleinen Unternehmen verfügen oftmals nicht über das erforderliche Personal für den Betrieb und die Absicherung der Informationstechnik des Unternehmens. So ist ein kleiner Handwerksbetrieb, eine mittlere Steuerberatungs- oder Rechtsanwaltskanzlei, ein metallverarbeitender Betrieb oder ein Pflegedienst oft nicht in der Lage, dediziertes IT-Personal einzustellen. Im Rahmen der Entscheidung zwischen selber machen oder einkaufen („make or buy“) wird dabei häufig nach dem Ansatz gehandelt: „Das bekommen wir schon irgendwie selbst hin.“ Dem steht eine wachsende Bedrohungslage gegenüber.

Viele Unternehmen besitzen auch im Jahr 2023 weder eine ausreichende Kenntnis über die allgemeine Cyberbedrohungslage noch über das eigene Risikoprofil. Sie kommen daher überhaupt nicht auf die Idee, dass sie mehr in ihre Sicherheit investieren müssen. Selbst elementare und oftmals kostenfrei umsetzbare Präventionsmaßnahmen werden daher häufig nicht ergriffen. So installieren nur 62 Prozent der Kleinstunternehmen regelmäßig Sicherheitsupdates. Noch weniger (46 %) überlassen ihre IT-Sicherheit einem externen Dienstleister. Und einen Notfallplan besitzen gar nur 18 Prozent der Kleinstunternehmen[15]. Etwas mehr als die Hälfte der kleinen und der mittleren Unternehmen (51 %) geben als dominierende „IT-Sicherheitsbremse“ den Aufwand und die Kosten für den laufenden technischen Betrieb, Anpassungen und Aktualisierungen an. Nur für 28 Prozent ist der initiale Aufwand ein Hindernis. Dies deckt sich mit den Rückmeldungen von IT-Dienstleistern an das BSI[16].

Diejenigen KMU hingegen, die ein Problembewusstsein entwickelt haben und Personal einstellen möchten, erleben häufig, dass sie in einem Angebotsmarkt als potenzieller Arbeitgeber nicht gegen die Gehälter bei

Unternehmen in Deutschland nach Größe
Angabe in %

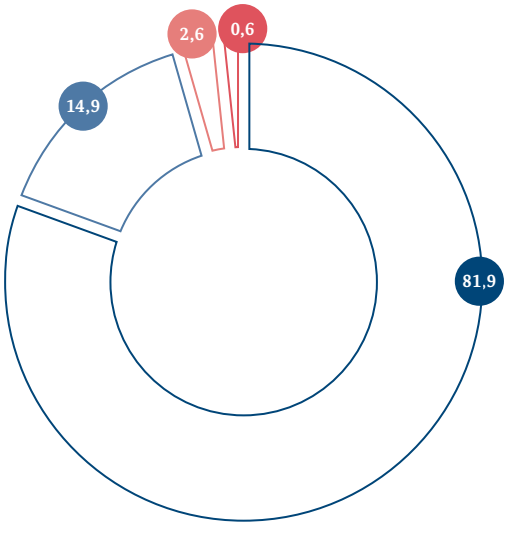


Abbildung 18: Unternehmen in Deutschland nach Größe
Quelle: Statistisches Bundesamt
Stand: Juli 2021

Großunternehmen oder IT-Dienstleistern bestehen können. Und diejenigen, die den Bereich IT/IT-Sicherheit an einen Dienstleister auslagern möchten, müssen häufig feststellen, dass es in ihrer Region entweder zu wenig qualifizierte Dienstleister gibt oder nur solche, die nicht zu ihrer eigenen Unternehmensgröße passen.

Dies alles führt dazu, dass KMU häufig zum Opfer Cyberkrimineller werden – und dann nicht wissen, was sie tun sollen. Eine im Auftrag des Bundesministeriums für Wirtschaft und Energie (jetzt Bundesministerium für Wirtschaft und Klimaschutz) im Jahr 2021 veröffentlichte Studie kam zu dem Ergebnis: „Im Ereignisfall wissen KMU oftmals nicht, an wen sie sich wenden können, um fachlich versierte Hilfe zu erhalten. Im Gegensatz zu Einbrüchen in der analogen Welt ist der digitale Schaden für viele KMU nicht immer und nicht unmittelbar ersichtlich. Die Hemmschwelle, Vorfälle und Angriffe an die Polizei, die Landeskriminalämter oder andere behördliche Stellen zu melden, ist hoch."[17]

Dementsprechend ist der Bereich Cyberkriminalität gegen KMU von einem großen Dunkelfeld geprägt, was es schwer macht, verlässliche Zahlen zu gewinnen. Weiter kommt die oben genannte Studie zu folgender Empfehlung: „Der Aufbau einer bundesweiten Notfall-Hotline für IT-Vorfälle mit zentraler Erreichbarkeit zur Vermittlung an regionale Ansprechstellen würde Abhilfe schaffen."

Notfall-Hotline

Aufgrund der Notwendigkeit einer solchen Hotline betreibt das BSI ein Service-Center. Dieses ist unter der Telefonnummer 0800 274 1000 kostenfrei zu erreichen. Von dort wird über das Cyber-Sicherheitsnetzwerk (CSN) bei Bedarf auch an regionale Ansprechstellen weitervermittelt, die vor Ort bei den Betroffenen helfen können.

Viele hilfreiche Tipps für KMU, inklusive eines Verzeichnisses von Dienstleistern, die im Notfall helfen können, und einer Möglichkeit, eine eigene Betroffenheit durch einen Cyberangriff an das BSI zu melden, finden sich hier:[k]

Im Ernstfall eine Notfall-Hotline kontaktieren zu können ist wichtig, wichtiger ist aber, durch präventive Maßnahmen zu verhindern, zum Opfer zu werden. Oft wissen KMU jedoch nicht, wie sie mehr für ihre IT-Sicherheit tun können. Bereits existierende Standardwerke zum Aufbau eines Managementsystems für Informationssicherheit, wie das IT-Grundschutz-Kompendium des BSI oder die Norm ISO/IEC 27001, eignen sich eher für Unternehmen, die einen eigenständigen IT-Betrieb haben. Dies trifft auf den überwiegenden Teil der Unternehmen mit weniger als 50 Beschäftigen jedoch nicht zu.

Durchführung des CyberRisikoChecks

Ein Angebot an KMU ist der vom BSI gemeinsam mit Partnern erarbeitete CyberRisikoCheck. Dabei befragt ein IT-Dienstleister ein Unternehmen in einem ein- bis zweistündigen Interview (in der Regel per Videokonferenz) zur IT-Sicherheit im Unternehmen. Darin werden 27 Anforderungen aus sechs Themenbereichen daraufhin überprüft, ob das Unternehmen sie erfüllt. Für die Antworten werden nach den Vorgaben der von einem Konsortium unter Leitung des BSI und des Bundesverbandes mittelständische Wirtschaft (BVMW) erstellten Richtlinie DIN-SPEC-Punkte vergeben. Als Ergebnis erhält das Unternehmen einen Bericht, der unter anderem die Punktzahl und für jede nicht erfüllte Anforderung eine Handlungsempfehlung enthält. Die Handlungsempfehlungen sind nach Dringlichkeit gegliedert und erhalten Hinweise darauf, welche staatlichen Fördermaßnahmen (auf Bundes-, Landes- und kommunaler Ebene) das jeweilige Unternehmen in Anspruch nehmen kann. Der CyberRisikoCheck ist keine IT-Sicherheitszertifizierung. Er ermöglicht einem Unternehmen jedoch eine Positionsbestimmung des eigenen IT-Sicherheitsniveaus und zeigt auf, welche konkreten Maßnahmen ein Unternehmen umsetzen beziehungsweise bei einem IT-Dienstleister beauftragen sollte.

Durch die anonymisierten Erhebungsdaten der CyberRisikoChecks kann das Nationale IT-Lagezentrum zukünftig erstmals auf valide Daten zur Cybersicherheit von KMU zurückgreifen und in die BSI-Berichte zur Cybersicherheitslage mit aufnehmen. Der CyberRisikoCheck trägt damit zur Weiterentwicklung präventiver Angebote von Bund, Ländern und Kommunen bei.

Weitere Informationen zum CyberRisikoCheck sowie eine Liste registrierter IT-Dienstleister, die den Check anbieten, finden sich hier:[l]

Darüber hinaus können Unternehmen Mitglied der von BSI und Bitkom e. V. gegründeten Public-Private-Partnership Allianz für Cybersicherheit werden, um von den zahlreichen Informationsangeboten der Mitglieder zu profitieren.

Einen guten Überblick über die wichtigsten IT-Sicherheitsmaßnahmen vermittelt die BSI-Broschüre „Cyber-Sicherheit für KMU – Die TOP 14 Fragen“.

9. — Erkenntnisse zur Gefährdungslage in Staat und Verwaltung

Staat und Verwaltung waren im Berichtszeitraum verstärkt Cyberangriffen ausgesetzt. Insbesondere hat sich in Deutschland das Phänomen des politisch motivierten Hacktivismus im Kontext des russischen Angriffskriegs gegen die Ukraine verstetigt. Von wenigen Ausnahmen abgesehen (vgl. Die Lage der IT-Sicherheit in Deutschland 2022, Seite 49ff) nutzten die prorussischen Hacktivisten *DDoS-Angriffe* (vgl. Vorfall *DDoS-Hacktivismus*, Seite 30). Da mit dieser Art Cyberangriff Internetdienste nur vorübergehend abgeschaltet werden können und keine tiefere Infiltration von IT-Systemen und Netzwerken stattfindet, können Angreifer damit nur begrenzten Schaden verursachen. Es ist daher davon auszugehen, dass es sich bei D*DoS*-Hacktivismus im Wesentlichen um ein Propaganda-Phänomen handelt, das Verunsicherung in der deutschen Gesellschaft verbreiten soll.

Demgegenüber hinterlassen Cyberangriffe mit *Ransomware* oder *Wiper*n nachhaltigen Schaden. Die Wiederherstellung betroffener Systeme nimmt viel Zeit in Anspruch und die betroffenen Behörden sind oft monatelang nur eingeschränkt arbeitsfähig.

9.1 — Bundesverwaltung

Tagtäglich sind die Regierungsnetze überwiegend ungezielten Massenangriffen aus dem Internet ausgesetzt, teilweise aber auch gezielt gegen die Bundesverwaltung gerichteten Angriffen. Zum Schutz der Regierungsnetze vor diesen Angriffen setzt das BSI eine Reihe sich gegenseitig ergänzender Maßnahmen ein.

Webfilter stellen eine präventive Komponente dar, die den Zugriff auf *maliziöse* Webseiten bzw. Webserver blockieren. So wird zum Beispiel der Zugriff auf Schadprogramme verhindert, die sich hinter Download-Links verstecken, welche im Rahmen von Social-Engineering-Angriffen über E-Mail, Social Media oder Webseiten verbreitet werden. Auch die Kommunikation von Schadsoftware mit den entsprechenden Webservern, zum Beispiel zum Nachladen von weiteren Komponenten oder Befehlen, wird unterbunden. Im aktuellen Berichtszeitraum wurden täglich durchschnittlich gut 370 *maliziöse* Webseiten neu gesperrt.

Antivirus-Schutzmaßnahmen verhindern die Zustellung von direkt in E-Mail-Anhängen versendeten Schadprogrammen. Dies betraf im Berichtszeitraum durchschnittlich täglich rund 775 E-Mails. Rund 82 E-Mails pro

Spam-Mail-Index für die Bundesverwaltung*
2018=100

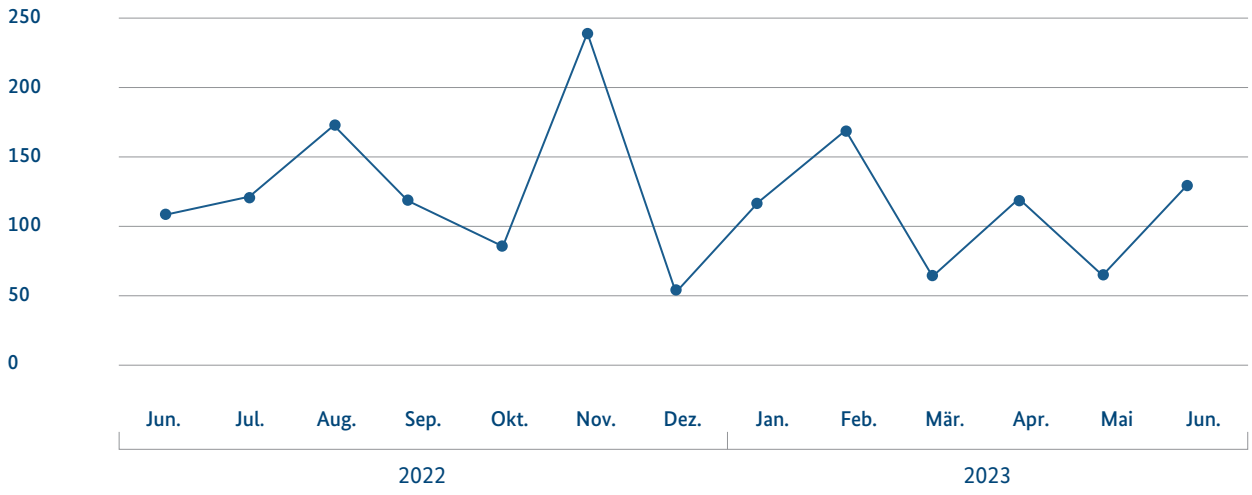


Abbildung 19: Spam-Mail-Index für die Bundesverwaltung
Quelle: Erhebung über den E-Mail-Verkehr mit der Bundesverwaltung (BSI)

*Ohne Spam-Mails an Behörden, die nicht an den zentralen Schutzmaßnahmen des BSI teilnehmen

Tag wurden ausschließlich auf Basis eigens durch das BSI erstellter Antivirus-Signaturen als schädlich identifiziert.

Insbesondere um gezielte Angriffe auf die Bundesverwaltung erkennen zu können, betreibt das BSI zusätzlich zu den bereits beschriebenen Maßnahmen ein System zur Detektion von Schadprogrammen im Datenverkehr der Regierungsnetze. Mit einer Kombination von automatisierten Testverfahren und manueller Analyse konnten die Analystinnen und Analysten des BSI durchschnittlich weitere gut 78 Angriffe pro Tag identifizieren, die weder durch eine kommerzielle noch durch eine der oben genannten automatisierten Lösungen erkannt wurden.

Ergänzend wird die Sicherheit der Regierungsnetze mit einem zentralen Schutz vor *Spam*-E-Mails erhöht. Diese Maßnahme wirkt nicht nur gegen unerwünschte Werbe-E-Mails. Auch Cyberangriffe wie *Phishing*-E-Mails werden damit erkannt. Die *Spam*-Quote, also der Anteil unerwünschter E-Mails an allen eingegangenen E-Mails, lag im Berichtszeitraum bei durchschnittlich 58 Prozent. Aufkommen und Entwicklung der *Spam*-E-Mails in den Netzen des Bundes werden durch den *Spam*-Mail-Index gemessen. Dieser erreichte im Berichtszeitraum durchschnittlich 124 Punkte. Das war ein Plus von rund zwölf Prozent im Vergleich zum vergangenen Berichtszeitraum (111 Punkte).

Dabei waren erhebliche Schwankungen zu verzeichnen. Während das *Spam*-Aufkommen im Sommer 2022 auf durchschnittlichem Niveau lag, stiegen die Index-Werte im November 2022 erheblich an. Die *Spam*-Filter der Bundesverwaltung wehren solche *Spam*-Wellen zuverlässig ab, sodass sie die adressierten Nutzerinnen und Nutzer nicht erreichen.

9.2 — Landes- und Kommunalverwaltungen

Landes- und Kommunalverwaltungen wurden im Berichtszeitraum verstärkt Opfer cyberkrimineller *Ransomware*-Angriffe.

Im aktuellen Berichtszeitraum wurden monatlich durchschnittlich zwei Kommunalverwaltungen oder kommunale Betriebe als Opfer von *Ransomware*-Angriffen bekannt (vgl. Vorfall *Ransomware-Angriffe auf Kommunalverwaltungen und kommunale Versorgungsbetriebe*, Seite 69). Damit waren sie überproportional häufig von *Ransomware*-Angriffen betroffen (vgl. auch Abb. 16, Seite 56).

Wie inzwischen üblich wurden dabei nicht nur Server verschlüsselt, sondern auch Daten von Bürgerinnen und Bürgern ausgeleitet und teilweise auch auf Leak-Seiten veröffentlicht. Betroffen waren unter anderem ganze Verzeichnisse, die die Akten von Einzelpersonen enthielten. Die betroffenen Verwaltungen waren in der Regel mehrere Tage bis hin zu mehreren Wochen nicht in der Lage, ihre bürger- und wirtschaftsnahen Verwaltungsdienstleistungen zu erbringen, und teils noch Monate später beeinträchtigt.

Während Bundesbehörden separat gesicherte Regierungsnetze mit zentralen Abwehrmaßnahmen zur Verfügung stehen, gestalten die Behörden der Kommunen ihre IT-Sicherheitsmaßnahmen unterschiedlich. Derzeit bestehen keine bundesweit einheitlichen Vorgaben bezüglich IT-Sicherheit oder Meldepflichten zu IT-Sicherheitsvorfällen auf Kommunalebene.

Auch Bildungs- und Forschungseinrichtungen gerieten im aktuellen Berichtszeitraum zunehmend ins Visier von *Ransomware*-Angreifern (vgl. Vorfall *Ransomware-Angriffe auf Bildungs- und Forschungseinrichtungen*, Seite 69).

Ransomware-Angriffe auf Kommunalverwaltungen und kommunale Versorgungsbetriebe

Im Berichtszeitraum wurden insgesamt 27 kommunale Verwaltungen und Betriebe als Opfer von Ransomware-Angriffen bekannt. Betroffen waren Kommunen jeder Art und Größe: von einer ländlichen Gemeinde mit 2.800 Einwohnerinnen und Einwohnern bis hin zu einer Großstadt mit mehr als 1,8 Millionen Einwohnerinnen und Einwohnern. Insgesamt hatten die betroffenen Kommunen knapp sechs Millionen Einwohnerinnen und Einwohner. Häufig waren die Stadt- oder Kreisverwaltungen direkt betroffen; jedoch wurden auch Nahverkehrsbetriebe, städtische Energieversorger oder Wohnungsbaugesellschaften, Stadtreinigungsbetriebe und ein Schulamt mit Zuständigkeit für 75 Schulen angegriffen. Selbst der Friedhofsbetrieb einer deutschen Großstadt blieb nicht verschont. Im Juni 2022 mussten nach einem besonders weitreichenden Ransomware-Angriff alle Rathäuser eines ganzen Landkreises sowie mehrere kommunale Betriebe einer angrenzenden kreisfreien Großstadt, darunter der Betrieb für den Nahverkehr, vom Internet getrennt werden.

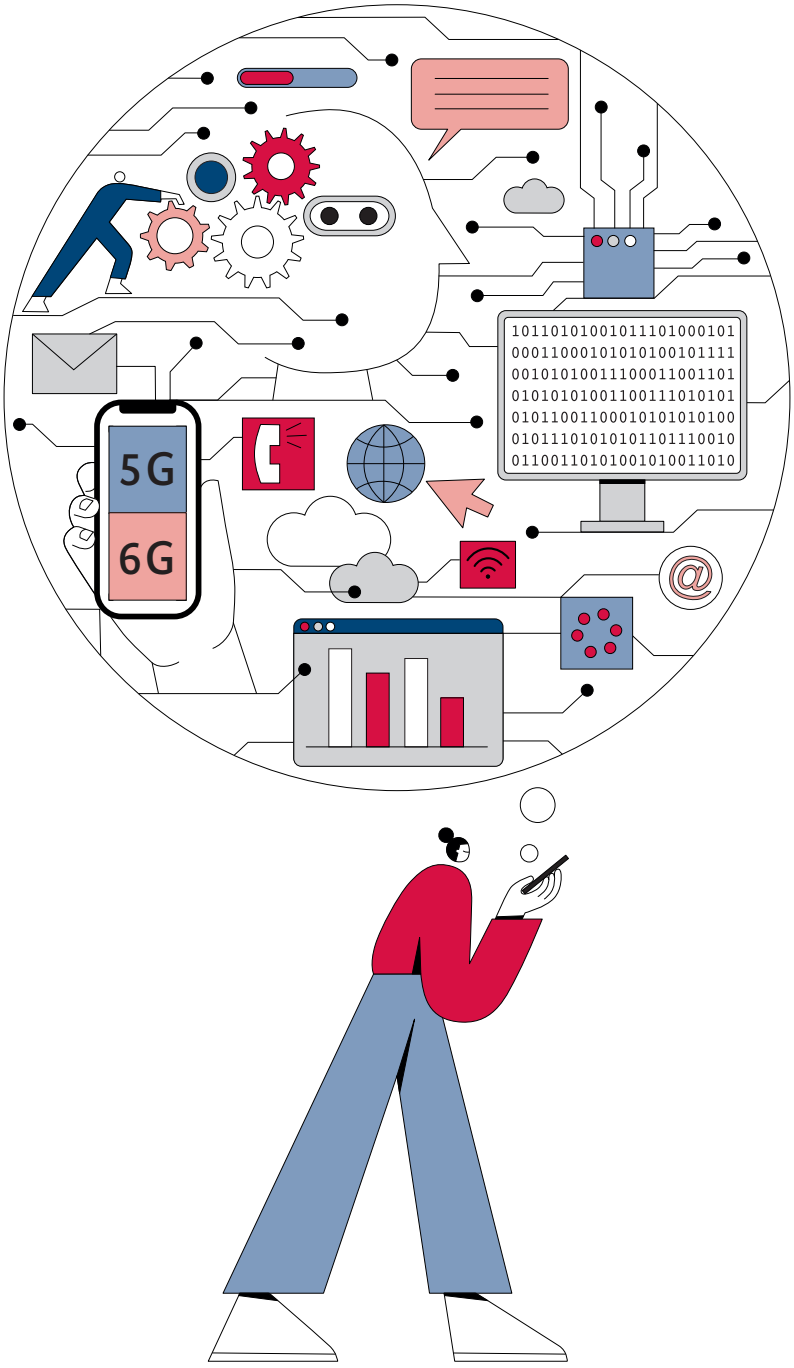
Auch wenn sich die Angreifergruppierungen, die ausgenutzten Schwachstellen und die eingesetzten RaaS im Detail unterschieden, waren die Abläufe doch meist gleich: Nach der Erstinfektion folgte das Auskundschaften der befallenen Systeme und die Verschlüsselung von Daten. Anschließend fanden sich die Opfer mit einer Lösegeldforderung konfrontiert. Die Opfer mussten ihre Systeme vollständig herunterfahren und vom Internet trennen, um weiteren Schaden und fortschreitende Verschlüsselung in ihren Netzwerken zu verhindern. Die Bereinigung der Systeme und die vollständige Wiederherstellung der Arbeitsfähigkeit nahmen oft Monate in Anspruch.

Das BSI empfiehlt, neben den verfügbaren Maßnahmen zur Abwehr von Ransomware-Angriffen das IT-Grundschutzprofil „Basis-Absicherung Kommunalverwaltung“ umzusetzen und dabei die Unterstützungsangebote des BSI zum leichteren Einstieg in die Informationssicherheit zu nutzen, wie zum Beispiel die neu erarbeiteten Checklisten zum „Weg in die Basis-Absicherung – WiBA“. Mit Hilfe der Checklisten ist eine erste Bestandsaufnahme der Informationssicherheit und die nahtlose Umsetzung des oben genannten Profils möglich. Langfristig sollte das Niveau der zertifizierungsfähigen Standard-Absicherung angestrebt werden.

Ransomware-Angriffe auf Bildungs- und Forschungseinrichtungen

Dass Universitäten für Cyberangreifer attraktive Opfer darstellen, ist bereits seit einigen Jahren bekannt (vgl. zum Beispiel den Fall eines Universitätsklinikums, Die Lage der IT-Sicherheit in Deutschland 2022, Seite 15). Auch im aktuellen Berichtszeitraum wurden wieder fünf Universitäten als Opfer von Ransomware-Angriffen bekannt. Insbesondere nahmen kriminelle Cyberangreifer aber Fachhochschulen ins Visier. Unter den insgesamt 23 bekannt gewordenen Ransomware-Opfern aus dem Bildungs- und Forschungsbereich befanden sich alleine 13 Universitäten und Fachhochschulen. Weiterhin wurden auch mehrere Institutionen namhafter Forschungsverbände sowie zehn allgemeinbildende Schulen zu Opfern.

Trends


5G
6G
10110101001011101000101
00011000101010100101111
00101010011100011001101
01010101001100111010101
01011001100010101010100
01011101010101101110010
01100110101001010011010

Teil C: Herausgehobene Trends in der IT-Sicherheit

10. — Künstliche Intelligenz

Künstliche Intelligenz (KI, engl. Artificial Intelligence, AI) ist derzeit in aller Munde. Nicht zuletzt durch große KI-Sprachmodelle wie zum Beispiel ChatGPT hat das Thema Einzug in den Alltag der Menschen gehalten. Und die Entwicklung ist rasant. Egal, ob ein Text geschrieben oder ein Bild kreiert werden soll, Künstliche Intelligenz ist inzwischen so weit, dass das Ergebnis kaum noch von dem eines Menschen zu unterscheiden ist – und das mit großer Zeitersparnis.

Auch in anderen Bereichen spielt KI eine immer größere Rolle, wie zum Beispiel durch KI-gestützte Empfehlungen bei der Kreditvergabe oder bei der Entscheidung für medizinische Behandlungsmethoden. Weitere Themen sind die Verwendung von KI in der Kryptografie und der Kryptoanalyse oder in den Bereichen autonomes Fahren und mediale Identitäten.

Künstliche Intelligenz ist eine der Schlüsseltechnologien der Digitalisierung. Das BSI hat den Anspruch, die Digitalisierung als Thought Leader in all ihren Facetten sicher zu gestalten und eine zentrale Stelle zu Fragen der Sicherheit und der Prüfung von KI-Systemen im Bund zu werden, weshalb IT-Sicherheit für KI und durch KI Kernthemen sind, welche hierfür aktiv mitgestaltet werden. Zusammen mit Partnern aus Forschung und Entwicklung, Wirtschaft und Verwaltung entwickelt das BSI die technologischen Grundlagen und Kriterien zur Bewertung und Prüfung von KI-Systemen, um sie anschließend in die Praxis zu überführen. Darüber hinaus wirkt das BSI bei der Entwicklung von KI-Normen und KI-Standards aktiv mit und bringt seine langjährige Erfahrung und fachliche Expertise in nationalen und internationalen Standardisierungsprozessen und –gremien ein.

Der Einsatz von KI birgt Risiken und Herausforderungen (siehe Kapitel *Große KI-Sprachemodelle*, Seite 40), aber auch Chancen und Potenziale. Das BSI setzt sich durch die oben aufgeführten Aktivitäten für die Schaffung nachweisbar sicherer, vertrauenswürdiger sowie transparenter KI-Systeme ein. Somit können diese Potenziale, die sich aus den derzeitigen Entwicklungen und Trends im Bereich der Künstlichen Intelligenz ergeben, für Wirtschaft und Gesellschaft sicher nutzbar gemacht und etabliert werden.

10.1 — Sicherheit großer KI-Sprachmodelle

Große KI-Sprachmodelle (LLMs) stehen gegenwärtig im Fokus des öffentlichen Interesses. Sie eignen sich gut zur Textverarbeitung und -generierung und erzeugen qualitativ hochwertigen Text, der sich nur schwer von menschengeschriebenen Texten unterscheiden lässt.

Abteilungs- und standortübergreifend baut das BSI seit Mitte 2022 Expertise zu Sicherheitsaspekten rund um LLMs aus und bietet diese im Rahmen von Beratungsleistungen und Vorträgen innerhalb des BSI sowie anderen Behörden und der Öffentlichkeit an. Im Mai 2023 hat das BSI eine Publikation veröffentlicht, in der die Chancen und Risiken des Einsatzes von LLMs in Industrie und Behörden sowie für Verbraucherinnen und Verbraucher beleuchtet werden.

Die BSI-Publikation zu Großen KI-Sprachmodellen:[m]

Bereits durch die Funktionsweise und das Training von LLMs ergeben sich diverse Schwächen, die Sicherheitsrisiken nach sich ziehen können. Sind die Daten, die genutzt werden, um ein LLM „anzulernen“, nicht ausgeglichen, sondern enthalten eine sogenannte Schiefe (Bias) oder auch veraltete oder diskriminierende Aussagen, können sich diese auch bei der Nutzung des LLM zeigen. Ferner liefert ein LLM auf Eingaben zu ihm bisher unbekannten Themen zwar ein Ergebnis (die sogenannte Ausgabe), dieses kann allerdings beliebig realitätsfern sein (sog. „Halluzinieren“). Ebenso kann ein durch das LLM erzeugter Programmcode für Schwachstellen anfällig sein (wenn diese beispielsweise in den Trainingsdaten vorhanden waren). Problematisch ist weiterhin, dass sich

die Entstehung der Ausgaben von LLMs wegen der hohen Komplexität dieser Modelle nur schwer erklären lassen.

Neben den bereits genannten Risiken ist auch der Einsatz von LLMs für die Generierung von *Spam*- und *Phishing*-E-Mails naheliegend. Durch die Fähigkeit, sprachlich korrekten, überzeugenden Text zu erzeugen, stellen ebenso die automatisierte Erstellung von Hate Speech, Desinformationen und gefälschten Rezensionen ein verbreitetes Missbrauchsszenario dar. Weiterhin können Kriminelle mittels LLMs Schadcode generieren und regelmäßig verändern, sodass dessen Erkennung erschwert wird.

Diese und weitere Szenarien machen es erforderlich, dass Hersteller und Anbieter von LLMs oder LLM-basierten Anwendungen entsprechende Vorkehrungen treffen, die die Erzeugung potenziell schädlicher Ausgaben weitestgehend verhindern oder erschweren. Nutzende dieser Anwendungen sollten über mögliche Sicherheitsrisiken bei der Verwendung von LLMs aufgeklärt werden, um verantwortungsvoll mit den Ausgaben eines solchen Modells umgehen zu können.

Die Integration von LLMs in Alltags- oder Office-Anwendungen kann durch die vielfältigen Möglichkeiten der Unterstützung bei Textverarbeitungs- und -produktionsaufgaben einen Schub für die Digitalisierung leisten. Gleichzeitig können aber je nach Anwendungsfall erhebliche Sicherheitsrisiken entstehen, die im Einzelfall gegen den Nutzen aufgewogen werden sollten.

10.2 — Digitaler Verbraucherschutz und KI

Entscheidungen eines KI-Systems sind wegen ihres Black-Box-Charakters für Verbraucherinnen und Verbraucher oft überraschend und wenig nachvollziehbar. Vor allem in Anwendungen mit weitreichenden Auswirkungen (z. B. Empfehlungen über Behandlungsmethoden oder Kreditvergabe) stellt die fehlende Transparenz dieser Systeme ein Problem dar. Aus diesem Grund untersucht das BSI, wie Verbraucheranwendungen, die KI einsetzen, evaluiert werden können. Ziel ist es, dass Verbraucherinnen und Verbraucher selbstbestimmt die Anwendung von KI-Systemen identifizieren, um somit ihre *Resilienz* in Bezug auf KI-Systeme zu stärken.

Des Weiteren untersucht das BSI Methoden, um die Robustheit von KI-Systemen zu bestimmen und deren Entscheidungen erklären und transparenter gestalten zu können. Die Untersuchungsergebnisse sollen verbraucherfreundlich aufbereitet und über diverse Kommunikationskanäle verbreitet werden.

10.3 — Einsatz von KI in der Kryptografie

Künstliche Intelligenz hat längst auch Einzug in verschiedene Bereiche der Kryptografie gehalten. Insbesondere in der Seitenkanalanalyse haben sich Methoden des maschinellen Lernens (ML) inzwischen fest etabliert. Die besten Ergebnisse lassen sich erzielen, wenn maschinelles Lernen mit Expertenwissen über mögliche Quellen von Seitenkanalinformationen kombiniert wird, wobei der Einsatz neuronaler Netze besonders erfolgreich ist. Das BSI beschäftigt sich daher sowohl im Kontext verschiedener Projekte als auch im Rahmen eigener Forschung mit dem Thema.

KI-Techniken können auch im Bereich der Kryptoanalyse verwendet werden, beispielsweise bei der Analyse und Bewertung von symmetrischen Kryptoverfahren. Dies ist Thema zweier aufeinander aufbauender BSI-Projekte, deren Ziel unter anderem die Entwicklung KI-gestützter Werkzeuge ist, die zu einer Sicherheitsbewertung von Blockchiffren beitragen können.

10.4 — KI-gestützte Analyse der IT-Sicherheitslage

Das BSI testet in einem Projekt KI-Methoden, mit denen sich aktuelle Nachrichten zur IT-Sicherheitslage automatisiert erfassen und analysieren lassen. Ein sogenannter Wissensgraph (Ontologie), bestehend aus Begriffen der IT-Sicherheitsdomäne, dient dabei als Wissensbasis, die diese Analyse unterstützt. Gleichzeitig wird ML dafür eingesetzt, den Wissensgraphen halbautomatisch zu verbessern.

Mit dem Wissensgraphen und trainierten Sprachmodellen werden Entitäten im Text identifiziert, das heißt Textstellen als Nennung einer Entität erkannt – zum Beispiel „Browser“ als Software – oder sogar einem konkreten Objekt zugeordnet, etwa wie die Zeichenkette „BSI“ dem Bundesamt. Diese Entitäten dienen sowohl der semantischen Suche als auch zur Leseunterstützung oder zur gezielten statistischen Auswertung ganzer Objekt-Klassen (z. B. *Malware*). Sprachmodelle ermöglichen auch

Textklassifikation und natürlichsprachliche Fragen mit Textstellen zu beantworten, was wiederum der Transparenz der Ergebnisse zuträglich ist.

10.5 — KI für autonomes Fahren und mediale Identitäten

Seit Dezember 2021 führt das BSI Projekte durch, in denen anhand der Betrachtung praktischer Anwendungsfälle erste konkrete Kriterien und Prüfmethoden für KI-Verfahren im autonomen Fahren erarbeitet werden. Im ersten Projekt[18] wurden unter anderem 50 technisch relevante Anforderungen an KI-Systeme zusammengestellt sowie eine erweiterbare Testumgebung für KI-Systeme entwickelt. Diese Anforderungen, Methoden und Werkzeuge werden seit Dezember 2022 in einem Folgeprojekt gezielt erprobt und weiterentwickelt. Mittelfristig plant das BSI, auf Basis dieser Vorarbeiten eine technische Richtlinie zu verfassen[19].

Weitere Informationen zum automatisierten Fahren:[n]

Auch im vergangenen Berichtszeitraum wurde eine kontinuierliche Qualitätssteigerung der öffentlich zugänglichen Werkzeuge zur Manipulation von Identitäten in den Medien Audio und Video (*Deepfakes*) beobachtet (siehe auch Kapitel *Skalierungseffekte bekannter Bedrohungen*, S. 44). Die Verfügbarkeit solcher Werkzeuge ist zum einen durch Open-Source-Software und zum anderen durch neue *Cloud*-Dienste gegeben. Teilweise können Identitäten auf Basis von nur wenigen Sekunden Material mit „One-Shot"-Verfahren auf eine Zielidentität hin ausgerichtet werden. Dies kann beispielsweise dazu genutzt werden, um Systeme für Sprechererkennung zu überwinden[20].

Das BSI konnte zeigen, dass mittlerweile sowohl im Audio- als auch im Videobereich Identitätsfälschungen mit annehmbarer Qualität in Echtzeit möglich sind. Im Projekt „Absicherung medialer Identitäten" sollen bis 2025 Gegenmaßnahmen erarbeitet und evaluiert werden.

10.6 — Weitere Entwicklungen im Bereich KI

Der Themenbereich der KI-Sicherheit steht weltweit weiterhin im Fokus von Standardisierungsgremien und Expertengruppen, in denen das BSI seine Expertise einbringt. In einer wachsenden Anzahl unterschiedlicher Anwendungsdomänen arbeitet das BSI an der Entwicklung von Prüfkriterien und Prüfmethoden für KI-Systeme, beispielsweise in den Bereichen Automotive, *Cloud*-Dienste, Medizin und Agrarwirtschaft. Damit werden die Kernthemen und Empfehlungen der Deutschen Normungsroadmap KI, an deren Erstellung das BSI aktiv mitwirkte, bearbeitet und umgesetzt.

Weitere Informationen zu dieser und weiteren Studien finden Sie hier:[o]

In einem Projekt wurde erfolgreich ein neuartiger Ansatz zur KI-gestützten statischen Code-Analyse implementiert und erprobt. Die Software ist als Open Source veröffentlicht, wodurch eine bessere Vernetzung mit der Forschungscommunity sowie weitere Impulse für die Forschung in diese Richtung erwartet werden.

Quantencomputer bieten Potenziale, die auch und speziell im Bereich des maschinellen Lernens von zunehmend hohem Interesse sind. Aktuell werden vor allem Ansätze diskutiert, die klassische und Quanten-Algorithmen in hybriden Methoden kombinieren[21]. In einer Grundlagenstudie[22] hat das BSI den aktuellen Forschungsstand zum Quantum Machine Learning (QML) erfasst und Chancen und Risiken hinsichtlich der IT-Sicherheit beleuchtet. In einem Folgeprojekt werden die Sicherheitseigenschaften von und die Bedrohungsszenarien für QML-Methoden und -Systeme anhand praktischer Experimente untersucht.

Im Bereich der Explainable AI untersuchte das BSI die fehlende Reproduzierbarkeit des Trainings von Machine-Learning-Modellen (ML-Modellen) und dessen Auswirkung auf Vorhersage und Erklärbarkeit der Ausgaben der Modelle. Weiterhin wurde der Einfluss der Dimensionalität von Daten auf die Qualität und Zuverlässigkeit wahrscheinlichkeitsbasierter ML-Modelle beleuchtet.

11. — Quantentechnologien

Die fortschreitende Entwicklung von Quantencomputern bedroht die Sicherheit vieler klassischer und weitverbreiteter Public-Key-Verfahren wie *RSA* und ECC. Deshalb ist die Migration zu kryptografischen Verfahren von hoher Dringlichkeit, die voraussichtlich auch mit Quantencomputern nicht gebrochen werden können (Post-Quanten-Kryptografie). Das BSI handelt dazu für den Hochsicherheitsbereich unter der Arbeitshypothese, dass kryptografisch relevante Quantencomputer Anfang der 2030er-Jahre zur Verfügung stehen werden. Dabei ist zu betonen, dass diese Aussage nicht als Prognose zur Verfügbarkeit von Quantencomputern zu verstehen ist, sondern einen Richtwert für die Risikobewertung darstellt.

Eine detaillierte Analyse „Entwicklungsstand Quantencomputer“ wurde im Auftrag des BSI bereits 2018 erstellt und seitdem zweimal aktualisiert. In einem weiteren BSI-Projekt erfolgten insgesamt drei weitere Updates.

Weitere Informationen zur Studie:[p]

In der Technischen Richtlinie TR-02102-1 des BSI werden mit FrodoKEM und Classic McEliece bereits seit März 2020 erste Post-Quanten-Verfahren zum Schlüsseltransport und die hashbasierten Signaturverfahren LMS und XMSS empfohlen. Einen Überblick zum gesamten Themenkomplex liefert der Leitfaden „Kryptografie quantensicher gestalten“ des BSI.

Den BSI-Leitfaden „Kryptografie quantensicher gestalten" finden Sie hier:[q]

Die technische Richtlinie TR-02102 finden Sie hier:[r]

Auch andere europäische Cybersicherheitsbehörden wie die französische ANSSI und das niederländische NCSC haben erste Empfehlungen zur Migration auf quantensichere Verfahren veröffentlicht. Besonders umfassende und konkrete Maßnahmen hat die US-amerikanische Regierung eingeleitet. In zwei Memoranden vom Mai und November 2022[23] wurden die verpflichtende Erstellung von Migrationsplänen, regelmäßige Berichtspflichten und ambitionierte Migrationszeitpläne für Behörden festgelegt. Bis 2035 soll die Gefährdung durch Quantentechnologien durch den flächendeckenden Einsatz von Post-Quanten-Kryptografie weitestgehend minimiert sein. Um dies zu erreichen, hat die NSA im November 2022 die Commercial National Security Algorithm Suite (CNSA) 2.0[24] veröffentlicht. Diese ist für Betreiber von National Security Systems bindend und beschreibt Zeitpläne für verschiedene technische Anwendungen. Beispielsweise ist ab 2027 Post-Quanten-Kryptografie als Standard für Web-Browser, Server und *Cloud*-Dienste vorgesehen.

Die Auswirkungen von Quantentechnologien auf die Cybersicherheit sind von der Bundesregierung und dem BMI aufgegriffen worden. Die Bundesregierung hat im September 2021 in der „Cybersicherheitsstrategie für Deutschland 2021“[25] die Förderung der „Entwicklung neuer Verschlüsselungslösungen, insbesondere im Bereich der Post-Quanten-Kryptografie“ als Ziel genannt. Dieses Ziel hat das BMI in der im April 2022 veröffentlichten Cybersicherheitsagenda[26] mit der Maßnahme „Ausstattung der Bundesbehörden mit weiterentwickelten IT-Produkten und -Systemen für sichere Kommunikation sowie Investition in Quantencomputing und Post-Quanten-Kryptografie“ hinterlegt.

Die Bundesregierung setzt sich im „Handlungskonzept Quantentechnologien“[27] das Ziel, bis 2026 eine Strategie der Migration zur Post-Quanten-Kryptografie zu erstellen.

11.1 — Post-Quanten-Kryptografie

Die Standardisierung von Post-Quanten-Verfahren geschah bisher hauptsächlich in einem vom US-amerikanischen National Institute of Standards and Technology (NIST) im Jahre 2016 initiierten Prozess mit internationaler Beteiligung. Im Juli 2022 hat NIST das Schlüsseltransportverfahren CRYSTALS-Kyber und die Signaturverfahren CRYSTALS-Dilithium, Falcon sowie SPHINCS+ zur Standardisierung ausgewählt[28] (vgl. auch Kapitel *Schwachstellen in Hardwareprodukten*, Seite 39).

Neben der Standardisierung der Post-Quanten-Verfahren laufen zurzeit viele konkrete Aktivitäten zur Migration auf Post-Quanten-Kryptografie. So sind erste Produkte für den Hochsicherheitsbereich, die hybride Schlüsseleinigung benutzen, bereits zugelassen und im Einsatz. Bei

NIST-Auswahlverfahren

Bis auf das hashbasierte SPHINCS+ beruht die Sicherheit dieser Verfahren auf Gitterproblemen in strukturierten Gittern. Standardisierungsentwürfe für Kyber, Dilithium und SPHINCS+ wurden im August 2023 veröffentlicht. Am Ende der zurzeit laufenden vierten Runde wird voraussichtlich ein weiteres Schlüsseltransportverfahren zur Standardisierung ausgewählt. Außerdem hat NIST einen neuen Aufruf zur Einreichung weiterer Signaturverfahren veröffentlicht, zu dem bis Anfang Juni 2023 Einreichungen akzeptiert wurden. Das vom BSI empfohlene FrodoKEM wird im NIST-Prozess nicht weiter betrachtet, weil es weniger effizient als Kyber ist. Classic McEliece, die zweite BSI-Empfehlung zum Schlüsseltransport, könnte eventuell am Ende der vierten Runde noch standardisiert werden. Das BSI hält an der Empfehlung von FrodoKEM und Classic McEliece auch nach der Entscheidung durch NIST fest. Diese Verfahren liefern eine eher konservative Alternative zur bisherigen NIST-Auswahl und werden derzeit bei ISO standardisiert.

In den letzten Jahren war die Forschungsaktivität im Bereich Post-Quanten-Kryptografie sehr hoch, was zum Teil an der hohen Öffentlichkeitswirksamkeit des NIST-Auswahlprozesses liegt. Tatsächlich haben sich einige der eingereichten Verfahren als unsicher erwiesen. So hat sich zum Beispiel das Sicherheitsniveau des multivariaten Signaturverfahrens Rainbow (ein Finalist in der 3. Runde des NIST-Prozesses) im Jahr 2022 durch neue Angriffe als unzureichend herausgestellt. Das isogeniebasierte Schlüsseltransportverfahren SIKE wurde, kurz nachdem es von der NIST in die 4. Runde aufgenommen wurde, sogar vollständig gebrochen. Die Sicherheit der vom BSI empfohlenen sowie der von NIST bislang zur Standardisierung ausgewählten Verfahren beruht jedoch auf ganz anderen mathematischen Problemen. Daher sind diese Verfahren von den neuen Angriffen nicht betroffen und gelten weiterhin als sicher. Auch sie müssen jedoch weiter aktiv untersucht werden und das BSI empfiehlt grundsätzlich den hybriden Einsatz von Post-Quanten-Kryptografie in Kombination mit klassischer Public-Key-Kryptografie.

der Internet Engineering Task Force (IETF) wird in zahlreichen Arbeitsgruppen daran gearbeitet, Post-Quanten-Kryptografie in die Standards der IETF zu integrieren. In einem BSI-Projekt zur Weiterentwicklung der FOSS-Kryptobibliothek Botan werden aktuell Post-Quanten-Verfahren und eine hybride Schlüsseleinigung in TLS 1.3 implementiert. Ein weiteres BSI-Projekt hat sich zum Ziel gesetzt, quantensichere E-Mail-Verschlüsselung und -Signaturen im E-Mail-Client Thunderbird zu realisieren. Im Rahmen dieses Projektes ist auch ein Standardisierungsentwurf für Post-Quanten-Kryptografie in OpenPGP entstanden.

Das BSI ist außerdem Betreiber der Wurzelzertifizierungsstelle für die Public-Key-Infrastruktur der öffentlichen Verwaltung (V-PKI). Die aktuell verwendeten kryptografischen Algorithmen in dieser V-PKI sind nicht quantensicher. Um der drohenden Gefährdung durch kryptografisch relevante Quantencomputer rechtzeitig begegnen zu können, plant das BSI aktuell die Migration zu einer quantensicheren V-PKI.

Auch außerhalb des Hochsicherheitsbereichs und der öffentlichen Verwaltung ist die Migration auf Post-Quanten-Kryptografie wichtig. Deshalb muss die Awareness für die Sicherheitsbedrohung durch Quantencomputing und mögliche Schutzmaßnahmen erhöht werden. Eine im April 2023 veröffentlichte Umfrage[29] zeigt, dass Unternehmen nicht genügend Maßnahmen ergreifen, um der Bedrohung der Informationssicherheit durch Quantencomputer zu begegnen. Zwar haben 97 Prozent der teilnehmenden Unternehmen die Relevanz von Quantencomputing für die Sicherheit heutiger Kryptografie als „hoch“ oder „eher hoch“ eingeschätzt. Diese Bedrohung wird aber nur von 25 Prozent der Unternehmen im Risikomanagement berücksichtigt.

11.2 — Quantum Key Distribution

Quantum Key Distribution (QKD) soll quantensichere Schlüsseleinigung auf Basis quantenmechanischer Prin-

zipien ermöglichen und kann somit für spezielle Anwendungsfälle eine Ergänzung zu Post-Quanten-Kryptografie sein. Die Entwicklung von QKD wird derzeit auf nationaler und europäischer Ebene intensiv gefördert, beispielsweise durch das Projekt EuroQCI der Europäischen Kommission. Im Rahmen von EuroQCI soll eine Quantenkommunikationsinfrastruktur in Europa aufgebaut werden, die sowohl eine terrestrische als auch eine satellitengestützte Komponente umfasst. Seit März 2023 ist EuroQCI Teil von IRIS2, dem Projekt zur Entwicklung eines europäischen satellitenbasierten sicheren Kommunikationssystems. Das BSI ist in der Security Working Group von EuroQCI vertreten.

Aus Sicht des BSI sind noch wesentliche Grundlagenarbeiten zu Sicherheitsfragen erforderlich, bis QKD einsatzreif ist. Um einen Beitrag zur Entwicklung sicherer QKD-Systeme zu leisten, hat das BSI gemeinsam mit dem European Telecommunications Standards Institute (ETSI) ein erstes Protection Profile (PP)[30] nach Common Criteria für Prepare-and-Measure-QKD-Systeme entwickelt. Dieses Profil wurde in einer ersten Version im April 2023 von ETSI veröffentlicht. Derzeit wird es beim BSI zertifiziert und soll danach in einer aktualisierten Version bereitgestellt werden. Um das PP zur Zertifizierung von Produkten zu nutzen, ist jedoch die Erarbeitung weiterer Hintergrunddokumente wie Standards sowie einer Evaluierungsmethodologie erforderlich. Standards zu QKD werden derzeit in mehreren Gremien entwickelt.

Um die Entwicklung einer Evaluierungsmethodologie für QKD zu unterstützen, hat das BSI 2022 eine wissenschaftliche Studie zu *Seitenkanalangriff*en auf QKD-Systeme in Auftrag gegeben. Die Ergebnisse werden voraussichtlich Ende 2023 veröffentlicht.

Das Bundesministerium für Bildung und Forschung (BMBF) fördert verschiedene Projekte zur Quantenkommunikation, darunter das Projekt QuNET. Im Rahmen des Innovationshubs Quantenkommunikation wird zudem ein Schirmprojekt gefördert, das die deutschlandweit vorhandenen Kompetenzen zur Quantenkommunikation bündeln und fokussieren soll. Dieses Schirmprojekt Quantenkommunikation Deutschland (SQuaD) wird von der Physikalisch-Technischen Bundesanstalt im engen Schulterschluss mit dem BSI koordiniert.

12. — Sicherheit moderner Telekommunikationsinfrastrukturen (5G/6G)

Ein für das BSI besonders wichtiges Zukunftsthema ist eine sicher gestaltete 5G/6G-Infrastruktur für Deutschland. Mit 5G- und 6G-Technologien lassen sich Anwendungsszenarien verwirklichen, die vorher nicht über Mobilfunk zu realisieren waren. So steigen beispielsweise die Geschwindigkeiten der Datenübertragung bei gleichzeitig sinkender Verzögerung.

Die höheren Übertragungsgeschwindigkeiten verbessern dabei die Effizienz. Zudem ermöglichen die geringen Latenzzeiten Echtzeitkommunikation von Endgeräten und bieten so völlig neue Möglichkeiten. Damit schaffen die modernen Mobilfunktechnologien eine wichtige Voraussetzung für die weitere Digitalisierung und entwickeln sich immer stärker zu einer kritischen Infrastruktur.

Die Erfüllung des Ziels einer sicher gestalteten 5G/6G-Infrastruktur lässt sich in drei Bereiche unterteilen:

- Entwicklung von Vorgaben zur Aufrechterhaltung des sicheren Betriebes von 5G-Netzen
- Überprüfung der Vorgaben durch Instrumente der Zertifizierung und Auditierung
- Mitarbeit in Standardisierungsorganisationen zur Entwicklung und Fortschreibung von Schemata sowie für die Implementierung von Anforderungen an die IT-Sicherheit von 5G/6G-Netzen

12.1 — Vorgaben und Zertifizierung für 5G-Netze

Öffentliche Mobilfunknetze der 5. Generation unterliegen gesetzlichen Regularien, an deren Erarbeitung und Fortschreibung das BSI beteiligt ist. Die folgenden Unterkapitel geben einen Überblick und beleuchten verschiedene zur Anwendung kommende Zertifizierungsschemata. Für den Bereich der privaten 5G-Netze, auch 5G-Campusnetze genannt, existieren keine gesetzlichen Regulierungen. Stattdessen werden den Betreibern und Anwendern standardisierte Werkzeuge zur Einführung von IT-Sicherheit im Rahmen von IT-Grundschutz-Profilen zur Verfügung gestellt.

12.1.1 — Mitgestaltung des IT-Sicherheitskatalogs und Fortschreibung der Technischen Richtlinie TR-03163

Unter Federführung der Bundesnetzagentur gestaltet das BSI gemeinsam mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit den Katalog von Sicherheitsanforderungen gemäß Telekommunikationsgesetz (TKG), der sich aktuell in Überarbeitung befindet.

Der Sicherheitskatalog regelt verpflichtende Maßnahmen, um die im TKG genannten Schutzziele zu erreichen, und richtet sich an alle Telekommunikationsbetreiber und Diensteanbieter. Dabei werden für den 5G-Netzbetrieb erhöhte Anforderungen festgelegt, um der Bedeutung des 5G-Mobilfunknetzes für die Gesellschaft Rechnung zu tragen. Der Sicherheitskatalog benennt den Rahmen und die Fristen zur Zertifizierung von kritischen 5G-Netzwerkkomponenten und verweist für die Details auf die Technische Richtlinie TR-03163 „Sicherheit in TK-Infrastrukturen“ des BSI, die Schemata benennt und regelmäßig fortgeschrieben wird.

Die Technische Richtlinie TR-03163:[5]

12.1.2 — Umsetzung Zertifizierungspflicht für kritische Komponenten in öffentlichen 5G-Netzen

Mit der Veröffentlichung der TR-03163 sowie der Produktivsetzung des nationalen Zertifizierungsprogramms für 5G-Mobilfunkausrüstung (*NESAS CCS-GI*) hat das BSI begonnen, die gesetzliche Zertifizierungspflicht gemäß TKG umzusetzen. Derzeit arbeitet das BSI zusammen mit interessierten Partnern daran, die Anforderungen an die Sicherheitszertifizierung verschiedener Netzelemente eines 5G-Netzes zu erstellen.

Das *NESAS CCS-GI* ermöglicht es Herstellern, mittels eines IT-Sicherheitszertifikats nachzuweisen, dass sie die durch das internationale Standardisierungsprojekt 3rd Generation Partnership Project (3GPP) geforderten Sicherheitseigenschaften einhalten. Das Zertifikat basiert auf dem Network Equipment Security Assurance Scheme (*NESAS*) der GSMA, der globalen Interessenvertretung der Mobilfunkanbieter und Hersteller, und umfasst eine Überprüfung der Produktentwicklungs- und Lebenszyklusprozesse sowie eine Evaluation des danach hergestellten Produkts. Im Berichtszeitraum wurden mit der TÜV Informationstechnik GmbH und der atsec information security GmbH zwei Unternehmen als Prüfstellen für *NESAS CCS-GI* anerkannt. Im Januar 2023 wurde das erste *NESAS*-CCS-GI-Zertifikat für eine 5G-Basisstation ausgestellt.

Ausgehend von den Produkteigenschaften und den Ansätzen zur Evaluierung innerhalb der verschiedenen vom BSI angebotenen Zertifizierungsschemata listet die TR-03163 weitere Zertifizierungsprogramme wie Common Criteria und Beschleunigte Sicherheitszertifizierung für definierte Produktklassen auf. Dies fördert die Verwendung von Produkten, die für ihren geplanten Einsatz bereits im Vorfeld bezüglich ihrer Sicherheitseigenschaften geprüft wurden.

12.1.3 — Überprüfung öffentlicher 5G-Netzbetreiber

Durch das *IT-Sicherheitsgesetz 2.0* erhielt das BSI die Aufgabe, Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste mit erhöhtem Gefährdungspotenzial alle zwei Jahre zu überprüfen. Überprüft wird im Bereich 5G, ob die Betreiber die gesetzlichen Vorgaben zur Informationssicherheit aus dem TKG einhalten. Die Anforderungen im TKG umfassen dabei organisatorische, technische und betriebliche Rahmenbedingungen, unter denen die Telekommunikationsnetze betrieben und die dazugehörigen Dienste erbracht werden. Dafür hat das BSI im Berichtszeitraum ein Prüfschema entwickelt und in Abstimmung mit den zuständigen Behörden die gesetzlichen Vorgaben durch eine Prüfgrundlage weiter untersetzt. Die ersten Überprüfungen werden im Laufe des Jahres 2023 stattfinden.

12.1.4 — IT-Grundschutz für sichere private 5G-Netze

Mit dem Einsatz von privaten 5G-Netzen ergeben sich neue Anforderungen an Unternehmen, Behörden, Forschungseinrichtungen und weitere Betreiber.

Das BSI widmet sich der Frage, wie sich 5G-Netze sicher betreiben lassen, und nutzt mit dem IT-Grundschutz ein erprobtes und anerkanntes Werkzeug für den Aufbau und Betrieb eines Managementsystems für Informationssicherheit.

Das „IT-Grundschutz-Profil zur Absicherung von 5G-Campusnetzen – Betrieb durch einen externen Dienstleister" ist eine Anleitung, mit deren Hilfe sich Organisationen mit dem Thema Informations- und IT-Sicherheit in privaten 5G-Netzen vertraut machen können. Die darin enthaltene Risikoanalyse gibt konkrete Handlungsempfehlungen, mit denen sich ein 5G-Campusnetz schützen lässt. Diese Schablone kann individuell an das Unternehmen angepasst werden. Die gesammelten Erfahrungen dienen als Grundlage für zukünftige Sicherheitskonzept-Blaupausen im Bereich der 5G-Campusnetze.

12.2 — Sicherheit in der Standardisierung von 5G und 6G

Das BSI ist überzeugt, dass IT-Sicherheitsbelange bereits bei der Ausarbeitung von Standards eingebracht werden müssen, aktuell und dringlich im Bereich von 6G. Zudem ist die hinreichende Implementierung von IT-Sicherheitsvorgaben bereits in der Standardisierung Grundlage einer erfolgreichen Sicherheitszertifizierung. Das BSI beteiligt sich deshalb in verschiedenen internationalen Standardisierungsorganisationen. Nachfolgend werden die wichtigsten Aktivitäten zur Sicherheit in Standards der Mobilfunkkommunikation aufgeführt.

Die GlobalPlatform ist eine internationale Industrie-Standardisierungsorganisation, deren Technologie das technische Management von Applikationen auf Secure Elements, SIM-Karten und *Trusted Execution Environments* ermöglicht.

Die Basis für *NESAS CCS-GI* bildet das *NESAS*-Prüfschema, das von der GSMA herausgegeben wird. Das BSI ist in der zugehörigen Expertengruppe vertreten und arbeitet an der Überführung zu einem Zertifizierungsverfahren mit. Zudem beteiligt sich das BSI daran, die Harmonisierung von *NESAS* mit den Anforderungen an das EU5G-Zertifizierungsschema nach dem EU-Cybersecurity Act sicherzustellen.

Im 3GPP werden, aufbauend auf GSM (2G), die Spezifikationen für die Mobilfunkstandards UMTS (3G), LTE (4G) und 5G entwickelt. Das BSI beteiligt sich seit 2022 mit eigenen Beiträgen zum Thema Roaming und bei der Gestaltung von Sicherheitstests gemäß *Security Assurance Specifications* (*SCAS*). Die *SCAS* definieren wichtige Sicherheitsfunktionen, die auch Grundlage für die Produktzertifizierung nach *NESAS CCS-GI* bilden.

Die Testdurchführung ist bisher sehr unterschiedlich genau ausgeführt. Das BSI definierte daher zu 59 Testfällen sogenannte Refinements. Diese müssen unter *NESAS CCS-GI* von den Prüfstellen beachtet werden und fördern die Vergleichbarkeit und Nachvollziehbarkeit der Ergebnisse.

Bei den Open-RAN-Spezifikationen der O-RAN Alliance, die eine weitere Modularisierung in den Funkzugangsnetzen (RAN) möglich machen sollen, hat das BSI einerseits die Standardisierung über das European Telecommunications Standards Institute (ETSI) kommentiert, andererseits wurden durch eine vom BSI beauftragte Studie Kritikpunkte an früheren O-RAN-Versionen aufgeworfen.

Die Standardisierung der aufkommenden 6G-Technologie steht noch bevor. Das BSI beteiligt sich bereits heute zu Sicherheitsaspekten an der 6G-Plattform, einer vom BMBF geförderten Koordinierungsplattform für Deutschland. Mit wichtigen deutschen 6G-Forschungsprojekten besteht kontinuierlicher Austausch.

Um die Standardisierung in den Organisationen voranzutreiben, nutzt das BSI ein eigenes Testlabor. Mit der Zielsetzung der Erhöhung des Sicherheitsniveaus von Mobilfunknetzen befindet sich das 5G/6G Security Lab TEMIS (Test Environment for Mobile Infrastructure Security) im Aufbau. Im Fokus stehen Sicherheitsuntersuchungen von 5G-Komponenten sowie Entwicklung und Verifikation von sicherheitsrelevanten Tests und Vorgaben für die 5G-Technologie. Mitte 2023 geht TEMIS mit Mobilfunkkomponenten des ersten Herstellers in Betrieb.

12.3 — Förderung von Cybersicherheit und digitaler Souveränität in den Kommunikationstechnologien 5G/6G

Die Nr. 45 des Konjunkturprogramms (KoPa) der Bundesregierung zur Adressierung der Folgen der Corona-Pandemie fördert Investitionen in zukünftige Kommunikationstechnologien (5G/6G). Das BSI setzt die Nr. 45 KoPa

mit dem eigenen Förderprogramm „Cybersicherheit und digitale Souveränität in den Kommunikationstechnologien 5G/6G“ sowie flankierenden Studien und Beschaffungen um. Ziele sind die Förderung der digitalen Souveränität und die Stärkung der Innovationskraft deutscher Unternehmen im IT-Sicherheitskontext. Seit dem Start des Förderprogramms im Juni 2022 wurden 32 Projekte bewilligt.

13. — eID: Novellierung der eIDAS-Verordnung

Eine der größten Bedrohungen für Verbraucherinnen und Verbraucher ist im aktuellen Berichtszeitraum Identitätsdiebstahl und Online-Betrug (vgl. Kapitel *Erkenntnisse zur Gefährdungslage in der Gesellschaft*, Seite 51). Digitale Geschäftsprozesse haben nicht erst durch die COVID-19-Pandemie eine steigende Bedeutung erfahren. Dadurch stieg auch der Bedarf an sicherer elektronischer Identifizierung und sicheren elektronischen Identitäten, um die Integrität digitaler Prozesse sowie ein hohes Maß an Vertrauen zwischen Nutzer und Dienstleister zu gewährleisten. Dies trägt maßgeblich dazu bei, Online-Betrug sowie insbesondere Identitätsdiebstahl zu erschweren. Das BSI arbeitet dafür seit Jahren daran, die Online-Ausweisfunktion zugänglicher zu machen und weitere Use Cases zu ermöglichen. Mit der Technischen Richtlinie TR-03128 Teil 3 hat das BSI so die technischen Möglichkeiten geschaffen, dass sich Bürgerinnen und Bürger eine neue PIN von zu Hause aus bestellen oder sich online bei der Meldebehörde ummelden können. Während die Nutzerzahlen beim PIN-Rücksetzdienst im Berichtszeitraum anstiegen, ist die elektronische Wohnsitzanmeldung zum aktuellen Zeitpunkt als eine EfA-Leistung des Landes Hamburg umgesetzt und wird dort bereits genutzt.

Im Rahmen der eIDAS-Verordnung akzeptieren die EU-Mitgliedsstaaten gegenseitig notifizierte elektronische Identifizierungsmittel (eID) in nationalen Anwendungen. So ist es aktuell zum Beispiel möglich, mit einer italienischen eID einen Dienst in Deutschland zu nutzen. Im Berichtszeitraum haben weitere Staaten per Verordnung elektronische Identifizierungssysteme zur grenzüberschreitenden Anerkennung notifiziert, die nach Ablauf einer einjährigen Übergangszeit einer gegenseitigen Anerkennungsverpflichtung unterliegen. Hier hat sich das BSI im Rahmen von Peer Reviews beteiligt. Insgesamt betrifft die Anerkennungsverpflichtung nun 23 elektronische Identifizierungssysteme aus 18 unterschiedlichen Staaten europaweit.

Für die Nutzung elektronischer Verwaltungsdienstleistungen im europäischen Ausland können Bürgerinnen und Bürger ihre deutsche eID-Karte (Personalausweis, elektronischer Aufenthaltstitel, Unionsbürgerkarte) zusammen mit der Online-Ausweisfunktion für die *Authentifizierung* und Identifizierung verwenden. Hierfür wird den EU-Mitgliedsstaaten eine Software bereitgestellt, die die Übersetzung vom deutschen eID-System zum europäischen eIDAS-System leistet: die eIDAS-Middle-ware. Momentan sind 20 Länder sowie die EU-Kommission an das deutsche eID-System angeschlossen. Im Berichtszeitraum wurden die europäischen technischen Richtlinien eIDAS Technical Specifications[31] aktualisiert und um zusätzliche Identitätsattribute erweitert. Darüber hinaus wurden die Stabilität und Nutzerfreundlichkeit der eIDAS-Middleware weiter verbessert, um Ausfallzeiten zu minimieren und die Verwendung zu erleichtern. Weiterhin ist geplant, den Austausch zwischen den Mitgliedsstaaten zu verbessern, um schneller über Änderungen an den Schnittstellen zwischen dem nationalen eID-System und dem europäischen eIDAS-System zu informieren. Damit wird die Interkonnektivität zwischen den Mitgliedsstaaten weiter erhöht.

Neben vielen kleineren Änderungen sieht der 2021 im Rahmen der turnusgemäßen Revision der eIDAS-Verordnung veröffentlichte neue Verordnungsentwurf eine digitale Brieftasche, die „EU Digital Identity Wallet“ (EUDI Wallet) vor, die als elektronisches Identifizierungsmittel grenzüberschreitend nutzbar sein soll. Diese soll neben klassischen Identitätsattributen (Vorname, Name etc.) noch weitere Attribute (z. B. Bildungsabschluss, Führerschein) in verifizierbarer Art für Diensteanbieter bereitstellen können und die Möglichkeit zur qualifizierten elektronischen Signatur bieten. Im Berichtszeitraum ist die Entwicklung der Vorgaben zu dieser EUDI Wallet massiv vorangeschritten. So wurde Anfang 2023 das Architecture and Reference Framework (ARF), das als Grundlage für die zukünftigen Umsetzungsrechtsakte dienen soll, in einer ersten Version durch die europäische Kommission veröffentlicht. Das BSI ist an der Erstellung dieses Dokuments und auch an der Fortentwicklung des ARF beteiligt, bringt die bestehende deutsche Infrastruktur ein und setzt sich weiterhin für sichere und nutzerfreundliche eID-Lösungen ein, die grenzüberschreitend verwendet werden können.

Im Rahmen der EUDI Wallet möchte die Kommission in sogenannten Large Scale Pilots (LSP) nachweisen, dass die Vorgaben umsetzbar sind, und eine oder mehrere Wallets als Piloten auf den Markt bringen. Des Weiteren soll es den Mitgliedsstaaten die Möglichkeit bieten, auch andere, nicht durch das ARF beschriebene Technologien und Ideen zu erproben. Die Entwicklungserkenntnisse dieser Wallets sollen weitergehend auch in die aktuelle Fortschreibung und Weiterentwicklung des ARF und zukünftiger Dokumente einfließen.

Anders als in der älteren eIDAS-Verordnung, die nur die Anerkennung von national bestehenden eID-Lösungen in den Partnerstaaten vorschrieb, sollen nun Mitgliedsstaaten verpflichtet werden, entsprechende eID-Lösungen im Rahmen einer Wallet anzubieten. Außerdem sollen sowohl öffentliche Stellen als auch große private Unternehmen, die eine Anforderung an die Identifizierung ihrer Nutzer haben, die EUDI Wallet als Identifizierungsmittel akzeptieren. Die LSP sollen hier Staaten, die noch keine anerkannte eID-Lösung haben, die Möglichkeit bieten, technisches Know-how wiederzuverwenden.

Die Handlungsstränge der eIDAS-Revision werden in Abbildung 20 dargestellt.

In den Verhandlungen zur eIDAS-Verordnung werden die Rahmenbedingungen definiert, unter denen die eIDAS Expert Group eine technische Ausarbeitung umsetzt. Diese Technik wird in der Referenzimplementierung und den eIDAS Large Scale Pilots erprobt. Hierbei sollen die LSP die Referenz-Wallet, eine Wallet-Implementierung durch die Kommission, verwenden und im Feld erproben, um Feedback sowohl zur Expert Group als auch zur Entwicklung der Referenz-Wallet zu geben.

Für die Online-Identifikation arbeitet das BSI aktuell an der Umsetzung der Online-Ausweisfunktion in einem Wallet-Modul. Dadurch soll sichergestellt werden, dass die aktuellen Systeme weiterverwendet werden können, um mögliche Investitionen zu senken und das für die Online-Ausweisfunktion bereits notifizierte und anerkannte hohe Vertrauensniveau zu übernehmen. Mithilfe eines modularen Aufbaus der Wallet (siehe Abbildung 21) sollen im Anschluss weitere Nutzungsmöglichkeiten implementiert werden, die nicht auf die bereits vorhandene Technik setzen müssen, entweder, weil es dort bereits international verwendete Standards gibt, oder auch, weil diese Anwendungsfälle kein hohes Vertrauensniveau benötigen. Zusätzlich ermöglicht ein modularer Ansatz eine technische Trennung zwischen den Standards, die eine Online-Kommunikation ermöglichen sollen, und der Nutzung in Offline-Anwendungsfällen, die ohne Internetverbindung einem ganz anderen Anforderungsspektrum genügen müssen. Auch können über Module, neben verschiedenen Anforderungen an Protokolle, verschiedene Anforderungen an die Datenspeicherung abgebildet werden. So wäre für eine Smart-eID die Speicherung in einem eigenen Sicherheitschip, beispielsweise einem Secure Element, notwendig, während andere Nachweise aus der EUDI Wallet diese Sicherheitsanforderungen nicht benötigen.

Handlungsstränge der eIDAS-Revision

Abbildung 20: Handlungsstränge der eIDAS-Revision
Quelle: BSI

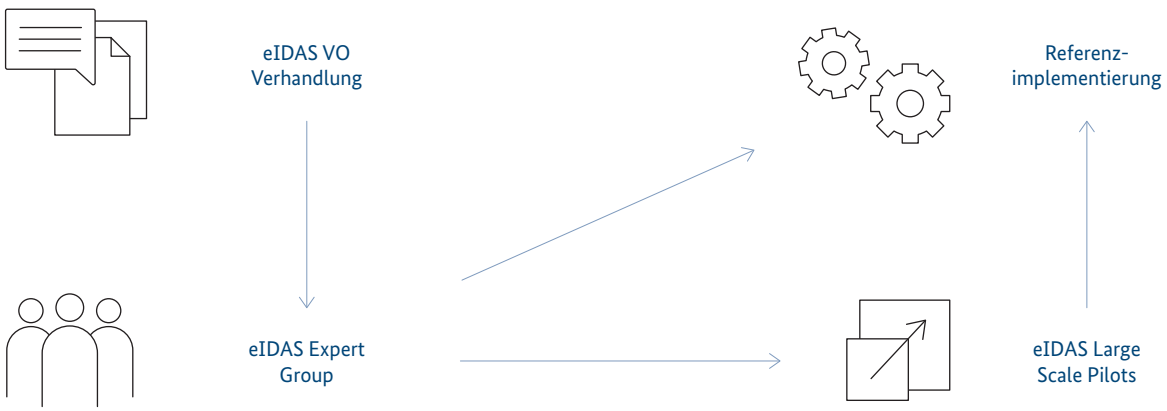
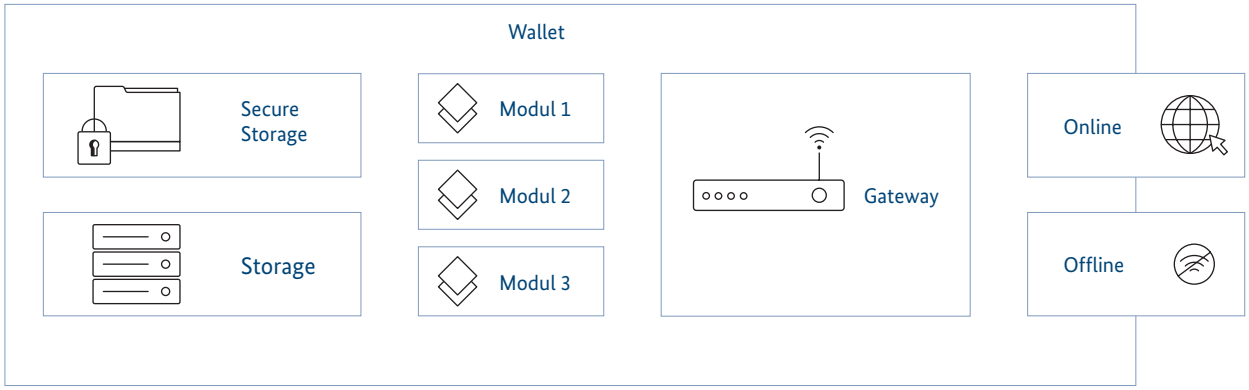


Schaubild Modulaufbau

Abbildung 21: Schaubild Modulaufbau
Quelle: BSI



14. — Bund-Länder-Zusammenarbeit

Mit der zunehmenden Digitalisierung und Vernetzung von Bund und Ländern geht auch eine Erhöhung der Angriffsfläche einher (vgl. *Erkenntnisse aus der Gefährdungslage in Staat und Verwaltung*, Seite 67). *Ransomware* war im Berichtszeitraum insbesondere für Kommunen die größte Bedrohung, was an der hohen Anzahl bekannt gewordener *Ransomware*-Angriffe zu sehen ist (vgl. Vorfall *Ransomware-Angriffe auf Kommunalverwaltungen und kommunale Versorgungsbetriebe*, Seite 69). Die erfolgreiche Gestaltung der Informationssicherheit in der Verwaltungsdigitalisierung bedarf der fortgesetzten vertrauensvollen Zusammenarbeit zwischen Bund und Ländern.

Aus diesem Grund hat das BSI die Zusammenarbeit mit den Ländern im Berichtszeitraum weiter ausgebaut. Ziel ist es, ein einheitlich hohes IT-Sicherheitsniveau in Deutschland zu schaffen. Dafür ist das BSI unter anderem in den Bund-Länder-Gremien aktiv und gestaltet die Zusammenarbeit mit den Ländern durch bilaterale Kooperationen und Veranstaltungsformate.

14.1 — Nationales Verbindungswesen

Das BSI hat seit 2017 insgesamt fünf Verbindungsstellen eröffnet, die für jeweils unterschiedliche Regionen im Bundesgebiet zuständig sind. Durch die Schaffung direkter Ansprechpartnerinnen und Ansprechpartner ist das BSI in der Fläche besser erreichbar. Dadurch kann es seine Aufgaben effizienter wahrnehmen und einen zusätzlichen Beitrag zur Erhöhung des gesamtstaatlichen Cybersicherheitsniveaus in Deutschland leisten. Regionale Verbände, Wirtschaftsunternehmen und auch Kommunal-, Landes-, Bundes- und EU-Behörden finden über die Verbindungsstellen einen kurzen Weg ins BSI und werden bei ihren Anliegen eng betreut. Ziel ist es, die Kooperation und Vernetzung zu stärken und einen aktiven Beitrag zu regionalen Netzwerkformaten zu leisten. Wesentliches Element ist hierbei der Abschluss von bilateralen Kooperationsvereinbarungen zwischen dem BSI und interessierten Ländern.

14.2 — Informationssicherheitsberatung für Länder und Kommunen

Die Informationssicherheitsberatung für Länder und Kommunen berät zielgruppenspezifisch Bedarfsträger auf Landes- und kommunaler Ebene zu allen Fragen der Informationssicherheit mit den thematischen Schwerpunkten Informationssicherheitsmanagement, Sicherheitskonzeption und IT-Grundschutz.

Länder

Die Beratung von Ländern konnte auf Basis der abgeschlossenen Kooperationsvereinbarungen ausgebaut werden. Neben den spezifischen Beratungen wurden praxisorientierte Lösungsansätze gemeinschaftlich mit Vertreterinnen und Vertretern aus Bund, Ländern und Kommunen weiterentwickelt. Dabei standen IT-Grundschutzprofile und skalierbare Handreichungen für den Einstieg und die Umsetzung des IT-Grundschutzes im Fokus. Hervorzuheben ist dabei das IT-Grundschutz-Profil „Schnellmeldungen – Absicherung der Schnellmeldungen bei bundesweiten parlamentarischen Wahlen“, das zum Jahreswechsel über den Bundeswahlleiter verteilt wurde.

Kommunen

Eine effiziente Zusammenarbeit mit fast 11.000 Kommunen erfordert strukturierte Ansätze, die nur gemeinsam mit Multiplikatoren aus den kommunalen Spitzenverbänden und Institutionen der Länder erfolgen kann.

Cyberangriffe auf Kommunen können weitreichende Auswirkungen auf die Bevölkerung haben, da auf dieser Ebene ein Großteil an Verwaltungsdienstleistungen für Bürgerinnen und Bürger erbracht wird. Umso wichtiger ist es, Kommunen bei der Einführung und der Umsetzung von Informationssicherheit zu unterstützen. Daher unterstützt die Informationssicherheitsberatung bei der Sensibilisierung der Management-Ebene im Rahmen von Kongressen und Tagungen und stellt für Informationssicherheitsbeauftragte über den internen Bereich für Länder und Kommunen unter anderem einen Werkzeugkasten und spezifische Hilfestellungen zum IT-Grundschutz bereit. Außerdem wird derzeit mit dem „Weg in die Basis-Absicherung – WiBA“ eine Einstiegsstufe in die etablierte Methodik des IT-Grundschutzes entwickelt. Mit WiBa wird eine Brücke zum IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung exklusiv für den kommunalen Sektor entwickelt, um zum Beispiel OZG-Anforderungen umsetzen zu können.

Im Berichtszeitraum unterstützte das BSI auf Initiative der kommunalen Spitzenverbände bei der Erstellung verschiedener Handreichungen für Führungskräfte in Verwaltungen. Diese bieten konkrete Hilfestellungen bei ersten Schritten für mehr Informationssicherheit.

14.3 — Roadshow Kommunen

Wie bereits berichtet, werden dem BSI regelmäßig erfolgreiche Cyberangriffe auf Kommunen bekannt (vgl. Kapitel *Landes- und Kommunalverwaltungen*, Seite 67). Aufgrund der zunehmenden ebenenübergreifenden Vernetzung stellen diese Angriffe auch eine gemeinsame Herausforderung für Bund, Länder und Kommunen dar. Das BSI hat deshalb die Roadshow Kommunen, eine virtuelle Veranstaltungsreihe für die Kommunen, entwickelt, die gemeinsam mit interessierten Ländern für die Zielgruppe Kommunen durchgeführt wird.

Die Planung und Durchführung der Veranstaltung erfolgt unter Einbeziehung der Länder und der kommunalen Spitzenverbände. Das BSI bringt unter anderem Vorträge aus den Bereichen Informationssicherheitsberatung für Länder und Kommunen, Nationales Verbindungswesen, *CERT-Bund*, BSI-Standards und IT-Grundschutz ein. Die Länder ergänzen diese mit unterschiedlichen, individuell auf das Land zugeschnittenen Vorträgen.

Ziel der Veranstaltung ist es, Kommunen bezüglich der Bedrohungen im Cyberraum zu sensibilisieren und Handlungsoptionen zur Erhöhung des Cybersicherheitsniveaus aufzuzeigen.

Im Berichtszeitraum wurden insgesamt sechs Roadshows Kommunen durchgeführt und weit über 700 Teilnehmende aus den Kommunen erreicht. Aufgrund der positiven Resonanz wird die Roadshow Kommunen fortgeführt und thematisch weiterentwickelt.

14.4 — Gremienarbeit

Das BSI arbeitet in beratender Rolle in unterschiedlichen Bund-Länder-Gremien im Bereich der Cyber- und Informationssicherheit mit, beispielsweise in der AG Informationssicherheit des IT-Planungsrates (AG InfoSic) und der Länderarbeitsgruppe Cybersicherheit (LAG Cybersicherheit) der Ständigen Konferenz der Innenminister und -senatoren der Länder (IMK).

Arbeitsgruppe Informationssicherheit

Das BSI berät den Bund und die Länder bei der Umsetzung der verschiedenen Handlungsfelder der „Leitlinie für Informationssicherheit der öffentlichen Verwaltung“ des IT-Planungsrats, die die strategischen ebenenübergreifenden Ziele zur Informationssicherheit definiert. Hierbei bringt das BSI seine Expertise ein und arbeitet aktiv in Arbeitsgruppen mit, wie zum Beispiel bei der Erstellung von Konzepten zum IT-Notfallmanagement und eines Standards zur Erkennung und Abwehr von IT-Angriffen. Außerdem betreibt das BSI die Geschäftsstelle der AG Informationssicherheit und unterstützt den jeweiligen Vorsitz (im Berichtszeitraum: Sachsen und Saarland) bei der Sitzungsdurchführung.

LAG Cybersicherheit

Die Innenministerkonferenz (IMK) unterhält eine LAG Cybersicherheit zur Abstimmung der länderübergreifenden fachlichen Zusammenarbeit im Themenfeld Cybersicherheit. Das BSI bringt seine Expertise hierbei in unterschiedlichen Unter-Arbeitsgruppen ein, im

Berichtszeitraum beispielsweise in die Arbeitsgruppe zur Umsetzung der Protokollerklärung zum IT-Sicherheitsgesetz. Ziel dieser Arbeitsgruppe ist es, die Informationsweitergabe zwischen BSI und den Ländern zu verbessern.

14.5 — Verwaltungs*CERT*-Verbund (VCV)

Die operative Zusammenarbeit mit den Ländern erfolgt über *CERT-Bund* im Rahmen des Verwaltungs-*CERT*-Verbundes (VCV). Der Informationsaustausch innerhalb des VCV ermöglicht es, bundesweit effektiver und schneller auf IT-Angriffe reagieren zu können. Dabei teilen die 13 verschiedenen Landes-*CERT*s lagerelevante Vorfallsinformationen und sprechen vertrauensvoll über operative Themen wie aktuelle Schwachstellen, die allgemeine Lage und Best-Practice-Ansätze. Der gemeinsame Austausch wurde im Berichtszeitraum auch in Anbetracht der abstrakt erhöhten Bedrohungslage intensiviert und durch bilaterale Gespräche, zwei hybride Arbeitstreffen und eine Hospitation von mehreren Landes-*CERT*s im BSI begleitet.

14.6 — Kooperationsvereinbarungen zwischen BSI und den Ländern

Bilaterale Kooperationsvereinbarungen zwischen dem BSI und den Ländern bilden den Rahmen der Zusammenarbeit und ermöglichen eine gegenseitige Unterstützung auf Augenhöhe im derzeit bestehenden Rechtsrahmen.

Das BSI kann gemäß § 3 BSIG die Länder in Fragen der Informationssicherheit beraten und warnen sowie auf deren Ersuchen bei der Sicherung ihrer Informationstechnik und Abwehr von Gefahren unterstützen. Basierend auf diesen Rahmenbedingungen hat das BSI einen Katalog von Kooperationsfeldern erarbeitet. Aus diesem können die Länder die Kooperationen auswählen, für die sie einen Bedarf haben.

Die Länder können diese Kooperationsangebote durch eigene Angebote ergänzen, die das BSI seinerseits nutzen kann. Es ist im Sinne der Kooperationsvereinbarung, dass mit dem BSI und den Ländern alle Kooperationspartner im gleichen Maße profitieren. Jede Vereinbarung kann so individuell auf die jeweiligen Bedarfe des Landes und des BSI zugeschnitten werden. In einem sogenannten Jahresarbeitsprogramm werden die Kooperationen, beispielsweise Beratungen zum Aufbau eines Managementsystems für Informationssicherheit, konkretisiert und dann sukzessive umgesetzt.

Zum aktuellen Stand hat das BSI vier Kooperationsvereinbarungen mit Ländern geschlossen. Weitere Vereinbarungen sind bereits geplant oder unmittelbar in Vorbereitung.

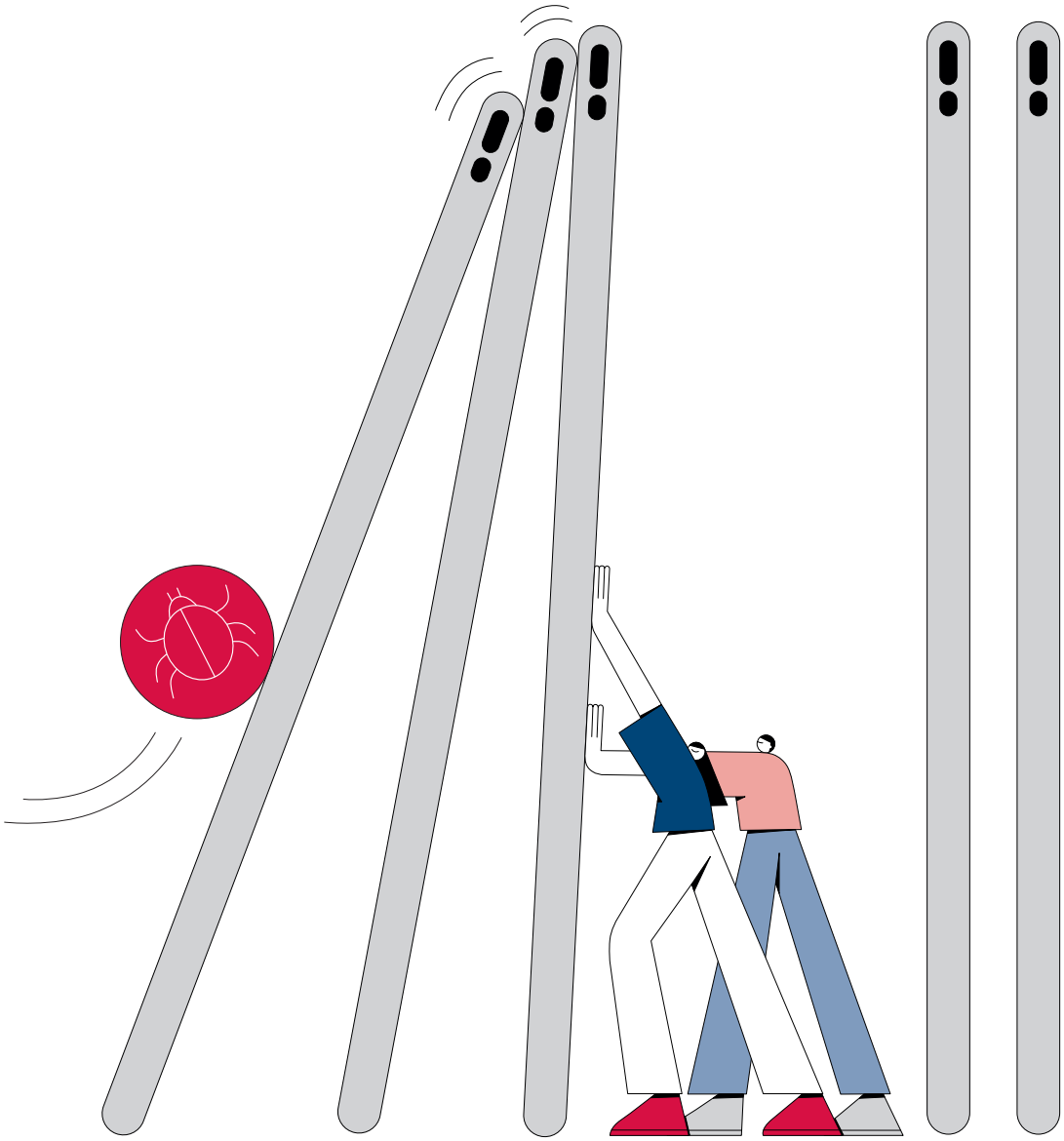
14.7 — Weiterentwicklung der Zusammenarbeit mit den Ländern

Die Kooperationsvereinbarungen zwischen dem BSI und den Bundesländern sind ein wichtiger Meilenstein auf dem Weg zu einer verbindlichen Bund-Länder-Zusammenarbeit im Bereich der Cybersicherheit. Sie schöpfen den derzeit gültigen Rechtsrahmen der ebenenübergreifenden Zusammenarbeit aus.

Allerdings gibt es den Bedarf an engerer Zusammenarbeit, um aktuellen und künftigen Bedrohungslagen im Cyberraum noch besser begegnen zu können. So hat das BSI aktuell zum Beispiel keine Möglichkeit, die Länder bei der Detektion von Schadsoftware in den Landesnetzen zu unterstützen, etwa durch Bereitstellung von Sensorik. Gleichzeit ist es im Sinne einer ganzheitlichen Betrachtung der Lage der Informationssicherheit in Deutschland zielführend, ein einheitliches Bund-Länder-Lagebild anzustreben. Ein vernetztes Lagebild ermöglicht es, in Gegenüberstellung zu einzelnen bundeslandspezifischen Erfassungen, Gefährdungstrends und grenzübergreifende Phänomene schneller und spezifischer zu identifizieren. Deshalb erarbeiten das BMI, das BSI und die Länder aktuell ein Konzept zum Ausbau des BSI zur Zentralstelle im Bund-Länder-Verhältnis, das einen Ausbau der gesetzlichen Grundlagen der Bund-Länder-Zusammenarbeit im Bereich Cybersicherheit näher beschreibt.

Aktuell werden die Vorhaben bzw. Bedarfe zwischen Bund und Ländern abgestimmt. Ziel der Bundesregierung ist es, durch eine Änderung des Grundgesetzes, die Zusammenarbeit zwischen Bund und Ländern im Bereich der Cybersicherheit zu verstetigen und zu vertiefen.

Fazit



Fazit

15. — Fazit

Resilienz ist das Gebot der Stunde

Die Bedrohungslage im Bereich der Cybersicherheit ist weiterhin von einer hohen Dynamik geprägt. Die rasante Entwicklung im Bereich der Künstlichen Intelligenz zeigt, wie schnell technische Neuerungen fortschreiten können. Diese bringt neben großen Chancen für die Digitalisierung auch ein hohes Bedrohungspotenzial mit sich. Nach wie vor bleiben Angriffe mit Ransomware die größte Bedrohung für die Cybersicherheit in Deutschland. Daneben rücken Cyberangriffe auf Lieferketten weiter in den Mittelpunkt. Sie können die Cybersicherheit ganzer Branchen gefährden.

Im vorliegenden Berichtszeitraum setzt sich die Entwicklung der Bedrohungslage demnach unverändert fort – sie gilt als angespannt bis kritisch. Wichtig ist daher, die Resilienz der Bundesrepublik Deutschland auch gegen Cyberangriffe und IT-Sicherheitsvorfälle weiter zu steigern.

Hauptrisiko Ransomware: größte Bedrohung für die Cybersicherheit in Deutschland

Bei Cyberangriffen mit *Ransomware* ist im Berichtszeitraum zu beobachten, dass das zuletzt vorherrschende Big Game Hunting abgenommen hat. Statt sich auf große, zahlungsfähige Unternehmen zu konzentrieren, haben Cyberkriminelle wieder vermehrt kleine und mittlere Unternehmen und auch staatliche Institutionen und Kommunen zum Ziel von *Ransomware*-Angriffen gemacht.

Immer häufiger sind auch Kommunalverwaltungen und kommunale Betriebe von erfolgreichen Cyberangriffen betroffen. Bürgerinnen und Bürger sind dabei oftmals auch unmittelbar betroffen. Entweder weil bürgernahe Dienstleistungen oft über Wochen nicht zur Verfügung stehen oder weil persönliche Daten in die Hände Krimineller gelangen. Dies zeigt, wie wichtig *Resilienz* ist. Sie umfasst auch die Fähigkeit, nach einem IT-Sicherheitsvorfall möglichst schnell wieder die erforderliche Handlungsfähigkeit zu erlangen und in den Normalzustand zurückkehren zu können.

Professionalisierung der Cyberkriminalität geht weiter

Bei der Cyberkriminalität ist eine stetig weiter voranschreitende Arbeitsteilung und Professionalisierung unter den Cyberkriminellen festzustellen, die sich in einem wachsenden Dienstleistungscharakter manifestiert. Die Schattenwirtschaft der Cyberkriminalität spiegelt damit in gewisser Weise die Realwirtschaft, die ebenfalls auf eine starke Arbeitsteilung setzt und sich immer stärker über Länder- und Branchengrenzen hinweg vernetzt.

Dieser Ausbau des Cybercrime-as-a-Service ist ein herausragender Faktor bei der Entwicklung der Bedrohungslage, denn die Spezialisierung auf bestimmte Dienstleistungen ermöglicht es Angreifenden, ihre Services gezielt zu entwickeln und zu professionalisieren. Dem lässt sich nur durch eine entsprechende Professionalisierung auf Abwehrseite entgegenwirken. Ein Mittel sind qualifizierte Sicherheitsexpertinnen und -experten – Dienstleister, die ihrerseits besonders gut geschützt sein müssen. Durch Standardisierung und Zentralisierung können Kommunen sowie kleine und mittlere Unternehmen ihre Cyberresilienz stärken. Eine Basisabsicherung nach dem IT-Grundschutz für Kommunen oder dem Cybersicherheitscheck für Unternehmen sind dafür wirksame Werkzeuge.

Schwachstellen bei Software auf besorgniserregendem Niveau

Eine beunruhigende Entwicklung ist auch im Bereich der Schwachstellen zu beobachten. Vor allem bei Schwachstellen von Softwareprodukten konnten starke Zuwächse registriert werden. Solche Lücken sind oft das erste Einfallstor für Cyberkriminelle auf ihrem Weg zu einer Kompromittierung von Systemen und Netzwerken. Die zunehmende und umfassende Vernetzung macht die Systeme überhaupt erst von außen zugänglich und erlaubt Angreifenden gleichzeitig, aus der Ferne zu agieren.

Im Berichtszeitraum wurden jeden Tag durchschnittlich knapp 70 neue Schwachstellen in Software-Produkten bekannt, rund ein Viertel mehr als im Berichtszeitraum davor. Mit der Anzahl der gefundenen Schwachstellen stieg auch ihre potenzielle Schadwirkung. 3.784 der identifizierten Lücken wurden als kritisch eingestuft (zuvor: 2.680). Das sind 15 Prozent aller festgestellten Schwachstellen. Die Entwicklung sowohl bei der Zahl als auch bei der Kritikalität sind besorgniserregend. Das BSI setzt dem unter anderem Initiativen zur (Teil-)Automatisierung von Unternehmens- und Security-Prozessen entgegen, beispielsweise durch die automatische Filterung der Meldung von Sicherheitslücken auf Relevanz für die eigenen Systeme. Die technische Grundlage hierfür ist das unter anderem vom BSI spezifizierte Common Security Advisory Format (CSAF), durch das Sicherheits-Advisories maschinenlesbar und automatisiert verarbeitbar sind.

Generative KI: Chance und Risiko für die Cybersicherheit

Das Aufkommen generativer Künstlicher Intelligenz führt im Sicherheitsbereich zu neuen Herausforderungen. Mit der Veröffentlichung von ChatGPT und einer Vielzahl weiterer Tools ist KI auch in einer breiten, wenig technikaffinen Öffentlichkeit angekommen. Große KI-Sprachmodelle, die hinter Modellen wie ChatGPT, LLaMA oder Bard stehen, sind teilweise frei verfügbar. Zu ihrem Aufschwung hat die hohe Qualität der von KI generierten Texte und Bilder beigetragen, ebenso die einfache Zugänglichkeit dieser und weiterer Tools, unter anderem für *Deepfakes*. Manipulierte Bilder, Videos und Stimmen werden durch die kontinuierliche Qualitätssteigerung der öffentlich zugänglichen Werkzeuge immer authentischer und dadurch schwerer zu entlarven.

Die Folgen sind vielfältig. Neben bereits bekannten Angriffen wie CEO-Fraud oder dem Enkeltrick werden die angesprochenen Tools auch von Cyberkriminellen auf weitere Einsatzfähigkeit bei Angriffen geprüft, zum Beispiel bei der Generierung von Schadcode oder bei Social Engineering und Desinformationskampagnen. Zu dieser Skalierung bereits bekannter Bedrohungen kommen neue Bedrohungen, die in der neuen Technik und der damit verbundenen Vergrößerung der Angriffsfläche begründet liegt. Künstliche Intelligenz selbst ist angreifbar und kann eine Schwachstelle sein. Unter anderem durch die Unschärfe im Design von KI und LLM steht das Schwachstellenmanagement in Unternehmen und Behörden vor noch nie da gewesenen Herausforderungen.

Neben diesen Sicherheitsrisiken ist die große Herausforderung, mit der rasanten Entwicklung im Bereich KI Schritt zu halten. Ziel muss es sein, über mögliche Sicherheitsrisiken bei der Verwendung von KI aufzuklären, um verantwortungsvoll mit den Fähigkeiten und Arbeitsergebnissen dieser Modelle umgehen zu können. So muss es technische Maßnahmen geben, um den Output von KI identifizieren zu können. Darüber hinaus müssen Hersteller und Anbieter von LLMs und LLM-basierten Anwendungen Vorkehrungen treffen, um die Erzeugung potenziell schädlicher Ausgaben weitestgehend zu verhindern oder zu erschweren.

Auswirkungen des Ukraine-Kriegs auf die IT-Sicherheitslage in Deutschland

Der russische Angriffskrieg gegen die Ukraine nahm im Berichtszeitraum weiterhin einen zentralen Platz in der öffentlichen Wahrnehmung ein. Die registrierten *DDoS-Angriffe* pro-russischer Aktivisten haben bisher wenig bis keinen bleibenden Schaden anrichten können. Da dies zum großen Teil auch an der gewählten Angriffsart D*DoS* liegt, sind die bisherigen Angriffe eher dem Bereich Propaganda zuzuordnen – mit dem Ziel, Verunsicherung zu stiften und das Vertrauen in den Staat zu untergraben. Die Vergangenheit hat gezeigt, dass sich dies jederzeit ändern kann, etwa durch Kollateralschäden oder Angriffe auf Kritische Infrastrukturen. Dem kann man mit einer ausgeprägten Cyberresilienz und der Lage angepassten Sicherheitsvorkehrungen durchaus erfolgreich begegnen.

Wachsam und handlungsfähig bleiben für eine erfolgreiche Digitalisierung

Cyberresilienz bedeutet, mit Angriffen umgehen zu können, ohne umzufallen. Cyberresilienz heißt auch, schnell wieder auf die Beine zu kommen, wenn man Opfer eines Cyberangriffs geworden ist – und sich wenn nötig auch wehren zu können. Um das zu schaffen, braucht es eine tragfähige Cybersicherheitsarchitektur.

Das BSI versteht sich als zentrale Stelle in der Sicherheitsarchitektur Deutschlands, die allen Akteuren Handlungsmöglichkeiten und Unterstützungsmaßnahmen anbietet. Diese zentrale Position sorgt nicht nur für mehr Effizienz, sondern ist auch für einen nachhaltigen Einsatz von Ressourcen geeignet. Deshalb begrüßt das BSI den von der Bundesregierung angestrebten Ausbau des BSI zur Zentralstelle im Bund-Länder-Verhältnis.

Cybersicherheit ist eine Gemeinschaftsaufgabe von Bund, Ländern und Kommunen, die nur mit einem adäquaten Ressourceneinsatz bewältigt werden kann. Das allein reicht aber nicht aus. Nötig ist der immerwährende Austausch zwischen Politik, Wirtschaft, Wissenschaft und Gesellschaft – in Deutschland, aber auch über Landesgrenzen hinweg.

Resilienz erhöhen – Cybersicherheit gestalten – Digitalisierung beschleunigen

Die Nationale Sicherheitsstrategie des Bundes betont die signifikant gestiegene Bedeutung von Cybersicherheit. Zu Recht, wie der BSI-Lagebericht zeigt. Als Cybersicherheitsbehörde des Bundes sieht das BSI seinen Auftrag darin,

- die Resilienz schnellstmöglich zu erhöhen, um Angriffen standzuhalten,
- Cybersicherheit pragmatisch zu gestalten, um Angreifern stets einen Schritt voraus zu sein,
- die Digitalisierung zu beschleunigen, um mit den Entwicklungen unserer Zeit Schritt zu halten.

Das alles kann gelingen, wenn die Positionen des BSI gehört, seine Vorgaben umgesetzt und seine Produkte genutzt werden. Das BSI wird seinen Beitrag dazu leisten, indem es seine Rolle als Partner, Helfer und Möglichmacher in Zukunft noch stärker ausfüllt: mit realistisch umsetzbaren Standards und einfach anwendbaren Lösungen für Staat, Wirtschaft und Gesellschaft. Ein Grundsatz, der das BSI dabei trägt: Abgrenzung gilt nicht – Kooperation gewinnt!

Glossar

Access Broker
Als *Access Broker* werden Cyberkriminelle bezeichnet, die sich über verschiedenste Wege Zugang zu einem Opfernetzwerk verschaffen und diesen Zugang regelmäßig an andere Cyberkriminelle oder interessierte Parteien veräußern.

Advanced Persistent Threats
Bei *Advanced Persistent Threats* (APT) handelt es sich um zielgerichtete Cyberangriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer persistenten (dauerhaften) Zugriff auf ein Netzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus und sind in der Regel schwierig zu detektieren.

Advisories/Security Advisories
Empfehlungen der Hersteller an IT-Sicherheitsverantwortliche in Unternehmen und anderen Organisationen zum Umgang mit aufgefundenen Schwachstellen.

Affiliates
Bei *Cybercrime-as-a-Service* wird der Cyberkriminelle, der den Service in Anspruch nimmt, in der Regel als *Affiliate* bezeichnet. Der Begriff leitet sich aus dem *Affiliate*-Marketing ab, bei dem ein kommerzieller Anbieter seinen Vertriebspartnern (*Affiliates*) Werbematerial zur Verfügung stellt und eine Provision anbietet. Im Kontext des Cybercrime wird statt Werbematerial beispielsweise eine *Ransomware* zur Verfügung gestellt und dem *Affiliate* eine Beteiligung am Lösegeld versprochen.

Angriffsvektor
Als *Angriffsvektor* wird die Kombination von Angriffsweg und -technik bezeichnet, mit der sich ein Angreifer Zugang zu IT-Systemen verschafft.

Authentifizierung
Die *Authentifizierung* bezeichnet den Vorgang, die Identität einer Person oder eines Rechnersystems anhand eines bestimmten Merkmals zu überprüfen. Dies kann unter anderem durch Passworteingabe, Chipkarte oder Biometrie erfolgen.

Backdoor
Eine *Backdoor* ist ein üblicherweise durch Viren, Würmer oder Trojanische Pferde installiertes Programm, das Dritten einen unbefugten Zugang (Hintertür) zum Computer verschafft, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen.

Backup
Unter *Backup* versteht man das Kopieren von Dateien oder Datenbanken auf physischen oder virtuellen Systemen an einen sekundären Speicherort, um diese im Falle eines Geräteausfalls oder einer Katastrophe für eine Wiederherstellung zu nutzen und bis dahin sicher vorzuhalten.

Bitcoin
Bitcoin (BTC) ist eine digitale Währung, sie wird auch Kryptowährung genannt. Durch Zahlungen zwischen pseudonymen Adressen wird die Identifizierung der Handelspartner deutlich erschwert.

Blockchain
Blockchain beschreibt eine verteilte, synchronisierte, dezentrale und konsensuale Datenhaltung in einem Peer-to-Peer-Netzwerk. Dabei wird redundant in allen Netzwerkknoten eine hashverkettete Liste von Datenblöcken geführt, die mithilfe eines Konsensverfahrens aktualisiert wird. *Blockchain* ist die technologische Grundlage für Kryptowährungen wie *Bitcoin*.

Bot / Botnetz
Als *Botnetz* wird ein Verbund von Rechnern (Systemen) bezeichnet, die von einem fernsteuerbaren Schadprogramm (*Bot*) befallen sind. Die betroffenen Systeme werden vom *Botnetz*-Betreiber mittels eines *Command-and-Control-Servers* (*C&C-Server*) kontrolliert und gesteuert.

Brute Forcing
Angriffsmethode nach dem Versuch-Irrtum-Prinzip. Angreifer probieren automatisch viele Zeichenkombinationen aus, um zum Beispiel Passwörter zu knacken und sich Zugang zu passwortgeschützten Systemen zu verschaffen.

Bug Bounty
Monetäre Belohnungen (Bounty) für das Finden von Schwachstellen (Bugs). Hersteller von Softwareprodukten verwenden legitime Bug-Bounty-Programme, um Sicherheitsforschende für das Finden und Melden einer Schwachstelle in ihrem Produkt zu belohnen.

CEO-Fraud
Als *CEO-Fraud* werden gezielte Social-Engineering-Angriffe auf Mitarbeitende von Unternehmen bezeichnet. Der Angreifer nutzt dabei zuvor erbeutete Identitätsdaten (z. B. Telefonnummern, Passwörter, E-Mail-Adressen etc.), um sich als Vorstandsvorsitzender (CEO), Geschäftsführung o. Ä. auszugeben und Mitarbeitende zur Auszahlung hoher Geldsummen zu veranlassen.

CERT / Computer Emergency Response Team
Computer-Notfallteam, das aus IT-Spezialisten besteht. In vielen Unternehmen und Institutionen sind mittlerweile *CERT*s etabliert, die sich um die Abwehr von Cyberangriffen, die Reaktion auf IT-Sicherheitsvorfälle sowie um die Umsetzung präventiver Maßnahmen kümmern.

CERT-Bund
Das *CERT-Bund* (*Computer Emergency Response Team* der Bundesverwaltung) ist im BSI angesiedelt und fungiert als zentrale Anlaufstelle für Bundesbehörden zu präventiven und reaktiven Maßnahmen bei sicherheitsrelevanten Vorfällen in Computersystemen.

Cloud / Cloud Computing
Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die im Rahmen von *Cloud Computing* angebotenen Dienstleistungen umfassen das komplette Spektrum der Informationstechnik und beinhalten u. a. Infrastrukturen (Rechenleistung, Speicherplatz), Plattformen und Software.

Command-and-Control-Server (C&C-Server)
Server-Infrastruktur, mit der Angreifer die in ein *Botnetz* integrierten infizierten Computersysteme (*Bots*) steuern. *Bots* (infizierte Systeme) melden sich in der Regel nach der Infektion bei dem *C&C-Server* des Angreifers, um dessen Befehle entgegenzunehmen.

CVSS-Score
Industriestandard, mit dem die Kritikalität von Schwachstellen international vergleichbar bewertet wird.

Cybercrime-as-a-Service (CCaaS)
Cybercrime-as-a-Service (*CCaaS*, Cybercrime als Dienstleistung) beschreibt einen Phänomenbereich des Cybercrime, bei dem Straftaten von Cyberkriminellen auftragsorientiert begangen bzw. dienstleistungsorientiert ermöglicht werden. So wird beispielsweise bei der dem *CCaaS* untergeordneten *Malware*-as-a-Service (*MaaS*) einem Cyberkriminellen von einem Außenstehenden oder einer darauf spezialisierten Angreifergruppe die *Malware* für die Begehung einer Straftat gegen Entgelt zur Verfügung gestellt und ggf. auch mit Updates und weiteren ähnlichen Services versorgt, ganz so wie die legale Softwareindustrie. Eine Art des *MaaS* ist *Ransomware*-as-a-Service (*RaaS*), bei dem oft die *Malware* für die Verschlüsselung eines infizierten Systems, Aktualisierungen dieser *Malware*, die Abwicklung der Lösegeldverhandlungen und -zahlungen und weitere Erpressungsmethoden gegen Entgelt zur Verfügung gestellt werden. Die mit *CCaaS* einhergehende Zergliederung eines Cyberangriffs in einzelne Services ermöglicht auch wenig IT-affinen Angreifern technisch anspruchsvolle Cyberangriffe.

Deepfake
Der Begriff „*Deepfake*“ ist eine umgangssprachliche Bezeichnung für Methoden, die dazu verwendet werden können, Identitäten in medialen Inhalten mithilfe von Methoden aus dem Bereich der Künstlichen Intelligenz gezielt zu manipulieren. Ein Beispiel hierfür sind Verfahren, die das in einem Video befindliche Gesicht einer Person mit dem Gesicht einer anderen Person tauschen, dabei jedoch die Gesichtsbewegungen unverändert lassen.

DoS / DDoS-Angriffe
Denial-of-Service(*DoS*)-Angriffe richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten *DoS*- oder *DDoS*(Distributed Denial of Service)-Angriff. *DDoS-Angriffe* erfolgen häufig durch eine sehr große Anzahl von Computern oder Servern.

Double Extortion
Angreifer versuchen nicht nur, Lösegeld für verschlüsselte Daten zu erpressen, sondern auch Schweigegeld für exfiltrierte Daten.

Drive-by-Download / Drive-by-Exploits
Drive-by-Exploits bezeichnen die automatisierte Ausnutzung von Schwachstellen auf einem PC. Dabei werden beim Betrachten einer Webseite ohne weitere Nutzerinteraktion Schwachstellen im Webbrowser, in Zusatzprogrammen des Browsers (*Plug-ins*) oder im Betriebssystem ausgenutzt, um Schadsoftware unbemerkt auf dem PC zu installieren.

Exploit
Als *Exploit* bezeichnet man eine Methode oder einen Programmcode, mit dem über eine Schwachstelle in Hard- oder Softwarekomponenten nicht vorgesehene Befehle oder Funktionen ausgeführt werden können. Je nach Art der Schwachstelle kann mithilfe eines *Exploits* z. B. ein Programm zum Absturz gebracht, Benutzerrechte ausgeweitet oder beliebiger Programmcode ausgeführt werden.

Hashwert
Ein *Hashwert* ist eine aus der Anwendung einer bestimmten Hashfunktion resultierende Zeichenkette aus Ziffern und Buchstaben. Der *Hashwert* besitzt eine definierte Länge und ermöglicht es daher, große Datenmengen (z. B. ein Schadprogramm) exakt in vergleichsweise wenigen Zeichen abzubilden. Bei der Hashfunktion handelt es sich um eine mathematische Funktion zur Umrechnung von Daten. Eine anschließende Rückrechnung

des *Hashwertes* in die ursprünglichen Daten ist praktisch kaum bzw. nur unter extrem hohem Rechenaufwand möglich.

Hybride Bedrohungen
Illegitime Einflussnahme fremder Staaten mithilfe von Maßnahmen in verschiedenen Räumen. Physische Angriffe können zum Beispiel durch Cyberangriffe oder Desinformationskampagnen begleitet werden.

Information Stealer
Schadprogramme, die es Cyberkriminellen ermöglichen, auf infizierten Geräten an unterschiedliche Arten persönlicher Daten, wie beispielsweise Login-Daten für verschiedene Onlinedienste, zu gelangen, ohne dass die Betroffenen dies bemerken.

Internet der Dinge / Internet of Things / IoT
Unter *Internet der Dinge* oder *Internet of Things* (*IoT*) versteht man informations- und sensortechnisch aufgerüstete Gegenstände, die aus der physischen und virtuellen Welt Daten erfassen, verarbeiten und speichern und miteinander vernetzt sind.

IT-Sicherheitsgesetz 2.0
Das „Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (IT-SiG 2.0) ist am 28. Mai 2021 in Kraft getreten. Das IT-SiG 2.0 ist die Weiterentwicklung des ersten IT-Sicherheitsgesetzes aus 2015.

Legitime Programme
Programme, die unschädliche, erwünschte Operationen ausführen.

MaaS
Malware-as-a-Service (siehe auch *CCaaS*).

Maliziös
In der IT-Sicherheit werden Programme oder Webseiten, die schädliche Operationen auf einem Computersystem ausführen können, als *maliziös* (boshaft, schädlich) bezeichnet.

Malware
Die Begriffe Schadfunktion, Schadprogramm, Schadsoftware und *Malware* werden häufig synonym benutzt. *Malware* ist ein Kunstwort, abgeleitet aus Malicious Software, und bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Beispiele sind Computerviren, Würmer und Trojanische Pferde. Schadsoftware ist üblicherweise für eine bestimmte Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben.

Mark-of-the-Web / MOTW
Ein *MOTW* kennzeichnet Download-Dateien, wenn diese aus einer wahrscheinlich nicht vertrauenswürdigen Quelle stammen. Öffnet ein Nutzer eine so markierte Datei, wird er entsprechend gewarnt.

Monero
Monero ist eine digitale Währung, sie wird auch Kryptowährung genannt. Durch Zahlungen zwischen pseudonymen Adressen wird die Identifizierung der Handelspartner deutlich erschwert.

NESAS
Zertifizierungsprogramm für 5G-Mobilfunkausrüstung (Network Equipment Security Assurance Scheme).

NESAS CCS-GI
Das nationale Zertifizierungsprogramm für 5G-Mobilfunkausrüstung (*NESAS* Cybersecurity Certification Scheme – German Implementation).

Network Attached Storage (NAS)
Ein mit einem Netzwerk verbundenes Speichergerät, das autorisierten Netzwerk-Nutzerinnen und -Nutzern das Speichern und Abrufen von Daten an einem zentralen Ort ermöglicht.

Password-Spraying
Angriffsmethode, bei der der Angreifer beliebte oder typische Passwörter (z. B. Test1234) verwendet, um auf zahlreiche Konten gleichzeitig Zugriff zu erlangen.

Patch / Patchmanagement
Ein *Patch* (Flicken) ist ein Softwarepaket, mit dem Softwarehersteller Schwachstellen in ihren Programmen schließen oder andere Verbesserungen integrieren. Das Einspielen dieser Updates erleichtern viele Programme durch automatische Update-Funktionen. Als *Patchmanagement* bezeichnet man Prozesse und Verfahren, die helfen, verfügbare *Patches* für die IT-Umgebung möglichst rasch erhalten, verwalten und einspielen zu können.

Phishing
Das Wort setzt sich aus Password und fishing zusammen, zu Deutsch: nach Passwörtern angeln. Der Angreifer versucht dabei, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten einer Internetnutzerin oder eines Internetnutzers zu gelangen und diese für seine Zwecke, meist zulasten des Opfers, zu missbrauchen.

Plug-in
Ein *Plug-in* ist eine Zusatzsoftware oder ein Softwaremodul, das in ein Computerprogramm eingebunden werden kann, um dessen Funktionalität zu erweitern.

Proliferation
Der Begriff stammt ursprünglich aus der militärischen Verteidigung und bezeichnet die Weitergabe von Massenvernichtungswaffen einschließlich ihres technischen Know-hows sowie des zu ihrer Herstellung benötigten Materials. In der IT-Sicherheit wird der Begriff entsprechend für die Weitergabe von Cyberwaffen (Software und Methoden) unter Angreifern verwendet. Durch *Proliferation* können sich Angriffsmittel und –wege sehr schnell unter verschiedenen Angreifergruppierungen verbreiten, ohne dass diese jeweils spezifische technische Kompetenzen aufbauen müssen.

Provider
Dienstanbieter mit verschiedenen Schwerpunkten, zum Beispiel Netzwerk-*Provider*, der als Mobilfunk-*Provider*, Internet-Service-*Provider* oder Carrier die Infrastrukturen für den Daten- und Sprachtransport bereitstellt, oder Service-*Provider*, der über die Netzwerkbereitstellung hinausgehende Dienstleistungen erbringt, beispielsweise den Netzbetrieb einer Organisation oder die Bereitstellung von sozialen Medien.

Public-Key-Kryptografie
Bei der *Public-Key-Kryptografie* bzw. der asymmetrischen Verschlüsselung gibt es immer zwei sich ergänzende Schlüssel. Ein Schlüssel, der Public Key, dient zur Verschlüsselung einer Nachricht, ein anderer, der Private Key, dient zum Entschlüsseln. Beide Schlüssel zusammen bilden ein Schlüsselpaar.

Quellcode
Der *Quellcode* eines Computerprogrammes ist die in einer Programmiersprache verfasste, für Menschen lesbare Beschreibung des Ablaufs des Programms. Der *Quellcode* wird durch ein Programm in eine Abfolge von Anweisungen übersetzt, die der Computer ausführen kann.

Ransomware
Als *Ransomware* werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (engl. ransom) wieder freigeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.

RaaS
Ransomware-as-a-Service (siehe auch *CCaaS*).

Resilienz
Der Begriff bezeichnet im vorliegenden Zusammenhang die Widerstandsfähigkeit von IT-Systemen gegen Sicherheitsvorfälle oder Angriffe. Die *Resilienz* von Systemen ergibt sich aus einem komplexen Zusammenspiel von organisatorischen und technischen Präventivmaßnahmen wie zum Beispiel Fachpersonal, IT-Sicherheitsbudget, verfügbare technische Infrastrukturen oder Ähnliches.

RSA
Der Begriff bezeichnet ein Verfahren der *Public-Key-Kryptografie*, das für Signaturen und Verschlüsselung eingesetzt wird und nach den Entwicklern Rivest, Shamir und Adleman benannt ist. Ein Teil des öffentlichen Schlüssels von *RSA* besteht aus dem *RSA*-Modul n, einer natürlichen Zahl, die das Produkt zweier geheimer Primzahlen p und q ist. Die Sicherheit von *RSA* beruht insbesondere auf der Schwierigkeit, den *RSA*-Modul n zu faktorisieren, d. h. nur aus Kenntnis von n die beiden Primfaktoren p und q zu berechnen.

Security Advisory
Empfehlungen an IT-Sicherheitsverantwortliche zum Umgang mit aufgefundenen Schwachstellen.

Security Assurance Specification (SCAS)
*Security Assurance Specification*s (*SCAS*) definieren wichtige Sicherheitsfunktionen, die auch Grundlage für die Produktzertifizierung nach *NESAS CCS-GI* bilden.

Scam-Mail
Betrugsmail: Kategorie von *Spam*-Mails, mit denen Angreifer vorgeben, z. B. Spendengelder zu sammeln.

Security by Design
Nach dem Prinzip *Security by Design* gehen Hersteller vor, wenn Anforderungen aus der Informationssicherheit bereits bei der Entwicklung eines Produktes berücksichtigt werden.

Seitenkanalangriff
Angriff auf ein kryptografisches System, der die Ergebnisse von physikalischen Messungen am System (zum Beispiel Energieverbrauch, elektromagnetische Abstrahlung, Zeitverbrauch einer Operation) ausnutzt, um Einblick in sensible Daten zu erhalten. *Seitenkanalangriff*e sind für die praktische Sicherheit informationsverarbeitender Systeme von hoher Relevanz.

Sinkhole
Als *Sinkhole* wird ein Computersystem bezeichnet, auf das Anfragen von botnetzinfizierten Systemen umgeleitet werden. *Sinkhole*-Systeme werden typischerweise von Sicherheitsfor-

scherinnen und -forschern betrieben, um *Botnet*infektionen aufzuspüren und betroffene Anwenderinnen und Anwender zu informieren.

Script-Kiddies
Angreifer, die trotz mangelnder Kenntnisse versuchen, in fremde Computersysteme einzudringen oder generell Schaden anzurichten.

Social Engineering
Bei Cyberangriffen durch *Social Engineering* versuchen Kriminelle, ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren. Sowohl im Bereich der Cyberkriminalität als auch bei der Spionage gehen die Angreifer geschickt vor, um vermeintliche menschliche Schwächen wie Neugier oder Angst auszunutzen und so Zugriff auf sensible Daten und Informationen zu erhalten.

Spam
Unter *Spam* versteht man unerwünschte Nachrichten, die massenhaft und ungezielt per E-Mail oder über andere Kommunikationsdienste versendet werden. In der harmlosen Variante enthalten *Spam*-Nachrichten meist unerwünschte Werbung. Häufig enthalten *Spam*-Nachrichten jedoch auch Schadprogramme im Anhang, Links zu verseuchten Webseiten oder sie werden für *Phishing*-Angriffe genutzt.

Stack Overflow
Ein *Stack Overflow* oder Pufferüberlauf ist eine oft auftretende und häufig ausgenutzte Schwachstelle. Ein Pufferüberlauf tritt auf, wenn es gelingt, mehr Daten in einen Speicher zu schreiben, als der dafür vorgesehene Puffer aufnehmen kann. Dadurch werden auch angrenzende Speicherbereiche mit Daten beschrieben. Die Folge können Programmabstürze, Kompromittierung der Daten, Verschaffen erweiterter Rechte oder Ausführung von Schadcode sein.

Trusted Execution Environment (TEE)
Ein *Trusted Execution Environment* (*TEE*) bezeichnet einen isolierten Teil innerhalb eines Systems, der eine besonders geschützte Laufzeitumgebung bereitstellt. Das *TEE* kann bspw. Bestandteil des Hauptprozessors (CPU) oder Teil des Ein-Chip-Systems (SoC) eines Smartphones sein. Das *TEE* schützt die Integrität und Vertraulichkeit der enthaltenen Daten und des Schlüsselmaterials vor unautorisierten Dritten, zum Beispiel auch der Nutzerin oder dem Nutzer eines Geräts. Lediglich autorisierten Stellen ist es möglich, Anwendungen in das *TEE* einzubringen oder zu verändern.

UP KRITIS
Der Umsetzungsplan Kritische Infrastrukturen (*UP KRITIS*) ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und staatlichen Stellen wie dem BSI.

Virtuelles Privates Netz (VPN)
Ein *Virtuelles Privates Netz (VPN)* ist ein Netz, das physisch innerhalb eines anderen Netzes (oft des Internets) betrieben wird, jedoch logisch von diesem Netz getrennt wird. In *VPN*s können unter Zuhilfenahme kryptografischer Verfahren die Integrität und Vertraulichkeit von Daten geschützt und die Kommunikationspartner sicher authentifiziert werden, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind. Der Begriff *VPN* wird oft als Bezeichnung für verschlüsselte Verbindungen verwendet, zur Absicherung des Transportkanals können jedoch auch andere Methoden eingesetzt werden, beispielsweise spezielle Funktionen des genutzten Transportprotokolls.

Webshell
Schadcode, den Angreifer nach dem Einbruch auf einem Webserver installieren. *Webshell*s ermöglichen Angreifern den Remote-Zugang zu Servern und können für die Ausführung von Schadcode verwendet werden.

Wiper
Schadsoftware, die Daten vernichtet. Im Gegensatz zu *Ransomware* zielen *Wiper* nicht auf Verschlüsselung mit anschließender Erpressung, sondern auf Sabotage durch endgültige Vernichtung von Daten.

Zwei- bzw. Multifaktor-Authentifizierung (2FA bzw. MFA)
Bei der *Zwei- bzw. Multifaktor-Authentifizierung* erfolgt die *Authentifizierung* einer Identität anhand verschiedener *Authentifizierung*sfaktoren aus getrennten Kategorien (Wissen, Besitz oder biometrische Merkmale).

Quellenverzeichnis

1) https://www.heise.de/news/Mehrere-Verhaftungen-Strafverfolger-gehen-gegen-D*DoS*-Booter-Dienste-vor-7396504.html
2) https://www.hertzbleed.com/hertzbleed.pdf
3) https://eprint.iacr.org/2022/975
4) https://samcurry.net/web-hackers-vs-the-auto-industry/
5) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/onlineshopping-plattformen.html
6) https://www.verbraucherzentrale.de/geld-versicherungen/phishingradar-archiv-71872
7) https://www.verbraucherzentrale.de/geld-versicherungen/phishingradar-archiv-71872
8) Studie des TÜV-Verbandes: „2023: Cybersicherheit in deutschen Unternehmen“
9) https://de.statista.com/infografik/26033/ausgaben-fuer-it-sicherheit-in-deutschland
10) https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022
11) https://www.dihk.de/resource/blob/91514/be8371c167a1468d387fdaa075327330/dihk-sonderauswertung-cybersicherheit-2023-data.pdf
12) https://eur-lex.europa.eu/eli/dir/2022/2555/oj
13) https://eur-lex.europa.eu/eli/dir/2022/2557/oj
14) https://www.bsi.bund.de/OHNachweise
15) https://www.dihk.de/resource/blob/91514/be8371c167a1468d387fdaa075327330/dihk-sonderauswertung-cybersicherheit-2023-data.pdf
16) https://www.dihk.de/resource/blob/91516/aac9a26dea81dc7c1bc1e5f28b6105e8/dihk-digitalisierungsumfrage-2022-2023-data.pdf
17) NKMG mbH & BIGS gGmbh im Auftrag des Bundesministeriums für Wirtschaft und Energie: IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU in Deutschland, 2021, S. 5
18) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/AIMobilityAuditPrep_final_results.pdf
19) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive.html
20) https://www.vice.com/en/article/dy7axa/how-i-broke-into-a-bank-account-with-an-ai-generated-voice
21) https://iopscience.iop.org/article/10.1088/2058-9565/ab4eb5/pdf
22) https://www.bsi.bund.de/dok/QML
23) https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/, https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf
24) https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.pdf
25) https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf
26) https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.pdf
27) https://dserver.bundestag.de/btd/20/066/2006610.pdf
28) https://csrc.nist.gov/publications/detail/nistir/8413/final
29) https://www.bsi.bund.de/dok/umfrage-pqc
30) https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/01.01.01_60/gs_QKD016v010101p.pdf
31) https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eIDAS+eID+Profile

Verzeichnis der im Dokument abgebildeten QR-Codes

a) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/dvs-bericht_2022.html
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive-2022-2023.html
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Lagebild_Gesundheit_2022.html
https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Broschueren/broschueren_node.html

b) https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/*Botnetze*/Fragen-und-Antworten/fragen-und-antworten_node.html

c) https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/APT/apt_node.html
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/*Ransomware*-Angriffe/ransomware-angriffe_node.html
https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/unternehmen_node.html
https://www.bsi.bund.de/dok/CSN

d) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.pdf

e) https://www.bsi.bund.de/ddos

f) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

g) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive-2022-2023.pdf

h) https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/Massnahmenkatalog/massnahmenkatalog_node.html

i) https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/Notfallkarte/One-Pager_Einstieg_ins_IT-Notfallmanagement_KMU.pdf

j) https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/UP-KRITIS/up-kritis_node.html

k) www.bsi.bund.de/kmu

l) www.bsi.bund.de/dok/crc.

m) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Grosse_KI_Sprachmodelle.pdf

n) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Automotive/Automatisiertes_Fahren/Automatisiertes_Fahren_node.html

o) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Security-of-AI-systems_fundamentals_considerations_symbolic_hybrid.pdf
https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/ML-SAST/ml-sast_node.html
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/KI/P464_Provision_use_external_data_trained_models.pdf

p) https://www.bsi.bund.de/qcstudie

q) https://www.bsi.bund.de/PQ-Migration

r) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

s) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03163/tr03163_node.html

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185–189
53175 Bonn

E-Mail
bsi@bsi.bund.de

Telefon
+49 (0) 22899 9582-0

Telefax
+49 (0) 22899 9582-5400

Stand
Oktober 2023

Druck
Appel & Klinger Druck und Medien GmbH, Schneckenlohe

Gestaltung
Faktor 3 AG

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Illustrationen
Anne Albert c/o kombinatrotweiss.de
Instagram: annealbert_illustration | kombinatrotweiss_illustration

Grafiken
Bundesamt für Sicherheit in der Informationstechnik (BSI)

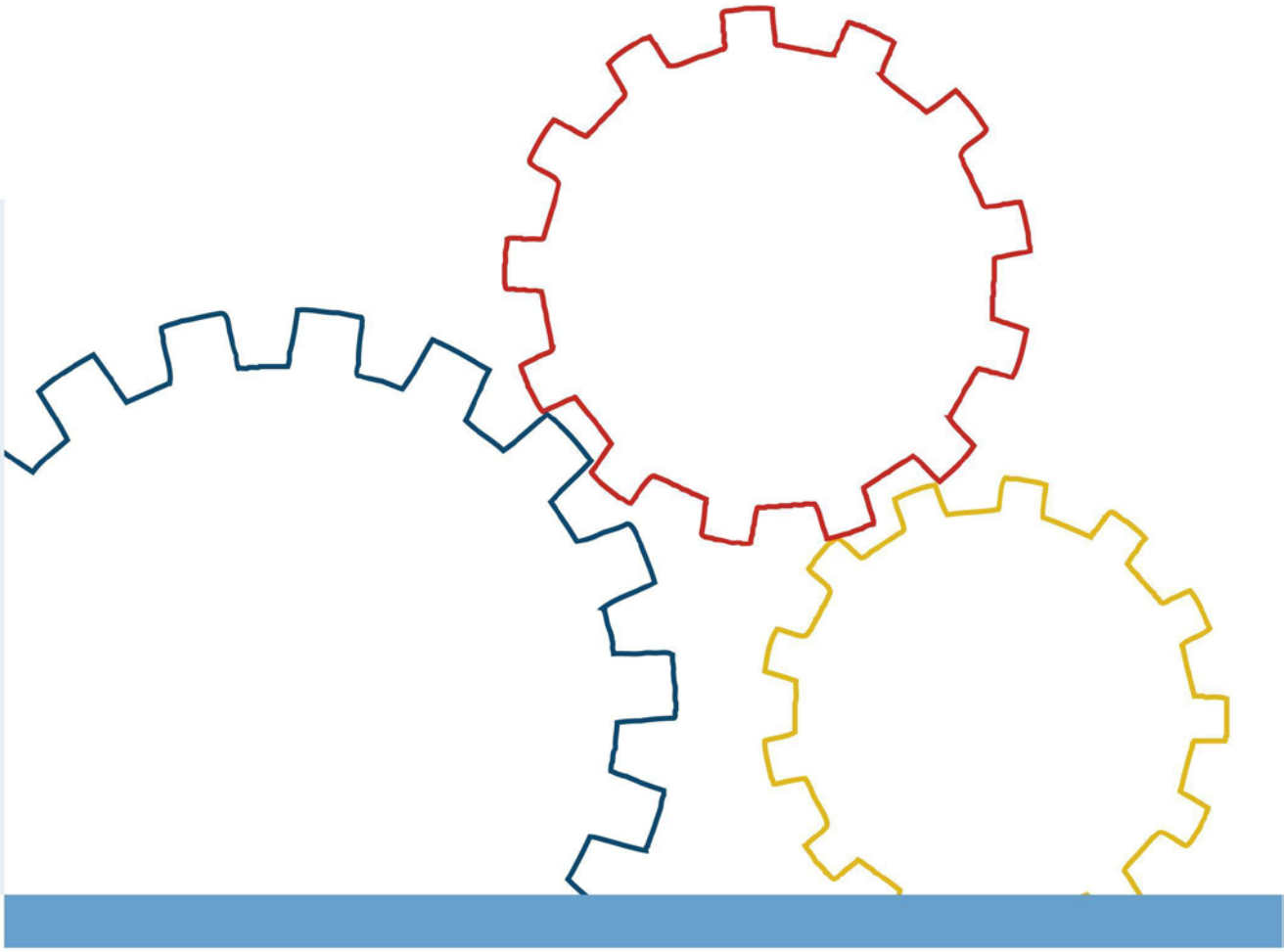
Bildnachweis
Seite 2: © BMI; Seite 4: © BMI/Henning Schacht

Artikelnummer
BSI-LB23/512

Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Standard 200-2

IT-Grundschutz-Methodik



www.bsi.bund.de/grundschutz

Version 1.0

Inhaltsverzeichnis

BSI-Standard 200-2
IT-Grundschutz-Methodik

1 Einleitung

1.1 Versionshistorie

Der BSI-Standard 200-2 löst den BSI-Standard 100-2 ab.

Stand	Version	Änderungen
März 2017	CD 1.0	Neukonzeption basierend auf BSI-Standard 100-2 • Im Rahmen der Modernisierung des IT-Grundschutzes wurden neben der Standard-Absicherung die Vorgehensweisen zur Basis-Absicherung und Kern-Absicherung eingefügt. • Erweiterung um Virtualisierung, Cloud-, ICS- und IoT-Absicherung • Klarstellung der Rollen und Aufgaben von IT-SiBe und ISB • Anpassungen an Fortschreibung der ISO-Standards • Informationsklassifizierung stärker herausgearbeitet • Informationsfluss im Informationssicherheitsprozess überarbeitet, Angleichung mit 100-4 • Beispiel BoV durch RECPLAST ausgetauscht
Oktober 2017	Version 1.0	Einarbeitung von Anwenderkommentaren • im Wesentlichen sprachliche Präzisierungen • Änderung des Begriffs „Aktiva“ in „Assets“

1.2 Zielsetzung

Mit dem BSI-Standard 200-2 stellt das BSI eine Methodik für ein effektives Management von Informationssicherheit zur Verfügung. Diese kann an die Anforderungen von Institutionen verschiedenster Art und Größe angepasst werden. Im BSI-Standard 200-2 wird dies über die drei Vorgehensweisen „Standard-Absicherung“, „Basis-Absicherung“ und „Kern-Absicherung“ realisiert.

Die Methodik baut auf dem BSI-Standard 200-1 *Managementsysteme für die Informationssicherheit (ISMS)* (siehe [BSI1]) und damit auch auf ISO 27001 [27001] auf. In diesem Dokument wird aufgezeigt, wie der im BSI-Standard 200-1 vorgestellte grundlegende Rahmen für ein Informationssicherheitsmanagementsystem durch IT-Grundschutz konkretisiert wird. Ein Managementsystem für die Informationssicherheit (ISMS) ist das geplante und organisierte Vorgehen, um ein angemessenes Sicherheitsniveau für die Informationssicherheit zu erzielen und aufrechtzuerhalten.

Der IT-Grundschutz ist ein etablierter Standard zum Aufbau und zur Aufrechterhaltung eines angemessenen Schutzes aller Informationen einer Institution. Die vom BSI kontinuierlich weiterentwickelte Methodik bietet sowohl Anleitungen für den Aufbau eines ISMS als auch eine umfassende Basis für die Risikoanalyse, die Überprüfung des vorhandenen Sicherheitsniveaus und die Implementierung eines angemessenen Grades an Informationssicherheit.

Eines der wichtigsten Ziele des IT-Grundschutzes ist es, den Aufwand im Informationssicherheitsprozess zu reduzieren. Dazu werden bekannte Ansätze und Methoden zur Verbesserung der Informationssicherheit gebündelt und kontinuierlich aktualisiert. Ergänzend veröffentlicht das BSI im IT-Grundschutz-Kompendium Bausteine mit konkreten Sicherheitsanforderungen für typische Geschäftsprozesse, Anwendungen, Systeme, Kommunikationsverbindungen und Räume, die nach Bedarf in der eigenen Institution eingesetzt werden können. Im IT-Grundschutz werden alle Bereiche einer Institution betrachtet, dazu gehören Produktion und Fertigung mit Industrial Control Systems (ICS) ebenso wie Komponenten aus dem Bereich des Internet of Things (IoT).

Durch die Umsetzung von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsanforderungen wird mit der Vorgehensweise „Standard-Absicherung" ein Sicherheitsniveau für die betrachteten Geschäftsprozesse erreicht, das für den normalen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen. Bei der Umsetzung der Vorgehensweise „Basis-Absicherung" wird ein Sicherheitsniveau erreicht, das zwar deutlich unter dem der Standard-Absicherung liegt, aber eine gute Grundlage für ISMS-Einsteiger bietet. Mit der Vorgehensweise „Kern-Absicherung" können besonders schützenswerte Informationen und Geschäftsprozesse vorrangig abgesichert werden.

Die IT-Grundschutz-Methodik wird regelmäßig erweitert und an die aktuellen Entwicklungen angepasst, die sich durch neue Prozesse, Normen und Regularien, vor allem aber durch die stetig fortschreitende Digitalisierung ergeben. Aufgrund des engen Erfahrungsaustauschs mit den Anwendern des IT-Grundschutzes fließen stetig neue Anforderungen und Aspekte in die Veröffentlichungen ein. Die Anwender können daher mit aktuellen Empfehlungen an einem ISMS für ihre Institution arbeiten und typische Sicherheitsprobleme schnell identifizieren und beheben.

1.3 Adressatenkreis

Der BSI-Standard 200-2 richtet sich primär an Sicherheitsverantwortliche, -beauftragte, -experten, -berater und alle Interessierten, die mit dem Management von Informationssicherheit betraut sind. Er ist zugleich eine sinnvolle Grundlage für IT- und ICS-Verantwortliche, Führungskräfte und Projektmanager, die dafür Sorge tragen, dass Aspekte der Informationssicherheit in ihrer Institution bzw. in ihren Projekten ausreichend berücksichtigt werden.

Der IT-Grundschutz bietet Institutionen jeder Größe und Sparte eine kosteneffektive und zielführende Methode zum Aufbau und zur Umsetzung der für sie angemessenen Informationssicherheit. Der Begriff „Institution" wird im folgenden Text für Unternehmen, Behörden und sonstige öffentliche oder private Organisationen verwendet.

IT-Grundschutz kann sowohl von kleinen als auch großen Institutionen eingesetzt werden. Dabei sollte aber beachtet werden, dass alle Empfehlungen im Kontext der jeweiligen Institution betrachtet werden sollten und an die jeweiligen Rahmenbedingungen angepasst werden müssten.

Im IT-Grundschutz gilt die Voraussetzung, dass die Informations- und Kommunikationstechnik ebenso wie die vorhandene industrielle Steuerungs- und Automatisierungstechnik von Fachpersonal administriert wird, dass es also einen IT-Betrieb mit klar definierten Rollen gibt. Dieser kann von einem einzelnen Administrator bis hin zu einer oder mehreren IT-Abteilungen reichen. Davon ausgehend werden die verschiedenen Aktivitäten im Sicherheitsprozess beschrieben.

1.4 Anwendungsweise

Im BSI-Standard 200-1 *Managementsysteme für Informationssicherheit (ISMS)* wird beschrieben, mit welchen Methoden Informationssicherheit in einer Institution generell initiiert und gesteuert werden kann. Der vorliegende BSI-Standard 200-2 bietet konkrete Hilfestellungen, wie ein Managementsystem für die Informationssicherheit Schritt für Schritt eingeführt werden kann: Im Fokus stehen hier somit einzelne Phasen dieses Prozesses sowie bewährte Best-Practice-Lösungen.

Die IT-Grundschutz-Methodik bietet ein umfangreiches Gerüst für ein ISMS und ist auf die individuellen Rahmenbedingungen einer Institution anzupassen, damit ein geeignetes Managementsystem für die Informationssicherheit aufgebaut werden kann. Für einen kontinuierlichen und effektiven Prozess der Informationssicherheit ist es entscheidend, eine ganze Reihe von Aktionen durchzuführen. Hierfür liefern die IT-Grundschutz-Methodik und das IT-Grundschutz-Kompendium zentrale Hinweise und praktische Umsetzungshilfen.

Des Weiteren bietet dieser Standard die Möglichkeit einer Zertifizierung an. Damit kann eine Institution nicht nur die Umsetzung von IT-Grundschutz, sondern auch die Qualität des eigenen ISMS mithilfe eines ISO 27001-Zertifikates auf Basis von IT-Grundschutz nachweisen. Das Zertifikat dient zugleich anderen Institutionen als Kriterium, um sich über den Reifegrad eines ISMS einer anderen Institution informieren zu können.

Eine Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz kann auch als Sicherheitsanforderung für mögliche Kooperationspartner verwendet werden, um das erforderliche Niveau an Informationssicherheit bei der anderen Institution zu definieren.

Auch wenn als Grundlage für das ISMS eine andere Methodik angewendet wird, ist es trotzdem möglich, vom IT-Grundschutz zu profitieren. So bietet der IT-Grundschutz auch Lösungsansätze für einzelne Aufgabenstellungen, beispielsweise für die Erstellung von Konzepten oder die Durchführung von Revisionen und Zertifizierungen im Bereich der Informationssicherheit. Je nach Anwendungsbereich bilden bereits einzelne Bausteine, Umsetzungshinweise oder weitere Hilfsmittel, die der IT-Grundschutz zur Verfügung stellt, hilfreiche Grundlagen für die Arbeit des Sicherheitsmanagements.

1.5 Aufbau des BSI-Standards 200-2

Kapitel 2 enthält die wichtigsten Schritte für die Einführung eines ISMS sowie der Erstellung einer Sicherheitskonzeption.

In Kapitel 3 wird beschrieben, wie die grundlegende Phase der Initiierung des Informationssicherheitsprozesses aussehen kann und welche Hintergrundinformationen erforderlich sind, um eine fundierte Entscheidung über die für die Institution geeignete Vorgehensweise zur Absicherung ihrer Informationen und Geschäftsprozesse zu treffen. Als wesentliche Grundlage für die weiteren Aktivitäten ist eine Leitlinie zur Informationssicherheit zu erstellen.

Für den Sicherheitsprozess müssen geeignete Organisationsstrukturen aufgebaut und ein funktionierendes Sicherheitsmanagement muss eingerichtet werden, siehe Kapitel 4.

Im Rahmen eines funktionierenden Sicherheitsprozesses müssen diverse Dokumentationen erstellt werden. Was hierbei zu beachten ist, wird in Kapitel 5 näher beschrieben.

Kapitel 6 veranschaulicht, wie vorzugehen ist, wenn als Vorgehensweise die Basis-Absicherung ausgewählt wurde. Die Basis-Absicherung verfolgt das Ziel, als Einstieg in den IT-Grundschutz zunächst eine breite, grundlegende Erst-Absicherung über alle Geschäftsprozesse bzw. Fachverfahren einer

Institution hinweg zu erzielen. Nach der Festlegung des Geltungsbereichs muss eine Auswahl und Zuordnung der IT-Grundschutz-Bausteine erfolgen und die Reihenfolge ihrer Anwendung festgelegt werden. Mit einem IT-Grundschutz-Check wird geprüft, inwieweit die Basis-Anforderungen bereits umgesetzt sind. Anschließend müssen konkrete Maßnahmen zur Erfüllung der offenen Anforderungen abgeleitet und umgesetzt werden. Durch die Auswahl einer der nachfolgenden Vorgehensweisen sollte das so erreichte Sicherheitsniveau aufrechterhalten und verbessert werden.

Wie ein vorgezogener Schutz der essenziellen Assets nach IT-Grundschutz mit der Kern-Absicherung erzielt werden kann, wird in Kapitel 7 verdeutlicht. Die Vorgehensweise orientiert sich dabei stark an den Schritten der Vorgehensweise zur Standard-Absicherung, die im darauffolgenden Kapitel 8 näher beschrieben werden soll.

Kapitel 8 widmet sich demnach der Vorgehensweise zur Standard-Absicherung. Dabei wird aufgezeigt, wie zunächst die Grundinformationen über einen Informationsverbund erhoben werden und diese durch Gruppenbildung reduziert werden können. Anschließend muss ausgehend von den Geschäftsprozessen der Schutzbedarf für Anwendungen, IT-Systeme, Kommunikationsverbindungen und Räume festgestellt werden. Aus den Empfehlungen des IT-Grundschutz-Kompendiums müssen ferner die für den jeweiligen Informationsverbund passenden Bausteine und Anforderungen ausgewählt, also die Modellierung nach IT-Grundschutz durchgeführt werden. Aus den gewählten Anforderungen erfolgt die Ableitung von Sicherheitsmaßnahmen. Vor der Realisierung von Sicherheitsmaßnahmen müssen vorhandene und zusätzliche Sicherheitsmaßnahmen, die beispielsweise durch die Risikoanalyse auf der Basis von IT-Grundschutz gemäß BSI-Standard 200-3 (siehe [BSI3]) ermittelt wurden, in das Sicherheitskonzept integriert werden.

Wie die Umsetzung der identifizierten und konsolidierten Sicherheitsmaßnahmen durchgeführt werden sollte, wird anschließend in Kapitel 9 beschrieben.

Die wesentliche Aufgabe eines ISMS ist es, die Aufrechterhaltung der Informationssicherheit zu gewährleisten und diese fortlaufend zu verbessern. Dieses Thema wird in Kapitel 10 vertiefend behandelt.

Die Vorgehensweisen nach IT-Grundschutz und das IT-Grundschutz-Kompendium werden nicht nur für die Sicherheitskonzeption, sondern auch als Referenzen im Sinne eines Sicherheitsstandards verwendet. Durch eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz kann eine Institution nach innen und außen hin dokumentieren, dass sie sowohl ISO 27001 als auch den IT-Grundschutz in der erforderlichen Tiefe umgesetzt hat. Kapitel 11 liefert einen kurzen Überblick darüber, welche Schritte hierfür notwendig sind, und erläutert abschließend, welche Bedingungen für eine erfolgreiche Zertifizierung erfüllt werden müssen.

2 Informationssicherheitsmanagement mit IT-Grundschutz

Informationen sind ein wesentlicher Wert für Unternehmen und Behörden und müssen daher angemessen geschützt werden. Die meisten Informationen werden heutzutage mit Informationstechnik (IT) erstellt, gespeichert, transportiert oder weiterverarbeitet. Moderne Geschäftsprozesse sind heute in Wirtschaft und Verwaltung ohne IT-Unterstützung längst nicht mehr vorstellbar. In Produktion und Fertigung hat mit Industrial Control Systems (ICS) die Informations- und Kommunikationstechnik ebenso Einzug gehalten wie das Internet of Things (IoT) in fast jedem anderem Bereich.

Unzureichend geschützte Informationen stellen einen häufig unterschätzten Risikofaktor dar, der für eine Institution existenzbedrohend werden kann. Dabei ist ein vernünftiger Informationsschutz ebenso wie eine Grundsicherung der IT schon mit verhältnismäßig geringen Mitteln zu erreichen.

2.1 Ganzheitliches Konzept

Um zu einem bedarfsgerechten Sicherheitsniveau für alle Geschäftsprozesse, Informationen und auch der IT-Systeme einer Institution zu kommen, ist allerdings mehr als das bloße Anschaffen von Virenschutzprogrammen, Firewalls oder Datensicherungssystemen notwendig. Ein ganzheitliches Konzept ist wichtig. Dazu gehört vor allem ein funktionierendes und in die Institution integriertes Sicherheitsmanagement. Informationssicherheitsmanagement (oder kurz: IS-Management) ist jener Teil des allgemeinen Risikomanagements, der die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Geschäftsprozessen, Anwendungen und IT-Systemen gewährleisten soll. Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.

Informationssicherheit ist nicht nur eine Frage der Technik, sondern hängt in erheblichem Maße von den organisatorischen und personellen Rahmenbedingungen ab. Der IT-Grundschutz trägt dem Ganzen Rechnung, indem er über die auf dem Stand der Technik basierenden Bausteine sowohl technische als auch nicht technische Sicherheitsanforderungen für typische Geschäftsbereiche, Anwendungen und Systeme beschreibt. Im Vordergrund stehen dabei praxisnahe und handlungsorientierte Sicherheitsanforderungen mit dem Ziel, die Einstiegshürde in den Sicherheitsprozess so niedrig wie möglich zu halten und hochkomplexe Vorgehensweisen zu vermeiden.

Unter dem Dach des IT-Grundschutzes werden mit der Basis-, der Standard- und der Kern-Absicherung verschiedene Vorgehensweisen angeboten, um den Institutionen je nach Art und Größe passende Instrumente zum Schutz ihrer Informationsverbünde an die Hand zu geben.

2.2 Managementsystem für die Informationssicherheit

Im BSI-Standard 200-2 wird dargestellt, wie ein effizientes Managementsystem für die Informationssicherheit aufgebaut und wie das IT-Grundschutz-Kompendium im Rahmen dieser Aufgabe verwendet werden kann. Die Vorgehensweisen nach IT-Grundschutz in Kombination mit dem IT-Grundschutz-Kompendium bieten eine systematische Methodik zur Erarbeitung von Sicherheitskonzepten und praxiserprobten Sicherheitsmaßnahmen, die in zahlreichen Behörden und Unternehmen erfolgreich eingesetzt werden.

Die Bausteine im IT-Grundschutz-Kompendium werden ständig weiterentwickelt und bedarfsgerecht um aktuelle Fachthemen ergänzt. Alle Informationen rund um den IT-Grundschutz sind kostenfrei über die Website des BSI abrufbar. Um die internationale Zusammenarbeit von Behörden und Unter-

nehmen zu unterstützen, werden alle Dokumente rund um den IT-Grundschutz auch in englischer Sprache und in elektronischer Form zur Verfügung gestellt.

Immer mehr Geschäftsprozesse werden über Informations- und Kommunikationstechnik miteinander verknüpft. Dies geht einher mit einer steigenden Komplexität der technischen Systeme und mit einer hohen Abhängigkeit vom korrekten Funktionieren der Technik. Daher ist ein geplantes und organisiertes Vorgehen aller Beteiligten notwendig, um ein angemessenes und ausreichendes Sicherheitsniveau durchzusetzen und aufrechtzuerhalten. Eine Verankerung dieses Prozesses in allen Geschäftsbereichen kann nur gewährleistet werden, wenn dieser zur Aufgabe der obersten Leitungs- bzw. Managementebene wird. Die oberste Managementebene ist verantwortlich für das zielgerichtete und ordnungsgemäße Funktionieren einer Institution und damit auch für die Gewährleistung der Informationssicherheit nach innen und außen. Daher muss diese den Sicherheitsprozess initiieren, steuern und kontrollieren. Dazu gehören strategische Leitaussagen zur Informationssicherheit, konzeptionelle Vorgaben und auch organisatorische Rahmenbedingungen sowie ausreichende Ressourcen, um Informationssicherheit innerhalb aller Geschäftsprozesse erreichen zu können.

2.3 Verantwortung für die Informationssicherheit

Die Verantwortung für Informationssicherheit verbleibt in jedem Fall bei der obersten Managementebene, die Aufgabe „Informationssicherheit" wird allerdings typischerweise an einen Beauftragten für Informationssicherheit delegiert. In den IT-Grundschutz-Dokumenten wurde bisher die Bezeichnung IT-Sicherheitsbeauftragter verwendet, da dieser Begriff in Unternehmen und Behörden lange Zeit der am weitesten verbreitete war. Die Bezeichnung Informationssicherheitsbeauftragter oder kurz IS-Beauftragter (ISB) ist allerdings treffender und ersetzt daher im IT-Grundschutz die alte Bezeichnung. Andere Varianten sind CISO (Chief Information Security Officer) oder Informationssicherheitsmanager (ISM).

Informationssicherheit umfasst den umfangreicheren Bereich des Schutzes von Informationen, zwar in und mit IT, aber auch ohne IT bzw. über IT hinaus. Somit ist IT-Sicherheit ein Teilbereich der Informationssicherheit und beschäftigt sich gezielt mit dem Schutz der eingesetzten IT. In großen Institutionen kann es weiterhin neben dem ISB auch einen dedizierten Beauftragten für IT-Sicherheit geben. Dieser ist dann typischerweise im IT-Bereich tätig, während der ISB unmittelbar der Leitungsebene zuarbeitet.

Wenn diese Randbedingungen in einer konkreten Situation nicht gegeben sind, sollte zunächst versucht werden, die fehlenden Sicherheitsmaßnahmen auf Arbeitsebene umzusetzen. In jedem Fall sollte aber darauf hingewirkt werden, die Leitungsebene für die Belange der Informationssicherheit zu sensibilisieren, sodass sie zukünftig ihrer Verantwortung Rechnung trägt. Der vielfach zu beobachtende, sich selbst auf Arbeitsebene initiierende Informationssicherheitsprozess führt zwar zu einer punktuellen Verbesserung der Sicherheitssituation, garantiert jedoch kein dauerhaftes Fortentwickeln des Informationssicherheitsniveaus.

2.4 Elemente des IT-Grundschutzes

Ein fundiertes und gut funktionierendes Sicherheitsmanagement ist die unerlässliche Basis für die zuverlässige und kontinuierliche Umsetzung von Sicherheitsmaßnahmen in einer Institution. Daher findet sich neben der ausführlichen Behandlung in diesem Dokument im IT-Grundschutz-Kompendium ein Baustein *Sicherheitsmanagement*. Dies dient sowohl dazu, eine einheitliche Methodik bei der Anwendung des IT-Grundschutzes zu erreichen, als auch dazu, das Sicherheitsmanagement seiner

Bedeutung angemessen in die Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz einbeziehen zu können.

Ergänzend zu den in diesem Standard beschriebenen Vorgehensweisen nach IT-Grundschutz werden im IT-Grundschutz-Kompendium Sicherheitsanforderungen nach dem Stand der Technik formuliert. Der IT-Grundschutz verfolgt dabei einen ganzheitlichen Ansatz. Durch die geeignete Umsetzung von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsanforderungen wird mit der Standard-Absicherung ein Sicherheitsniveau erreicht, das für den normalen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen. Bei der Umsetzung der Basis-Absicherung wird ein Sicherheitsniveau erreicht, das zwar deutlich unter dem der Standard-Absicherung liegt, aber eine gute Grundlage für Einsteiger bietet. Mit der Kern-Absicherung können hochschutzbedürftige Informationen und Geschäftsprozesse vorrangig geschützt werden. Für typische Prozesse, Anwendungen und Komponenten in der Informations-, Kommunikations- und Fertigungstechnik finden sich in den Bausteinen des IT-Grundschutz-Kompendiums geeignete „Bündel" mit Sicherheitsanforderungen zur Basis-, Standard- und Kern-Absicherung.

Diese Bausteine sind entsprechend ihrem jeweiligen Fokus in prozess- und systemorientierte Bausteine aufgeteilt und nach zusammengehörigen Themen in ein Schichtenmodell einsortiert. Die prozessorientierten Bausteine finden sich in den folgenden Schichten:

- ISMS (Managementsysteme für Informationssicherheit)
- ORP (Organisation und Personal)
- CON (Konzepte und Vorgehensweisen)
- OPS (Betrieb)
- DER (Detektion und Reaktion)

Die systemorientierten Bausteine sind in die folgenden Schichten gruppiert:

- INF (Infrastruktur)
- NET (Netze und Kommunikation)
- SYS (IT-Systeme)
- APP (Anwendungen)
- IND (Industrielle IT)

Jeder Baustein enthält eine kurze Beschreibung der Thematik und des Ziels, das mit der Umsetzung des Bausteins erreicht werden soll, sowie eine Abgrenzung zu anderen Bausteinen, die einen ähnlichen thematischen Bezug haben. Weiterhin gibt es einen kurzen Überblick über die spezifischen Gefährdungen des betrachteten Themengebietes. Die konkreten Sicherheitsanforderungen für die Basis-, Standard- und Kern-Absicherung bilden den Hauptteil.

Zusätzlich kann es zu den Bausteinen des IT-Grundschutz-Kompendiums Umsetzungshinweise geben. Diese beschreiben, wie die Anforderungen der Bausteine in der Praxis erfüllt werden können, und enthalten dafür passende Sicherheitsmaßnahmen mit detaillierten Beschreibungen, die auf dem Erfahrungsschatz des BSI und von IT-Grundschutz-Anwendern basieren.

2.5 Thematische Abgrenzung

Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl in IT-Systemen, aber auch auf Papier oder in Köpfen gespeichert sein. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung. Das Aktionsfeld der klassischen IT-Sicherheit wird bei der Cyber-Sicherheit auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Der Begriff „Informationssicherheit" statt IT-Sicherheit oder Cyber-Sicherheit ist daher umfassender. Der IT-Grundschutz verfolgt seit Langem einen ganzheitlichen Ansatz, mit dem auch geschäftsrelevante Informationen und Geschäftsprozesse geschützt werden, die nicht oder nur teilweise mit IT unterstützt werden. Da aber in der Literatur noch überwiegend der Begriff „IT-Sicherheit" zu finden ist, wird er auch in dieser sowie in anderen Publikationen des IT-Grundschutzes weiterhin verwendet, allerdings werden die Texte sukzessive stärker auf die Betrachtung von Informationssicherheit ausgerichtet.

Aufgabe der Informationssicherheit ist der angemessene Schutz der Grundwerte Vertraulichkeit, Integrität (Unverfälschtheit) und Verfügbarkeit von Informationen. Dazu gehört auch die Absicherung der Informationsverarbeitung, also insbesondere der IT. Darüber hinaus müssen auch die Systeme einbezogen werden, die häufig nicht unmittelbar als IT-Systeme wahrgenommen werden, wie beispielsweise ICS- und IoT-Systeme. Außerdem schließt dies auch die Authentizität und Nicht-abstreitbarkeit als Spezialfälle der Integrität ein. Je nach Anwendungsfall kann es hilfreich sein, weitere Grundwerte in die Betrachtungen einzubeziehen. Im Bereich Datenschutz werden, im Rahmen des Standard-Datenschutzmodells (siehe [SDM]), weitere Schutzziele herangezogen, nämlich Datenminimierung, Intervenierbarkeit (als technische Gestaltung von Verfahren zur Ausübung der Betroffenenrechte), Transparenz und Nichtverkettung (als Sicherung der Zweckbindung).

Die Planungs- und Lenkungsaufgabe, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen, wird als Informationssicherheitsmanagement bezeichnet. Aus den gleichen Gründen, die oben für die Begriffe „Informationssicherheit" und „IT-Sicherheit" genannt sind, wird in einigen BSI-Dokumenten statt Informationssicherheitsmanagement (oder der Kurzform IS-Management) noch der Begriff „IT-Sicherheitsmanagement" verwendet.

2.6 Übersicht über den Informationssicherheitsprozess

Die Vorgehensweisen nach IT-Grundschutz bieten Hilfestellung beim Aufbau und bei der Aufrechterhaltung des Prozesses der Informationssicherheit in einer Institution, indem Wege und Methoden für das generelle Vorgehen, aber auch für die Lösung spezieller Probleme aufgezeigt werden.

Für die Gestaltung des Sicherheitsprozesses ist ein systematisches Vorgehen erforderlich, damit ein angemessenes Sicherheitsniveau erreicht werden kann. Im Rahmen des IT-Grundschutzes besteht der Sicherheitsprozess aus den folgenden Phasen:

- Initiierung des Sicherheitsprozesses
  - Übernahme der Verantwortung durch die Leitungsebene
  - Konzeption und Planung des Sicherheitsprozesses
  - Bereitstellung von finanziellen, personellen und zeitlichen Ressourcen
  - Entscheidung für eine Vorgehensweise

- Erstellung der Leitlinie zur Informationssicherheit
- Aufbau einer geeigneten Organisationsstruktur für das Informationssicherheitsmanagement
- Erstellung einer Sicherheitskonzeption
- Umsetzung der Sicherheitskonzeption
- Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit
  - Fortentwicklung des ISMS
  - Erweiterung der gewählten Vorgehensweise

Die ganzheitliche Umsetzung von Informationssicherheit (Standard-Absicherung) in einem einzelnen großen Schritt ist oft ein zu ehrgeiziges Ziel. Viele kleine Schritte und ein langfristiger, kontinuierlicher Verbesserungsprozess ohne hohe Investitionskosten zu Beginn sind oft erfolgversprechender. So kann es besser sein, zunächst nur die dringend erforderlichen Sicherheitsvorkehrungen umzusetzen (Basis-Absicherung) oder in Bereichen mit höchsten Sicherheitsanforderungen schnell das erforderliche hohe Sicherheitsniveau zu erreichen (Kern-Absicherung). Von diesen Keimzellen ausgehend, sollte dann kontinuierlich die Sicherheit in der Gesamtorganisation verbessert werden.

Informationssicherheitsverantwortliche können die Vorgehensweisen nach IT-Grundschutz und das IT-Grundschutz-Kompendium aus verschiedenen Gründen und Zielsetzungen anwenden. Dementsprechend ist auch die Reihenfolge und Intensität der einzelnen Phasen abhängig vom bereits vorhandenen Sicherheitsumfeld und dem jeweiligen Blickwinkel der Anwender. Beispielsweise werden bei einer regulären Überarbeitung des Sicherheitskonzepts häufig andere Schwerpunkte als bei der Integration neuer Geschäftsprozesse gesetzt.

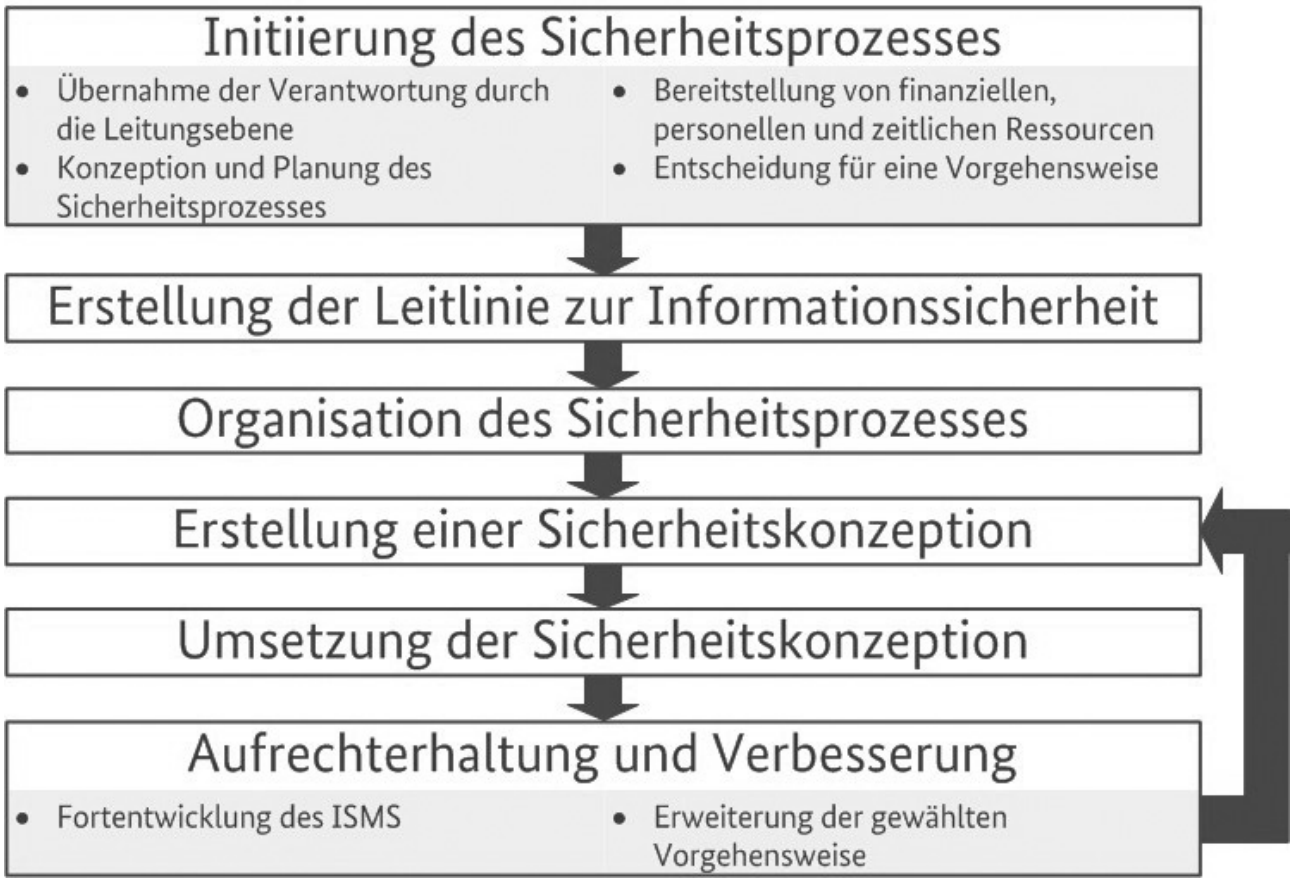


Abbildung 1: Phasen des Sicherheitsprozesses

Einige der Phasen können auch parallel durchgeführt werden, z. B. kann die Konzeption und Planung des Sicherheitsprozesses gleichzeitig zum Aufbau der Informationssicherheitsorganisation erfolgen. In diesem Fall müssen die vorgezogenen Phasen mit den neuen Ergebnissen zeitnah aktualisiert werden.

Im Folgenden wird eine kurze Darstellung über die Phasen des Sicherheitsprozesses gegeben.

Initiierung des Sicherheitsprozesses

Die Leitungsebene muss den Sicherheitsprozess initiieren, steuern und kontrollieren. Hierfür sind einerseits strategische Leitaussagen zur Informationssicherheit und andererseits organisatorische Rahmenbedingungen erforderlich. Wie ein funktionierender Sicherheitsprozess aufgebaut ist und welche Organisationsstrukturen dafür sinnvoll sind, ist in Kapitel 3 beschrieben.

Erstellung der Leitlinie zur Informationssicherheit

Eine wesentliche Grundlage für die Ausgestaltung des Sicherheitsprozesses ist die Leitlinie zur Informationssicherheit. Sie beschreibt, welche Sicherheitsziele und welches Sicherheitsniveau die Institution anstrebt, was die Motivation hierfür ist und mit welchen Maßnahmen und mit welchen Strukturen dies erreicht werden soll. Alle Mitarbeiter sollten daher die Inhalte der Sicherheitsleitlinie kennen und nachvollziehen können. Was für die Leitlinie und andere Dokumente im Sicherheitsprozess zu beachten ist, wird in Kapitel 3.4 beschrieben.

Aufbau einer geeigneten Organisationsstruktur

Für das Informationssicherheitsmanagement muss eine für Größe und Art der Institution geeignete Organisationsstruktur aufgebaut werden, siehe Kapitel 4.

Erstellung einer Sicherheitskonzeption

Nachdem ein Informationssicherheitsprozess initiiert wurde und die Sicherheitsleitlinie und Informationssicherheitsorganisation definiert wurden, wird die Sicherheitskonzeption für die Institution erstellt. Als Grundlage hierfür finden sich in den Bausteinen des IT-Grundschutz-Kompendiums für typische Komponenten von Geschäftsprozessen, Anwendungen, IT-Systeme und weitere Objekte entsprechende Sicherheitsanforderungen nach dem Stand der Technik. Diese sind thematisch in Bausteine strukturiert, so dass sie modular aufeinander aufsetzen.

Abhängig davon, ob eine Basis-, Standard- oder Kern-Absicherung angestrebt ist, sehen die einzelnen Aktivitäten zur Erstellung einer Sicherheitskonzeption etwas anders aus, grundsätzlich basieren sie aber alle auf den Vorarbeiten, die mit der Erstellung des IT-Grundschutz-Kompendiums geleistet worden sind.

Bei Anwendung des IT-Grundschutzes wird ein Soll-Ist-Vergleich zwischen den Sicherheitsanforderungen aus den relevanten Bausteinen des IT-Grundschutz-Kompendiums und den in der Institution bereits realisierten Maßnahmen durchgeführt. Dabei festgestellte fehlende oder nur unzureichend erfüllte Anforderungen zeigen die Sicherheitsdefizite auf, die es durch die Umsetzung von aus den Anforderungen abgeleiteten Maßnahmen zu beheben gilt.

Nur bei einem signifikant höheren Schutzbedarf muss zusätzlich eine Risikoanalyse unter Beachtung von Kosten- und Wirksamkeitsaspekten durchgeführt werden. In der Regel reicht es hierbei aus, die Sicherheitsanforderungen des IT-Grundschutz-Kompendiums durch entsprechende individuelle, qualitativ höherwertige Maßnahmen zu ergänzen. Hierzu ist im BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz* (siehe [BSI3]) eine im Vergleich zu traditionellen Risikoanalyse-Methoden einfachere Vorgehensweise beschrieben.

Umsetzung von Sicherheitskonzepten

Ein ausreichendes Sicherheitsniveau lässt sich nur erreichen, wenn bestehende Defizite ermittelt, der Status quo in einem Sicherheitskonzept festgehalten, erforderliche Maßnahmen identifiziert und diese Maßnahmen insbesondere auch konsequent umgesetzt werden. In Kapitel 9 wird beschrieben, was bei der Umsetzungsplanung von Sicherheitsmaßnahmen beachtet werden muss.

Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit

Ziel des Sicherheitsmanagements ist es, das angestrebte Sicherheitsniveau zu erreichen und dieses auch dauerhaft aufrechtzuerhalten und zu verbessern. Daher müssen der Sicherheitsprozess und die Organisationsstrukturen für Informationssicherheit regelmäßig darauf überprüft werden, ob sie angemessen, wirksam und effizient sind. Ebenso ist zu analysieren, ob die Maßnahmen des Sicherheitskonzepts noch zum Informationsverbund passen, ob sie praxisnah sind und ob sie korrekt umgesetzt wurden. In Kapitel 10 wird überblicksartig dargestellt, welche Aktionen für die Aufrechterhaltung und Verbesserung der Informationssicherheit ergriffen werden sollten. Dazu gehört auch, zu überlegen, ob die gewählte Vorgehensweise ergänzt oder erweitert werden soll, beispielsweise von Basis- auf Standard- oder von Kern-Absicherung eines eingegrenzten Bereiches auf einen größeren Informationsverbund.

2.7 Anwendung des IT-Grundschutz-Kompendiums

Nachdem die Leitungsebene mit der Erstellung der Leitlinie zur Informationssicherheit und dem Aufbau der Informationssicherheitsorganisation den Sicherheitsprozess auf der strategischen Ebene definiert hat, wird dieser mithilfe der Sicherheitskonzeption auf der operativen Ebene fortgeführt. Somit ist die Erstellung einer Sicherheitskonzeption eine der zentralen Aufgaben des Informationssicherheitsmanagements. Hier werden die erforderlichen Sicherheitsmaßnahmen identifiziert und dokumentiert.

Um die sehr heterogenen Ausgestaltungen von Institutionen der verschiedenen Branchen und Größenordnungen sowie der von ihnen eingesetzten IT- oder ICS-Systeme einschließlich der Einsatzumgebung besser strukturieren und aufbereiten zu können, verfolgt der IT-Grundschutz das Baukastenprinzip. Die einzelnen Bausteine, die im IT-Grundschutz-Kompendium beschrieben werden, spiegeln typische Bereiche und Aspekte der Informationssicherheit in einer Institution wider, von übergeordneten Themen, wie dem IS-Management, der Notfallvorsorge oder der Datensicherungskonzeption bis hin zu speziellen Komponenten einer IT- oder ICS-Umgebung. Das IT-Grundschutz-Kompendium beschreibt die spezifische Gefährdungslage und die Sicherheitsanforderungen für verschiedene Komponenten, Vorgehensweisen und Systeme, die jeweils in einem Baustein zusammengefasst werden. Das BSI überarbeitet und aktualisiert zusammen mit vielen engagierten Anwendern regelmäßig die bestehenden Bausteine, um die Empfehlungen auf dem Stand der Technik zu halten. Darüber hinaus wird das bestehende Werk regelmäßig um weitere Bausteine ergänzt. Anwender können Bausteine vorschlagen oder erstellen. Unter Federführung des IT-Grundschutz-Teams des BSI werden diese dann zunächst als Community Draft aufbereitet, in den dann weitere Anregungen einfließen können, bevor sie ins IT-Grundschutz-Kompendium aufgenommen werden.

Die Bausteine spielen eine zentrale Rolle in der Methodik des IT-Grundschutzes. Sie sind einheitlich aufgebaut, um ihre Anwendung zu vereinfachen. Jeder Baustein beginnt mit einer kurzen Beschreibung der betrachteten Komponente, der Vorgehensweise bzw. des Systems inklusive Zielsetzung sowie einer Abgrenzung zu anderen Bausteinen mit thematischem Bezug. Im Anschluss daran wird die spezifische Gefährdungslage dargestellt.

Danach folgen die Sicherheitsanforderungen, gegliedert nach Basis- und Standard-Anforderungen sowie Anforderungen bei erhöhtem Schutzbedarf. Die im IT-Grundschutz-Kompendium aufgeführten Basis- und Standard-Anforderungen stellen zusammengenommen den Stand der Technik dar. Diese müssen für die Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz erfüllt werden.

In den Anforderungen werden die in Versalien geschriebenen Modalverben „SOLLTE" und „MUSS" in ihren jeweiligen Formen sowie den zugehörigen Verneinungen genutzt, um deutlich zu machen, wie die jeweiligen Anforderungen zu interpretieren sind. Die hier genutzte Definition basiert auf [RFC2119] sowie DIN 820-2:2012, Anhang H [820-2].

MUSS/DARF NUR:	Dieser Ausdruck bedeutet, dass es sich um eine Anforderung handelt, die unbedingt erfüllt werden muss (uneingeschränkte Anforderung).
DARF NICHT/DARF KEIN:	Dieser Ausdruck bedeutet, dass etwas in keinem Fall getan werden darf (uneingeschränktes Verbot).
SOLLTE:	Dieser Ausdruck bedeutet, dass eine Anforderung normalerweise erfüllt werden muss, es aber Gründe geben kann, dies doch nicht zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden.
SOLLTE NICHT/SOLLTE KEIN:	Dieser Ausdruck bedeutet, dass etwas normalerweise nicht getan werden sollte, es aber Gründe gibt, dies doch zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden.

Sicherheitskonzepte, die mithilfe des IT-Grundschutzes erstellt werden, sind kompakt, da innerhalb des Konzepts jeweils nur auf die entsprechenden Sicherheitsanforderungen im IT-Grundschutz-Kompendium referenziert werden muss. Dies fördert die Verständlichkeit und die Übersichtlichkeit. Um die Sicherheitsanforderungen leichter umsetzen zu können, gibt es zu vielen Bausteinen des IT-Grundschutz-Kompendiums zusätzlich Umsetzungshinweise. Diese beschreiben, wie die Anforderungen der Bausteine in der Praxis erfüllt werden können, und enthalten dafür passende Sicherheitsmaßnahmen mit einer detaillierten Beschreibung. Bei der verwendeten Fachterminologie wird darauf geachtet, dass die Beschreibungen für diejenigen verständlich sind, die die Maßnahmen realisieren müssen. Zu beachten ist, dass es sich bei den Umsetzungshinweisen um Hilfestellungen zur Erfüllung der Anforderungen des jeweiligen Bausteins und nicht um verbindliche Vorgaben handelt.

Hinweis:

Die umfangreichen Informationen rund um IT-Grundschutz ersetzen nicht den gesunden Menschenverstand. Informationssicherheit zu verstehen, umzusetzen und zu leben, sollte Priorität haben. Das IT-Grundschutz-Kompendium bietet zu vielen Aspekten eine Menge an Informationen und Empfehlungen. Bei deren Bearbeitung sollte immer im Auge behalten werden, dass aus diesen die für die jeweilige Institution und ihre Rahmenbedingungen geeigneten Sicherheitsanforderungen ausgewählt und angepasst werden. Weiterführende Informationen zur Anpassung der Baustein-Anforderungen finden sich in Kapitel 8.3.6. Weder die Anforderungen der Bausteine des IT-Grundschutz-Kompendiums noch die Maßnahmen der Umsetzungshinweise sollten als pure Checklisten zur Statusfeststellung genutzt werden, sondern mit Augenmaß an die individuellen Bedingungen angepasst werden.

Um die Realisierung der Maßnahmen zu vereinfachen, werden die IT-Grundschutz-Texte konsequent auch in elektronischer Form zur Verfügung gestellt. Darüber hinaus wird die Realisierung der Sicherheitsanforderungen und Maßnahmen auch durch Hilfsmittel und Musterlösungen unterstützt, die teilweise durch das BSI und teilweise auch von Anwendern des IT-Grundschutzes bereitgestellt werden.

3 Initiierung des Sicherheitsprozesses

Um ein angemessenes und ausreichendes Niveau der Informationssicherheit in der Institution zu erzielen bzw. dieses aufrechtzuerhalten, ist einerseits ein *geplantes Vorgehen* und andererseits eine *adäquate Organisationsstruktur* erforderlich. Darüber hinaus ist es notwendig, *Sicherheitsziele* und eine *Strategie zur Erreichung* dieser Ziele zu definieren sowie letztendlich einen kontinuierlichen Sicherheitsprozess zur Aufrechterhaltung des einmal erreichten Sicherheitsniveaus einzurichten. Aufgrund der großen Bedeutung, der weitreichenden Konsequenzen der zu treffenden Entscheidungen und der hohen Verantwortung muss dieses Thema von der obersten Leitungsebene initiiert werden.

3.1 Übernahme von Verantwortung durch die Leitungsebene

Die oberste Leitungsebene jeder Behörde und jedes Unternehmens ist dafür verantwortlich, dass alle Geschäftsbereiche zielgerichtet und ordnungsgemäß funktionieren und dass Risiken frühzeitig erkannt und minimiert werden. Mit der steigenden Abhängigkeit der Geschäftsprozesse von der Informationsverarbeitung steigen also auch die Anforderungen, dass die Informationssicherheit nach innen und außen gewährleistet ist.

Die oberste Leitungsebene muss den Sicherheitsprozess initiieren, steuern und kontrollieren. Die Leitungsebene ist diejenige Instanz, die die Entscheidung über den Umgang mit Risiken treffen und die entsprechenden Ressourcen zur Verfügung stellen muss. Die Verantwortung für Informationssicherheit verbleibt dort. Die operative Aufgabe „Informationssicherheit" wird allerdings typischerweise an einen Informationssicherheitsbeauftragten (ISB) delegiert.

In der Einstiegsphase in den Sicherheitsprozess ist üblicherweise noch keine Sicherheitsorganisation aufgebaut und häufig auch noch nicht der spätere ISB benannt. Für die Initiierung des Sicherheitsprozesses muss aber zumindest ein Verantwortlicher für Informationssicherheit benannt werden, der die ersten Schritte zur Konzeption und Planung des Einstiegs in die Informationssicherheit durchführt.

Eine rechtzeitige Unterrichtung über mögliche Risiken beim Umgang mit Informationen, Geschäftsprozessen und IT kann von der Geschäftsführung oder Behördenleitung nach einem Sicherheitsvorfall als Bringschuld der IT- oder Sicherheitsexperten gesehen werden. Aus diesem Grund ist es für die Inhaber dieser Rollen empfehlenswert, die oberste Leitungsebene über mögliche Risiken und Konsequenzen aufgrund fehlender Informationssicherheit nachweislich aufzuklären. Auf jeden Fall ist aber die Leitungsebene ebenfalls dafür verantwortlich, sicherzustellen, dass alle entscheidungsrelevanten Informationen sie rechtzeitig und im nötigen Umfang erreichen. Zu den sicherheitsrelevanten Themen gehören beispielsweise:

- die Sicherheitsrisiken für die Institution und deren Informationen sowie die damit verbundenen Auswirkungen und Kosten,
- die Auswirkungen von Sicherheitsvorfällen auf die kritischen Geschäftsprozesse,
- die Sicherheitsanforderungen, die sich aus gesetzlichen und vertraglichen Vorgaben ergeben,
- die für die Branche typischen Standardvorgehensweisen zur Informationssicherheit,
- der aktuelle Stand der Informationssicherheit im Sinne eines Reifegrades und daraus abgeleitete Handlungsempfehlungen.

Die Leitungsebene trägt zwar die Verantwortung für die Erreichung der Sicherheitsziele, der Sicherheitsprozess muss aber von allen Beschäftigten in einer Organisation mitgetragen und mitgestaltet werden.

Die Leitungsebene muss sich vor allem dafür einsetzen, dass Informationssicherheit in alle relevanten Geschäftsprozesse bzw. Fachverfahren und Projekte integriert wird. Der ISB braucht hierbei erfahrungsgemäß die volle Unterstützung der Behörden- oder Unternehmensleitung, um unter dem überall herrschenden Leistungsdruck von den jeweiligen Fachverantwortlichen in jede wesentliche Aktivität eingebunden zu werden.

Die Leitungsebene muss die Ziele sowohl für das Informationssicherheitsmanagement als auch für alle anderen Bereiche so setzen, dass das angestrebte Sicherheitsniveau in allen Bereichen mit den bereitgestellten Ressourcen (Personal, Zeit, Finanzmittel) erreichbar ist.

Aktionspunkte zu 3.1 Übernahme von Verantwortung durch die Leitungsebene
• Die Leitungsebene informiert sich über mögliche Risiken und Konsequenzen aufgrund fehlender Informationssicherheit.
• Die Leitungsebene übernimmt die Gesamtverantwortung für Informationssicherheit.
• Die Leitungsebene initiiert den Informationssicherheitsprozess innerhalb der Institution und benennt einen Verantwortlichen für Informationssicherheit.

3.2 Konzeption und Planung des Sicherheitsprozesses

Um ein angemessenes Sicherheitsniveau zu erreichen und aufrechterhalten zu können, ist es notwendig, einen kontinuierlichen Informationssicherheitsprozess zu etablieren und eine angemessene Strategie für Informationssicherheit (IS-Strategie) festzulegen. Diese dient der Orientierung für die Planung des weiteren Vorgehens, um die gesetzten Sicherheitsziele zu erreichen. Sie wird von der Leitungsebene vorgegeben und basiert auf den Geschäftszielen des Unternehmens bzw. dem Auftrag der Behörde. Die Leitungsebene gibt grundlegende Sicherheitsziele vor und legt fest, welches Informationssicherheitsniveau im Hinblick auf die Geschäftsziele und Fachaufgaben angemessen ist. Die dafür erforderlichen Mittel müssen ebenfalls von der Leitungsebene zur Verfügung gestellt werden.

3.2.1 Ermittlung von Rahmenbedingungen

Um eine angemessene IS-Strategie festzulegen, müssen alle relevanten Rahmenbedingungen identifiziert werden. Daher sollte jede Institution ihre wichtigsten Geschäftsprozesse und Fachaufgaben sowie deren Bedarf an Informationssicherheit ermitteln. Dazu gehört auch die Analyse der Stakeholder (also der relevanten internen und externen Parteien), von Geschäftszielen, Aufgaben und deren Anforderungen an Sicherheit. Die Zusammenhänge zwischen Geschäftsabläufen und den dort verarbeiteten Informationen sowie der eingesetzten Informationstechnik bilden die Basis für die Entscheidung, welches Sicherheitsniveau zum Schutz der Informationen und für die Informationstechnik jeweils angemessen ist.

Die Ermittlung von Rahmenbedingungen ist eine wesentliche Grundlage für die weiteren Betrachtungen der Informationssicherheit, da hierdurch identifiziert werden kann, wo wichtige Hintergrundinformationen fehlen, um die Bedeutung der Informationssicherheit für die Institution korrekt einschätzen zu können. Außerdem wird dadurch ein erstes *Self Assessment* möglich, da bei der Zusammenstellung der Hintergrundinformationen bereits deutlich wird, wo Konfliktpotenzial liegt und wo Aktivitäten erforderlich sind.

Allgemeine Einflussfaktoren

Informationssicherheit dient der Institution zur Erreichung der Geschäftsziele. Daher müssen die sich hieraus abgeleiteten Einflussfaktoren betrachtet werden:

- Geschäftsziele: Welche Faktoren sind wesentlich für den Erfolg des Unternehmens oder der Behörde? Welche Produkte, Angebote und Aufträge bilden die Grundlage der Geschäftstätigkeit? Was sind die generellen Ziele der Institution? Welche Rolle spielt Informationssicherheit hierbei?
- Organisationsstruktur: Wie ist die Institution organisiert und strukturiert? Welche Managementsysteme sind vorhanden (beispielsweise Risikomanagement oder Qualitätsmanagement)?
- Zusammenarbeit mit Externen: Welche sind die wichtigsten internen und externen Kunden, Partner und einflussnehmenden Gremien? Was sind deren grundlegenden Anforderungen und Erwartungen an die Informationssicherheit der Institution? Was sind die wichtigsten Dienstleister und Zulieferer? Welche Rolle spielen diese für die Informationssicherheit der Institution?
- Strategischer Kontext: Was sind die wesentlichen Herausforderungen für die Institution? Wie ist die Wettbewerbsposition? Wie beeinflusst dies den Risikoappetit der Institution und den Umgang mit Informationssicherheit?

Interne Rahmenbedingungen

Viele interne Rahmenbedingungen können Auswirkungen auf die Informationssicherheit haben und müssen folglich ermittelt werden. Über die Analyse der Geschäftsprozesse und Fachaufgaben lassen sich Aussagen über die Auswirkungen von Sicherheitsvorfällen auf die Geschäftstätigkeit und die Aufgabenerfüllung ableiten. Es geht zu diesem frühen Zeitpunkt jedoch nicht darum, detailliert die Informationstechnik zu beschreiben. Es sollte aber eine grobe Übersicht vorliegen, welche Informationen für einen Geschäftsprozess mit welchen Anwendungen und IT-Systemen verarbeitet werden.

Oft gibt es in Institutionen schon Übersichten von Geschäftsprozessen, Objekten oder Datensammlungen, die für betriebliche Aspekte oder die Verwaltung benötigt werden. Falls vorhanden, können vorhandene Prozesslandkarten, Geschäftsverteilungspläne, Datenbanken, Übersichten, Netzpläne und Inventarisierungstools genutzt werden, um die wesentlichen Geschäftsprozesse zu identifizieren. Werden diese Übersichten berücksichtigt, sollte darauf geachtet werden, dass hierdurch der Detaillierungsgrad der Erfassung nicht zu tief wird, damit der Umfang für einen ersten Überblick und als Grundlage für spätere Entscheidungen nicht zu umfangreich ist.

Folgende Aspekte sollten bedacht werden:

- Welche Geschäftsprozesse gibt es in der Institution und wie hängen diese mit den Geschäftszielen zusammen?
- Welche Geschäftsprozesse hängen von einer funktionierenden, also einer ordnungsgemäß und anforderungsgerecht arbeitenden Informationstechnik ab?
- Welche Informationen werden im Rahmen dieser Geschäftsprozesse verarbeitet?
- Welche Informationen sind besonders wichtig und damit in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit schützenswert und warum? Beispiele sind personenbezogene Daten, Kundendaten, strategische Informationen oder Geheimnisse, wie z. B. Entwicklungsdaten, Patente, Verfahrensbeschreibungen.

Zu jedem Geschäftsprozess und jeder Fachaufgabe muss ein verantwortlicher Ansprechpartner benannt werden, der als sogenannter Informationseigentümer für alle Fragen der Informationsverarbeitung im Rahmen dieses Geschäftsprozesses verantwortlich ist.

Externe Rahmenbedingungen

Daneben müssen ebenso alle externen Rahmenbedingungen ermittelt werden, die Auswirkungen auf die Informationssicherheit haben, wie beispielsweise

- gesetzliche Rahmenbedingungen (nationale und internationale Gesetze und Bestimmungen),
- Anforderungen von Kunden, Lieferanten und Geschäftspartnern, aktuelle Marktlage, Wettbewerbssituation und weitere relevante marktspezifische Abhängigkeiten,
- branchenspezifische Sicherheitsstandards.

Brainstorming

Um alle relevanten Rahmenbedingungen für jeden wesentlichen Geschäftsprozess möglichst schnell und umfassend zu ermitteln, empfiehlt es sich, dass ein kurzes Sicherheitsgespräch (Brainstorming) zu jedem Geschäftsprozess durchgeführt wird. Diese Sicherheitsgespräche sollten unter der Leitung des ISB mit den jeweiligen Informationseigentümern bzw. Fachverantwortlichen sowie dem entsprechenden IT-Verantwortlichen durchgeführt werden. Ob insgesamt eine oder mehrere Besprechungen erforderlich sind, hängt von der Größe und Komplexität der Institution ab.

Es sollten vorrangig geschäftskritische Informationen und Kernprozesse ermittelt und die zugehörigen Anwendungen, IT-Systeme, Netze und Räume erfasst werden. Dabei sollten ausgehend von den Kernprozessen der Institution die wesentlichen unterstützenden Prozesse und die hauptsächlich betroffenen Objekte ermittelt werden. Es hat sich gezeigt, dass es schwerfällt, abstrakte Prozesse losgelöst von konkreten technischen Komponenten zu betrachten. Daher kann es gegebenenfalls sinnvoll sein, nicht nur aus Prozesssicht kommend die Assets zu ermitteln, sondern auch aus der Perspektive der bekannten Assets zu ermitteln, welche Prozesse diese verwenden. Dieses optionale Vorgehen ist besonders dann sinnvoll, wenn keine vollständige Prozesslandkarte vorhanden ist und die Geschäftsführung Schwierigkeiten hat, diese zu definieren.

Die Teilnahme der Leitungsebene am Brainstorming ist nicht zwingend notwendig. Viel wichtiger ist es, dass jeder Teilnehmer für den Bereich, den er vertritt, auskunftsfähig ist und die wesentlichen Geschäftsprozesse seines Bereiches sowie die eingesetzten Assets benennen kann. Die Erstaufnahme sollte typischerweise nicht mehr als einen halben Tag beanspruchen. Die Ergebnisse sollten nach einem vorher festgelegten Schema dokumentiert und an die Leitungsebene berichtet werden.

3.2.2 Formulierung von allgemeinen Informationssicherheitszielen

Zu Beginn jedes Sicherheitsprozesses sollten die Informationssicherheitsziele sorgfältig bestimmt werden. Anderenfalls besteht die Gefahr, dass Sicherheitsstrategien und -konzepte erarbeitet werden, die die eigentlichen Anforderungen der Institution verfehlen.

Aus den grundsätzlichen Zielen der Institution und den allgemeinen Rahmenbedingungen sollten daher zunächst allgemeine Sicherheitsziele abgeleitet werden. Aus diesen werden später bei der Erstellung des Sicherheitskonzepts und bei der Ausgestaltung der Informationssicherheitsorganisation konkrete Sicherheitsanforderungen bezüglich des Umgangs mit Informationen und mit dem IT-Betrieb abgeleitet. Mögliche allgemeine Sicherheitsziele einer Institution könnten z. B. sein:

- Hohe Verlässlichkeit des Handelns, auch in Bezug auf den Umgang mit Informationen (Verfügbarkeit, Integrität, Vertraulichkeit),
- Gewährleistung des guten Rufs der Institution in der Öffentlichkeit,
- Erhaltung der in Technik, Informationen, Arbeitsprozesse und Wissen investierten Werte,

- Sicherung der hohen, möglicherweise unwiederbringlichen Werte der verarbeiteten Informationen,
- Gewährleistung der aus gesetzlichen Vorgaben resultierenden Anforderungen,
- Schutz von natürlichen Personen hinsichtlich ihrer körperlichen und geistigen Unversehrtheit.

Um die Sicherheitsziele definieren zu können, sollte zunächst abgeschätzt werden, welche Geschäftsprozesse bzw. Fachverfahren und Informationen für die Aufgabenerfüllung notwendig sind und welcher Wert diesen beigemessen wird. Dabei ist es wichtig, klarzustellen, wie stark die Aufgabenerfüllung innerhalb der Institution von der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und von der eingesetzten IT und deren sicherem Funktionieren abhängt. Für die Definition der Sicherheitsziele ist es sinnvoll, die zu schützenden Grundwerte Verfügbarkeit, Integrität und Vertraulichkeit ausdrücklich zu benennen und eventuell zu priorisieren. Diese Aussagen werden im Lauf des Sicherheitsprozesses bei der Wahl der Sicherheitsmaßnahmen und Strategien eine entscheidende Rolle spielen.

An dieser Stelle muss keine detaillierte Analyse des Informationsverbunds und der möglichen Kosten von Sicherheitsmaßnahmen erfolgen, sondern lediglich die Aussage, was für die Institution von besonderer Bedeutung ist und warum.

3.2.3 Bestimmung des angemessenen Sicherheitsniveaus der Geschäftsprozesse

Zur besseren Verständlichkeit der Informationssicherheitsziele kann das angestrebte Sicherheitsniveau für einzelne, besonders hervorgehobene Geschäftsprozesse bzw. Bereiche der Institution in Bezug auf die Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) dargestellt werden. Dies ist für die spätere Formulierung der detaillierten Sicherheitskonzeption hilfreich.

Nachstehend sind einige beispielhafte Kriterien zur Bestimmung eines angemessenen Sicherheitsniveaus aufgeführt. Anhand derjenigen Aussagen, die am ehesten zutreffen, lässt sich das Sicherheitsniveau (normal, hoch oder sehr hoch) einzelner Geschäftsprozesse bzw. Bereiche bestimmen. In dieser Phase des Sicherheitsprozesses geht es um die Formulierung der ersten richtungweisenden Aussagen, die in den späteren Phasen als Grundlage dienen werden, und nicht um eine detaillierte Schutzbedarfsfeststellung.

Sehr hoch:

- Der Schutz vertraulicher Informationen muss unbedingt gewährleistet sein und in sicherheitskritischen Bereichen strengen Vertraulichkeitsanforderungen genügen. Die Offenlegung besonders kritischer oder hoch vertraulicher Information kann zu schweren Folgen für den Weiterbestand der Institution führen.
- Die Informationen müssen im höchsten Maße korrekt sein.
- Die zentralen Aufgaben der Institution sind ohne IT-Einsatz nicht durchführbar. Knappe Reaktionszeiten für kritische Entscheidungen fordern eine ständige Präsenz der aktuellen Informationen, Ausfallzeiten sind nicht akzeptabel.
- Der Schutz personenbezogener Daten muss unbedingt gewährleistet sein. Anderenfalls kann es zu einer Gefahr für Leib und Leben oder für die persönliche Freiheit des Betroffenen kommen.

Insgesamt gilt: Der Ausfall der IT oder wesentlicher Geschäftsprozesse oder die Offenlegung bzw. Manipulation von kritischen Informationen führt zum Zusammenbruch der Institution oder hat schwerwiegende Folgen für breite gesellschaftliche oder wirtschaftliche Bereiche.

Hoch:

- Der Schutz vertraulicher Informationen muss hohen Anforderungen genügen und in sicherheitskritischen Bereichen stärker ausgeprägt sein.
- Die verarbeiteten Informationen müssen korrekt sein, auftretende Fehler müssen erkennbar und vermeidbar sein.
- In zentralen Bereichen der Institution laufen zeitkritische Vorgänge oder es werden dort Massenaufgaben wahrgenommen, die ohne IT-Einsatz nicht zu erledigen sind. Es können nur kurze Ausfallzeiten toleriert werden.
- Der Schutz personenbezogener Daten muss hohen Anforderungen genügen. Anderenfalls besteht die Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt wird.

Insgesamt gilt: Im Schadensfall tritt Handlungsunfähigkeit zentraler Bereiche der Institution ein. Schäden haben erhebliche Beeinträchtigungen der Institution selbst oder betroffener Dritter zur Folge.

Normal:

- Der Schutz von Informationen, die nur für den internen Gebrauch bestimmt sind, muss gewährleistet sein.
- Informationen sollten korrekt sein. Kleinere Fehler können toleriert werden. Fehler, die die Aufgabenerfüllung erheblich beeinträchtigen, müssen jedoch erkenn- oder vermeidbar sein.
- Längere Ausfallzeiten, die zu Terminüberschreitungen führen, sind nicht zu tolerieren.
- Der Schutz personenbezogener Daten muss gewährleistet sein. Anderenfalls besteht die Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt wird.

Insgesamt gilt: Schäden haben Beeinträchtigungen der Institution zur Folge.

Hinweis:

Jede Institution sollte die Formulierungen auf ihre individuellen Gegebenheiten anpassen. Es kann auch sinnvoll sein, weitere Kategorien zu definieren, beispielsweise, um Abgrenzungen nach oben oder unten deutlicher zu machen. Die Sicherheitsziele spiegeln auch wider, welche Sicherheitskultur in einer Institution vorhanden ist, also wie mit Sicherheitsrisiken und -maßnahmen umgegangen wird.

Für die Formulierung der Informationssicherheitsziele ist die Mitwirkung der Leitungsebene unbedingt notwendig. Zur Bestimmung des angestrebten Sicherheitsniveaus müssen die Ziele der Institution in Bezug auf ihre Anforderungen zur Sicherheit betrachtet werden, jedoch unter Berücksichtigung der Tatsache, dass in der Regel begrenzte Ressourcen für die Implementierung von Sicherheitsmaßnahmen zur Verfügung stehen. Aus diesem Grund ist es von besonderer Bedeutung, den tatsächlichen Bedarf an Verfügbarkeit, Integrität und Vertraulichkeit zu identifizieren, da ein hohes Sicherheitsniveau in der Regel auch mit einem hohen Implementierungsaufwand verbunden ist. Es ist zudem empfehlenswert, die formulierten Anforderungen zu priorisieren, wenn dies zu diesem Zeitpunkt bereits möglich ist.

Hinweis zur Beschreibungstiefe

In dieser frühen Phase des Informationssicherheitsprozesses geht es nicht um eine detaillierte Betrachtung aller Anwendungen und IT-Systeme oder eine aufwendige Risikoanalyse. Wichtig ist, eine Übersicht zu haben, welche Sicherheitsanforderungen aufgrund der Geschäftsprozesse oder Fachverfahren an die Informationstechnik gestellt werden. Zum Beispiel sollten sich nach der Bestimmung des angestrebten Sicherheitsniveaus die nachfolgenden Fragen beantworten lassen:

- Welche Informationen sind in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit besonders kritisch für die Institution?
- Welche kritischen Aufgaben der Institution können ohne Unterstützung durch IT nicht, nur unzureichend oder mit erheblichem Mehraufwand ausgeführt werden?
- Welche Auswirkungen können absichtliche oder ungewollte Sicherheitszwischenfälle haben?
- Werden mit der eingesetzten IT Informationen verarbeitet, deren Vertraulichkeit besonders zu schützen ist?
- Welche wesentlichen Entscheidungen der Institution beruhen auf Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und IT-Systemen?
- Welche organisatorischen oder gesetzlichen Anforderungen (z. B. Datenschutz) haben besondere Maßnahmen zur Folge?

Die Beschreibungen des angestrebten Sicherheitsniveaus sollten auf das jeweilige Umfeld angepasst sein. Kurze Begründungen sind für die Motivation darauf aufbauender Maßnahmen hilfreich. Diese könnte beispielsweise für ein Krankenhaus heißen: „In der Röntgenabteilung ist ein sehr hohes Informationssicherheitsniveau notwendig, weil von der korrekten Funktion der IT-Systeme Menschenleben abhängen."

3.2.4 Ersterfassung der Prozesse, Anwendungen und IT-Systeme

Die Ergebnisse der vorherigen Schritte, also der Ermittlung von Rahmenbedingungen, der Formulierung von Informationssicherheitszielen und der Bestimmung des angemessenen Sicherheitsniveaus der Geschäftsprozesse, sollten als Nächstes in einer Übersicht der vorhandenen Assets der Institution konsolidiert werden.

Diese Übersicht dient als Entscheidungshilfe für die Auswahl einer geeigneten Vorgehensweise und ist die Basis für die späteren Schritte, wie die Auswahl der relevanten IT-Grundschutz-Bausteine bei der Basis-Absicherung oder die Strukturanalyse bei der Standard-Absicherung. Hierbei sollte die Erstaufnahme der Prozesse, Anwendungen und IT-Systeme insoweit vollständig sein, dass sie als Entscheidungshilfe für die Auswahl der geeigneten Vorgehensweise zur Absicherung der Institution verwendet werden kann, sie ist aber bei Weitem nicht so umfangreich wie das Ergebnis einer Strukturanalyse.

Die Ersterfassung liefert als Ergebnis eine vergleichsweise schnell und ressourcenschonend erstellbare Übersicht. Die bei der Standard-Absicherung durchzuführende Strukturanalyse kann darauf aufsetzen und liefert ein vollständigeres Bild des abzusichernden Informationsverbunds.

Im Rahmen der Ersterfassung müssen ausgehend von den wesentlichen Geschäftsprozessen und Fachverfahren die Anwendungen, IT-Systeme, Netzkomponenten, Räume und ähnliche Objekte identifiziert werden, die für die Durchführung der Geschäftsprozesse wesentlich sind. Hierbei sollten nicht nur die primären Abhängigkeiten betrachtet werden, also die für einen Geschäftsprozess direkt benötigten Applikationen und IT-Systeme. Auch sekundäre Abhängigkeiten, d.h. die kritischen Unter-

stützungsprozesse bzw. -systeme (wie Gebäudetechnik, Logistik usw.) sollten bei der Betrachtung berücksichtigt werden.

Wenn möglich, sollte zu diesem Zeitpunkt abgeschätzt werden, ob die identifizierten Objekte ein höheres Sicherheitsniveau als „normal" erfordern.

Dabei ist es häufig nicht zweckmäßig, jedes Objekt einzeln zu erfassen, da Informationsverbünde meist aus vielen Einzelobjekten bestehen. Stattdessen sollten ähnliche Objekte sinnvoll zu Gruppen zusammengefasst werden. Für die Ersterfassung kann es auch einfacher sein, in einem zweiten Schritt eine grafische Netzübersicht zu erstellen und ausgehend von dieser die IT-Systeme zu erfassen. Hierbei geht es nicht um Vollständigkeit oder Form. Das Ziel ist eine stark vereinfachte Netzübersicht.

Bei der Ersterfassung sollten auch nur die wesentlichen Objekte aufgenommen werden, nicht jede einzelne IT-Komponente. Beispielsweise sollten bei dieser keine typischen Büroräume aufgelistet werden, Serverräume mit ihrem speziellen, meist höheren Sicherheitsniveau sollten jedoch Erwähnung finden.

Erfassung der relevanten Objekte

Ausgehend von jedem Geschäftsprozess bzw. jeder Fachaufgabe, die im Informationsverbund enthalten ist, sollten folgende Objekte tabellarisch mit einem eindeutigen Bezeichner und mindestens folgenden Hinweisen erfasst werden:

- Geschäftsprozess oder Fachaufgabe: Name und (falls erforderlich) Beschreibung, fachverantwortliche Stelle
- Anwendung: Name, (falls erforderlich) Beschreibung und dazugehöriger Geschäftsprozess
- IT-, ICS-Systeme und sonstige Objekte: Name, Plattform und sofern sinnvoll Aufstellungsort
- für die Aufrechterhaltung des Betriebes wesentliche Räume, die dadurch ein höheres Sicherheitsniveau erfordern (z. B. Rechenzentrum, Serverräume): Art, Raumnummer und Gebäude

Virtuelle IT-Systeme und Netze sollten wie physische Strukturen behandelt werden, sollten aber geeignet gekennzeichnet sein.

Abschätzung des Sicherheitsniveaus

Für spätere Betrachtungen kann es sich als sinnvoll erweisen, schon zu einem frühen Zeitpunkt das angestrebte Sicherheitsniveau der einzelnen Assets abzuschätzen. Die eigentliche Schutzbedarfsfeststellung sollte allerdings zu einem späteren Zeitpunkt erfolgen. Diese Abschätzung des Sicherheitsniveaus bietet eine grobe Orientierung für den zu erwartenden Aufwand und erleichtert eine geeignete Gruppenbildung der identifizierten Assets.

Die bisher identifizierten Objekte, bei denen ein höheres Sicherheitsniveau als „normal" angestrebt wird, sollten in der bereits erstellten Tabelle gekennzeichnet werden.

Erstellung eines grafischen Netzplans

Auf Grundlage der erfassten Informationen sollte ein rudimentärer Netzplan als Übersicht erstellt werden. Wenn ein aktueller Netzplan vorhanden ist, kann dieser natürlich genutzt werden. Ein Netzplan ist eine grafische Übersicht über die im betrachteten Bereich der Informations- und Kommunikationstechnik eingesetzten Komponenten und deren Vernetzung. Im Gegensatz zu einem vollständigen oder vereinfachten Netzplan, wie er in der später folgenden Strukturanalyse erstellt wird, dient diese Netzübersicht vielmehr als Überblick, die die weitere Diskussion vereinfacht und zeigt, ob essenzielle IT-Systeme vergessen wurden. Im Einzelnen sollte der Plan in Bezug auf die Informationssicherheit mindestens folgende Objekte darstellen:

- IT-Systeme, d.h. Clients und Server, aktive Netzkomponenten
- Netzverbindungen zwischen diesen Systemen
- Verbindungen des betrachteten Bereichs nach außen

Die grafische Netzübersicht sollte sich aber nicht auf physische Komponenten beschränken, sondern auch virtualisierte Strukturen beinhalten. Hierbei können entweder virtuelle Strukturen (geeignet gekennzeichnet) direkt in der grafischen Netzübersicht aufgenommen werden oder bei unübersichtlichen Architekturen in eine separate Netzübersicht eingetragen werden.

Ein Beispiel für eine Ersterfassung einschließlich einer Netzübersicht ist in den Hilfsmitteln zum IT-Grundschutz zu finden. In der später durchzuführenden Strukturanalyse werden die hier gewonnenen Ergebnisse präzisiert und vervollständigt.

Aktionspunkte zu 3.2 Konzeption und Planung des Sicherheitsprozesses
• Ansprechpartner für alle Geschäftsprozesse und Fachaufgaben benennen • Grobeinschätzung der Wertigkeit und des Sicherheitsniveaus von Informationen, Geschäftsprozessen und Fachaufgaben durchführen • Interne und externe Rahmenbedingungen ermitteln • Bedeutung der Geschäftsprozesse, Fachaufgaben und Informationen abschätzen • Allgemeine Informationssicherheitsziele festlegen • Konsolidierte Übersicht der vorhandenen Assets mit den zuvor gewonnenen Erkenntnissen erstellen • Zustimmung der Leitungsebene einholen

3.3 Entscheidung für Vorgehensweise

Der IT-Grundschutz bietet verschiedene Vorgehensweisen an, die sich an unterschiedliche Anwendergruppen richten und unterschiedliche Ziele verfolgen: Basis-, Standard- und Kern-Absicherung. In diesem Schritt erfolgt die Auswahl der für die Institution optimalen Vorgehensweise basierend auf der bereits vorliegenden Entscheidungshilfe unter Zuhilfenahme der oben durchgeführten Ersterfassung.

Bei der Basis-Absicherung handelt es sich um eine grundlegende Absicherung der Geschäftsprozesse und Ressourcen einer Institution. Sie ermöglicht einen ersten Einstieg in den Sicherheitsprozess, um schnellstmöglich die größten Risiken zu senken. Im nächsten Schritt können die tatsächlichen Sicherheitsanforderungen im Detail analysiert werden. Diese Vorgehensweise ist daher besonders für kleinere Institutionen geeignet, die noch am Anfang ihres Sicherheitsprozesses stehen.

Die Kern-Absicherung dient als weitere Einstiegsvorgehensweise zum Schutz der essenziellen Geschäftsprozesse und Ressourcen einer Institution. Diese Vorgehensweise unterscheidet sich vom klassischen IT-Grundschutz durch die Fokussierung auf einen kleinen, aber sehr wichtigen Teil eines Informationsverbunds, die sogenannten „Kronjuwelen". Die Kern-Absicherung ist vor allem für Institutionen geeignet, die einige wenige Geschäftsprozesse identifiziert haben, die wesentlich für den Fortbestand der Institution sind und vorrangig abgesichert werden müssen.

Die dritte und vom BSI präferierte Vorgehensweise ist die Standard-Absicherung. Diese entspricht in den Grundzügen der bekannten und bewährten IT-Grundschutz-Vorgehensweise.

Die Basis- und die Kern-Absicherung sind jeweils Methoden, um zunächst zeitnah die wichtigsten Sicherheitsempfehlungen für den ausgewählten Einsatzbereich identifizieren und umsetzen zu können. Ziel muss es sein, mittelfristig ein vollständiges Sicherheitskonzept gemäß der Standard-Absicherung zu erstellen.

3.3.1 Basis-Absicherung

Die Basis-Absicherung verfolgt das Ziel, als Einstieg in den IT-Grundschutz zunächst eine breite, grundlegende Erst-Absicherung über alle relevanten Geschäftsprozesse bzw. Fachverfahren einer Institution hinweg zu erlangen. Diese Vorgehensweise ist für Institutionen empfehlenswert, bei denen folgende Punkte zutreffen:

- Die Umsetzung von Informationssicherheit steht noch am Anfang, d. h. die Informationssicherheit hat bisher nur einen niedrigen Reifegrad erreicht.
- Die Geschäftsprozesse weisen kein deutlich erhöhtes Gefährdungspotenzial bezüglich der Informationssicherheit auf.
- Das angestrebte Sicherheitsniveau ist normal.
- Es sind keine Assets vorhanden, deren Diebstahl, Zerstörung oder Kompromittierung einen existenzbedrohenden Schaden für die Institution bedeutet.
- Kleinere Sicherheitsvorfälle können toleriert werden – also solche, die zwar Geld kosten oder anderweitig Schaden verursachen, aber in der Summe nicht existenzbedrohend sind.

Mit der Basis-Absicherung können zeitnah zunächst die wichtigsten Sicherheitsanforderungen umgesetzt werden, um darauf aufbauend zu einem späteren Zeitpunkt das Sicherheitsniveau weiter zu erhöhen, indem beispielsweise alle Bereiche mit der Standard-Absicherung oder kritische Geschäftsprozesse mit der Kern-Absicherung geschützt werden.

3.3.2 Kern-Absicherung

Über die Kern-Absicherung kann eine Institution als Einstieg in den IT-Grundschutz bzw. den Sicherheitsprozess zunächst besonders gefährdete Geschäftsprozesse und Assets vorrangig absichern. Diese Vorgehensweise ist empfehlenswert, wenn für eine Institution folgende Aspekte überwiegend zutreffen:

- Die Menge der Geschäftsprozesse mit deutlich erhöhtem Schutzbedarf ist überschaubar bzw. umfasst nur einen kleinen Anteil aller Geschäftsprozesse der Institution.
- Die Institution kann die Geschäftsprozesse, die ein deutlich erhöhtes Gefährdungspotenzial bezüglich der Informationssicherheit aufweisen, zügig identifizieren und eindeutig abgrenzen.
- Die Institution besitzt eindeutig benennbare Assets, deren Diebstahl, Zerstörung oder Kompromittierung einen existenzbedrohenden Schaden für die Institution bedeuten würde (sogenannte Kronjuwelen). Diese sollen vorrangig geschützt werden.
- Kleinere Sicherheitsvorfälle, die Geld kosten oder anderweitig Schaden verursachen, aber keinen existenzbedrohenden Schaden bedeuten, sind für die Institution akzeptabel.

Mit der Kern-Absicherung können zeitnah die wichtigsten Ressourcen und Geschäftsprozesse abgesichert werden. So kann in einem ersten Schritt zunächst der kritischste Geschäftsprozess abgesichert werden, um in weiteren Schritten wahlweise die nächsten kritischen Geschäftsprozesse abzusichern oder für alle Bereiche der Institution die Basis- oder Standard-Absicherung zu beginnen. Eine Zertifi-

zierung nach ISO 27001 ist für den betrachteten abgegrenzten Informationsverbund grundsätzlich möglich.

3.3.3 Standard-Absicherung

Die Standard-Absicherung entspricht im Wesentlichen der klassischen IT-Grundschutz-Vorgehensweise nach BSI-Standard 100-2. Mit der Standard-Absicherung kann eine Institution umfassend und tiefgehend abgesichert werden. Dies sollte grundsätzlich das Ziel jeglicher Anwendung des IT-Grundschutzes sein, auch wenn zuvor zunächst eine der beiden bereits genannten anderen Vorgehensweisen gewählt wurde. Ein direkter Einstieg in den Sicherheitsprozess mit der Standard-Absicherung ist empfehlenswert, wenn für die Institution die folgenden Punkte überwiegend zutreffen:

- Die Institution arbeitet bereits mit dem IT-Grundschutz.
- Es wurden schon Sicherheitskonzepte nach IT-Grundschutz oder ISO 27001 erstellt.
- Die Umsetzung von Informationssicherheit hat in der Institution bereits einen ausreichenden Reifegrad erreicht, sodass in wesentlichen Bereichen bereits Sicherheitsmaßnahmen vorhanden sind und keine grundlegende Erst-Absicherung mehr notwendig ist.
- Es besteht kein Handlungsbedarf, einzelne Geschäftsprozesse vordringlich abzusichern, die ein deutlich höheres Gefährdungspotenzial bezüglich der Informationssicherheit besitzen (vergleiche Kern-Absicherung).
- Die Institution hat keine Assets, deren Diebstahl, Zerstörung oder Kompromittierung einen unmittelbar existenzbedrohenden Schaden nach sich ziehen könnte und die daher vorrangig abgesichert werden sollten.
- Sicherheitsvorfälle, die wahrnehmbar die Aufgabenerfüllung beeinträchtigen, Geld kosten oder anderweitig erkennbaren Schaden verursachen, sind für die Institution nicht akzeptabel, auch wenn sie noch keinen existenzbedrohenden Schaden verursachen.

Die Standard-Absicherung ist die Vorgehensweise, die grundsätzlich angestrebt werden sollte, um alle Bereiche einer Institution angemessen und umfassend zu schützen. Auch für eine angestrebte Zertifizierung des Informationsverbunds nach ISO 27001 ist diese Vorgehensweise (bzw. die Kern-Absicherung) die erforderliche Grundlage.

3.3.4 Festlegung des Geltungsbereichs

Der Geltungsbereich für die Erstellung der Sicherheitskonzeption wird im Folgenden „Informationsverbund“ genannt. Ein Informationsverbund umfasst die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei als Ausprägung die gesamte Informationsverarbeitung einer Institution oder auch einzelne Bereiche umfassen, die durch organisatorische oder technische Strukturen (z. B. Abteilungsnetz) oder gemeinsame Geschäftsprozesse bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind.

Neben der Vorgehensweise muss also auch festgelegt werden, wie der damit zu schützende Informationsverbund aussehen soll. Dieser kann die gesamte Institution umfassen oder aus Teilbereichen bestehen. Als Informationsverbund können beispielsweise bestimmte Organisationseinheiten einer Institution betrachtet werden. Es könnten aber auch Bereiche sein, die definierte Geschäftsprozesse bearbeiten, inklusive der dafür notwendigen Infrastruktur. Wichtig ist jedoch dabei, dass die betrachteten Geschäftsprozesse komplett im Geltungsbereich enthalten sind.

Während bei der Basis- und Standard-Absicherung der Geltungsbereich häufig die gesamte Institution umfasst, konzentriert man sich bei der Kern-Absicherung auf einige herausragende, besonders geschäftskritische Prozesse.

Es kann auch sinnvoll sein, Sicherheitskonzeptionen für mehrere kleinere Bereiche zu entwickeln. Dies kann beispielsweise der Fall sein, wenn der Aufwand für eine Gesamtabsicherung im ersten Schritt als zu hoch eingeschätzt wird und bestimmte Geschäftsprozesse priorisiert behandelt werden müssen. Hierfür könnten beispielsweise Bereiche identifiziert werden, für die parallel oder nacheinander Basis-, Standard- bzw. Kern-Absicherungen durchgeführt werden.

So könnte eine Institution beschließen, zunächst für einen kleinen Bereich mit besonders gefährdeten Assets die Kern-Absicherung umzusetzen. Damit aber auch für die restliche Institution ein Mindestmaß an Sicherheit vorhanden ist, sollte dort die Basis-Absicherung garantiert werden.

Es sollten nicht nur technische, sondern auch organisatorische Aspekte bei der Abgrenzung des Geltungsbereichs berücksichtigt werden, damit die Verantwortung und die Zuständigkeiten eindeutig festgelegt werden können. In jedem Fall sollte klar sein, welche Informationen, Fachaufgaben oder Geschäftsprozesse in der Sicherheitskonzeption explizit betrachtet werden.

Bei der Abgrenzung des Geltungsbereichs für die Sicherheitskonzeption müssen folgende Faktoren berücksichtigt werden:

- Der Geltungsbereich sollte möglichst alle Bereiche, Aspekte und Komponenten umfassen, die zur Unterstützung der Fachaufgaben, Geschäftsprozesse oder Organisationseinheiten dienen und deren Verwaltung innerhalb der Institution stattfindet.
- Wenn dies nicht möglich ist, weil Teile der betrachteten Fachaufgaben oder Geschäftsprozesse organisatorisch von externen Partnern abhängig sind, beispielsweise im Rahmen von Outsourcing, sollten die Schnittstellen klar definiert werden, damit dies im Rahmen der Sicherheitskonzeption berücksichtigt werden kann.

Aktionspunkte zu 3.3.4 Definition des Geltungsbereichs für die Sicherheitskonzeption
• Festlegen, welche kritischen Geschäftsprozesse, Fachaufgaben oder Teile der Institution der Geltungsbereich beinhalten soll
• Den Geltungsbereich eindeutig abgrenzen
• Schnittstellen zu externen Partnern beschreiben

3.3.5 Managemententscheidung

Der von der Leitungsebene benannte Verantwortliche für Informationssicherheit muss basierend auf den ermittelten Rahmenbedingungen, den formulierten Sicherheitszielen und dem angestrebten Sicherheitsniveau einen Vorschlag erarbeiten, wie die weiteren Schritte zur Erreichung der kurzfristigen sowie der langfristigen Sicherheitsziele aussehen sollten. Das Management muss auf dieser Grundlage entscheiden, für welche Bereiche der Institution welche Vorgehensweise zu deren Absicherung gewählt werden soll.

Es sollte anschließend dokumentiert werden, für welchen Bereich mit welchem Zeitplan eine Basis-, Standard- bzw. Kern-Absicherung umgesetzt werden soll. Die entsprechenden Geltungsbereiche des Informationsverbunds müssen festgelegt werden.

Die folgende Übersicht zeigt die wichtigsten Vor- und Nachteile der einzelnen Vorgehensweisen auf.

Basis-Absicherung

Pro Der Aufwand ist verhältnismäßig niedrig. Dadurch ist ein schneller Einstieg in die Informationssicherheit möglich. So lässt sich schnell eine grundlegende Erst-Absicherung erzielen.

Contra Durch eine pauschale Erfüllung der Erstanforderungen wird nur ein niedriges Sicherheitsniveau erreicht. Eventuell ist das erzielbare Schutzniveau nicht hoch genug für die tatsächlichen Sicherheitsanforderungen. Eine Zertifizierung nach ISO 27001 ist auf dieser Basis nicht möglich.

Kern-Absicherung

Pro Die Kern-Absicherung ermöglicht eine volle Fokussierung auf die Kronjuwelen, also die existenziell wichtigen Assets der Institution. Die Umsetzung ist schneller als bei der Einbeziehung aller Geschäftsprozesse. Eine Zertifizierung nach ISO 27001 ist für den betrachteten abgegrenzten Informationsverbund grundsätzlich möglich.

Contra Kronjuwelen können unter Umständen nicht isoliert betrachtet werden, wodurch umfangreichere Anteile der Institution einbezogen werden müssen. Alle nicht als kritisch eingestuften Geschäftsprozesse bleiben zunächst unbeachtet. Dabei besteht die Gefahr, dass einerseits wichtige Bereiche übersehen und somit gänzlich ungeschützt gelassen werden. Andererseits könnten kumulierte Risiken übersehen werden.

Standard-Absicherung

Pro Die Standard-Absicherung bietet ein hohes und an die vorhandenen Geschäftsprozesse spezifisch angepasstes Sicherheitsniveau. Es wird ein gleichmäßiges Sicherheitsniveau über die gesamte Institution erzielt. Das erreichte Sicherheitsniveau ist mit jenem anderer Institutionen gut vergleichbar. Eine Zertifizierung nach ISO 27001 und eine Messbarkeit des ISMS sind möglich. Es werden alle notwendigen Ressourcen der Institution vollständig betrachtet.

Contra Der Aufwand ist bei einem niedrigen Reifegrad der vorhandenen Informationssicherheit höher als bei den beiden anderen Vorgehensweisen.

Aktionspunkte zu 3.3.5 Managemententscheidung
• Erarbeitung einer Managementvorlage zur Entscheidungsfindung
• Entscheidung, für welche Bereiche der Institution welche Vorgehensweise zu deren Absicherung gewählt werden soll
• Dokumentation der Entscheidung und des Zeitplans für die Umsetzung

3.4 Erstellung einer Leitlinie zur Informationssicherheit

Die Leitlinie zur Informationssicherheit beschreibt allgemein verständlich, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Institution hergestellt werden soll. Sie beinhaltet die von der Institution angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Die Sicherheitsleitlinie beschreibt damit auch über die Sicherheitsziele das angestrebte Sicherheitsniveau in einer Behörde oder einem Unternehmen. Sie ist somit Anspruch und Aussage zugleich, dass dieses Sicherheitsniveau auf allen Ebenen der Institution erreicht werden soll.

Die Erstellung der Sicherheitsleitlinie sollte in den nachfolgenden Schritten vollzogen werden:

3.4.1 Verantwortung der Behörden- bzw. Unternehmensleitung für die Sicherheitsleitlinie

Mit der Leitlinie zur Informationssicherheit wird dokumentiert, welche strategische Position die Institutionsleitung zur Erreichung der Informationssicherheitsziele auf allen Ebenen der Organisation einnimmt.

Da die Sicherheitsleitlinie ein zentrales Strategiepapier für die Informationssicherheit einer Institution darstellt, muss sie so gestaltet sein, dass sich alle adressierten Organisationseinheiten mit ihrem Inhalt identifizieren können. An ihrer Erstellung sollten daher möglichst viele Bereiche beteiligt werden. Jede Institution muss letztendlich aber selbst entscheiden, welche Abteilungen und Hierarchieebenen an der Formulierung der Sicherheitsleitlinie mitwirken.

Es empfiehlt sich bei der Erarbeitung der Sicherheitsleitlinie, das Fachwissen der folgenden Organisationseinheiten zu nutzen: Fachverantwortliche für wichtige Anwendungen, IT-Betrieb, Sicherheit (Informations-, IT- und Infrastruktur-Sicherheit), Datenschutzbeauftragter, Produktion und Fertigung, Personalabteilung, Personalvertretung, Revision, Vertreter für Finanzfragen, Rechtsabteilung.

3.4.2 Einberufung einer Entwicklungsgruppe für die Sicherheitsleitlinie

Falls es innerhalb der Institution bereits ein IS-Management-Team gibt, so sollte dieses die Informationssicherheitsleitlinie entwickeln bzw. überprüfen und überarbeiten. Danach wird dieser Entwurf der Behörden- bzw. Unternehmensleitung zur Genehmigung vorgelegt.

Befindet sich das Informationssicherheitsmanagement erst im Aufbau, so sollte eine Entwicklungsgruppe zur Erarbeitung der Sicherheitsleitlinie eingerichtet werden. Diese Gruppe kann im Laufe des Sicherheitsprozesses die Funktion des IS-Management-Teams übernehmen. Sinnvollerweise sollten in dieser Entwicklungsgruppe Vertreter der IT- bzw. ICS-Anwender, Vertreter des IT- bzw. ICS-Betriebs und ein oder mehrere in Sachen Informationssicherheit ausreichend vorgebildete Mitarbeiter mitwirken. Idealerweise sollte zeitweise auch ein Mitglied der Leitungsebene, das die Bedeutung der Informationsverarbeitung für die Institution einschätzen kann, hinzugezogen werden.

3.4.3 Festlegung des Geltungsbereichs und Inhalt der Sicherheitsleitlinie

In der Informationssicherheitsleitlinie muss beschrieben werden, für welche Bereiche diese gelten soll. Der Geltungsbereich kann die gesamte Institution umfassen oder aus Teilbereichen dieser bestehen. Wichtig ist jedoch dabei, dass die betrachteten Geschäftsaufgaben und -prozesse in dem Geltungsbereich komplett enthalten sind. Insbesondere bei größeren Institutionen ist die Festlegung des Geltungsbereichs keine triviale Aufgabe. Eine Orientierung nach den jeweiligen Verantwortlichkeiten kann dabei behilflich sein.

Die Sicherheitsleitlinie sollte kurz und bündig formuliert sein, da sich mehr als 20 Seiten in der Praxis nicht bewährt haben. Sie sollte jedoch mindestens die folgenden Informationen beinhalten:

- Stellenwert der Informationssicherheit und Bedeutung der wesentlichen Informationen, Geschäftsprozesse und der IT für die Aufgabenerfüllung,
- Bezug der Informationssicherheitsziele zu den Geschäftszielen oder Aufgaben der Institution,
- Sicherheitsziele und die Kernelemente der Sicherheitsstrategie für die Geschäftsprozesse und die eingesetzte IT,
- Zusicherung, dass die Sicherheitsleitlinie von der Institutionsleitung durchgesetzt wird, sowie Leitaussagen zur Erfolgskontrolle und

- Beschreibung der für die Umsetzung des Informationssicherheitsprozesses etablierten Organisationsstruktur.

Zusätzlich können z. B. noch folgende Aussagen hinzukommen:

- Zur Motivation können einige, für die Geschäftsprozesse wichtige Gefährdungen, thematisiert und die wichtigsten gesetzlichen Regelungen und sonstige wichtige Rahmenbedingungen (wie vertragliche Vereinbarungen) genannt werden.
- Die wesentlichen Aufgaben und Zuständigkeiten im Sicherheitsprozess sollten aufgezeigt werden (insbesondere für das IS-Management-Team, den IS-Beauftragten, die Mitarbeiter und den IT-Betrieb, ausführliche Informationen zu den einzelnen Rollen finden sich in Kapitel 4 *Organisation des Sicherheitsprozesses*. Außerdem sollten die Organisationseinheiten oder Rollen benannt werden, die als Ansprechpartner für Sicherheitsfragen fungieren.
- Programme zur Förderung der Informationssicherheit durch Schulungs- und Sensibilisierungsmaßnahmen können angekündigt werden.

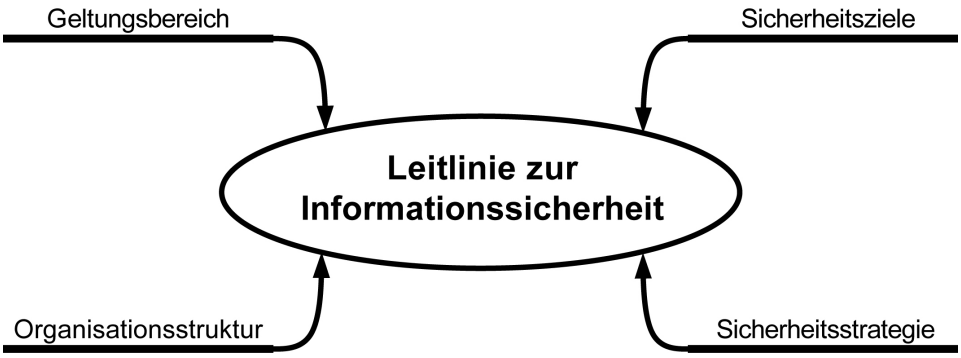


Abbildung 2: Inhalte der Sicherheitsleitlinie

3.4.4 Bekanntgabe der Sicherheitsleitlinie

Es ist wichtig, dass die Behörden- bzw. Unternehmensleitung ihre Zielsetzungen und Erwartungshaltungen durch Bekanntgabe der Sicherheitsleitlinie unterstreicht und den Stellenwert sowie die Bedeutung der Informationssicherheit in der gesamten Institution verdeutlicht. Alle Mitarbeiter sollten daher die Inhalte der Sicherheitsleitlinie kennen und nachvollziehen können. Neuen Mitarbeitern sollte die Sicherheitsleitlinie erläutert werden, bevor sie Zugang zur Informationsverarbeitung erhalten.

Da die Verantwortung der Behörden- bzw. Unternehmensleitung in Bezug auf die Sicherheitsleitlinie entscheidend ist, sollte die Leitlinie schriftlich fixiert sein. Die Behörden- bzw. Unternehmensleitung sollte ihr formell zugestimmt haben. Die Inhalte der Sicherheitsleitlinie sollten also innerhalb der Institution nicht nur bekannt sein, sondern auf diese sollte auch möglichst einfach zuzugreifen sein, z. B. im Intranet der Institution. Wenn die Leitlinie vertrauliche Aussagen enthält, sollten diese in einer Anlage abgespeichert werden, die deutlich als vertraulich gekennzeichnet ist.

Schließlich sollten alle Mitarbeiter darauf aufmerksam gemacht werden, dass nicht nur bei der Aufgabenerfüllung allgemein, sondern auch bei der Erfüllung der Aufgabe „Informationssicherheit“ von jedem Mitarbeiter ein engagiertes, kooperatives sowie verantwortungsbewusstes Handeln erwartet wird.

3.4.5 Aktualisierung der Sicherheitsleitlinie

Die Leitlinie zur Informationssicherheit sollte in regelmäßigen Abständen auf ihre Aktualität hin überprüft und gegebenenfalls angepasst werden. Hierbei sollte beispielsweise überlegt werden, ob sich Geschäftsziele oder Aufgaben und damit Geschäftsprozesse geändert haben, ob wesentliche IT-Verfahren oder ICS-Komponenten geändert worden sind, ob die Organisationsstruktur neu ausgerichtet wurde oder ob neue IT- oder ICS-Systeme eingeführt worden sind. Bei den häufig rasanten Entwicklungen im Bereich der IT einerseits und der Sicherheitslage andererseits empfiehlt es sich, die Sicherheitsleitlinie spätestens alle zwei Jahre erneut zu überdenken.

Aktionspunkte zu 3.4 Erstellung einer Sicherheitsleitlinie
• Auftrag der Leitungsebene zur Erarbeitung einer Sicherheitsleitlinie einholen
• Entwicklungsgruppe für die Sicherheitsleitlinie einberufen
• Geltungsbereich und Inhalte festlegen
• Inkraftsetzung der Sicherheitsleitlinie durch die Leitungsebene veranlassen
• Sicherheitsleitlinie bekannt geben
• Sicherheitsleitlinie regelmäßig überprüfen und gegebenenfalls aktualisieren

4 Organisation des Sicherheitsprozesses

Das angestrebte Sicherheitsniveau kann nur erreicht werden, wenn der Informationssicherheitsprozess für den gesamten Geltungsbereich umgesetzt wird. Dieser übergreifende Charakter des Sicherheitsprozesses macht es notwendig, Rollen innerhalb der Institution festzulegen und den Rollen die entsprechenden Aufgaben zuzuordnen. Diese Rollen müssen dann qualifizierten Mitarbeitern übertragen und von diesen ausgeführt werden. Nur so kann gewährleistet werden, dass alle wichtigen Aspekte berücksichtigt und sämtliche anfallende Aufgaben effizient und effektiv erledigt werden.

Die Aufbauorganisation, die zur Förderung und Durchsetzung des Informationssicherheitsprozesses erforderlich ist, wird als Informationssicherheitsorganisation oder kurz IS-Organisation bezeichnet.

Wie viele Personen in welcher Organisationsstruktur und mit welchen Ressourcen mit Informationssicherheit beschäftigt sind, hängt von der Größe, Beschaffenheit und Struktur der jeweiligen Institution ab. Auf jeden Fall sollte als zentraler Ansprechpartner für die Koordination, Verwaltung und Kommunikation des Prozesses „Informationssicherheit" ein Informationssicherheitsbeauftragter (ISB) benannt werden. In größeren Institutionen gibt es darüber hinaus typischerweise weitere Personen, die verschiedene Teilaufgaben für Informationssicherheit wahrnehmen. Um deren Tätigkeiten aufeinander abzustimmen, sollte ein IS-Management-Team aufgebaut werden, das sämtliche übergreifenden Belange der Informationssicherheit regelt und Pläne, Vorgaben und Richtlinien erarbeitet.

Um den direkten Zugang zur Institutionsleitung sicherzustellen, sollten diese Rollen als Stabsstelle organisiert sein. Auf Leitungsebene sollte die Aufgabe der Informationssicherheit eindeutig einem verantwortlichen Manager zugeordnet sein, an den der ISB berichtet.

Unabhängig davon, wie eine optimale Struktur für die eigene IS-Organisation zu gestalten ist, sind die drei folgenden Grundregeln dabei unbedingt zu beachten.

Grundregeln bei der Definition von Rollen im Informationssicherheitsmanagement

- Die Gesamtverantwortung für die ordnungsgemäße und sichere Aufgabenerfüllung (und damit für die Informationssicherheit) verbleibt bei der Leitungsebene.
- Es ist mindestens eine Person (typischerweise als Informationssicherheitsbeauftragter) zu benennen, die den Informationssicherheitsprozess fördert und koordiniert.
- Jeder Mitarbeiter ist gleichermaßen für seine originäre Aufgabe wie für die Aufrechterhaltung der Informationssicherheit an seinem Arbeitsplatz und in seiner Umgebung verantwortlich.

4.1 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse

Das Management der Informationssicherheit ist zwar nur eine von vielen wichtigen Managementaufgaben, hat jedoch Einfluss auf nahezu alle Bereiche einer Institution. Daher muss das Informationssicherheitsmanagement vernünftig in bestehende Organisationsstrukturen integriert und Ansprechpartner festgelegt werden. Aufgaben und Zuständigkeiten müssen klar voneinander abgegrenzt sein. Es muss dabei gewährleistet sein, dass nicht nur bei einzelnen Maßnahmen, sondern bei allen strategischen Entscheidungen die notwendigen Sicherheitsaspekte berücksichtigt werden. Dazu gehören zum Beispiel Entscheidungen über Outsourcing oder die Nutzung neuer elektronischer Vertriebskanäle ebenso wie die Anmietung neuer Räumlichkeiten. Daher muss die IS-Organisation bei allen Projekten, die Auswirkungen auf die Informationssicherheit haben könnten, rechtzeitig beteiligt werden.

Vor allem in größeren Institutionen existiert bereits häufig ein übergreifendes Risikomanagementsystem. Da Informationssicherheitsrisiken ebenso wie IT-Risiken zu den wichtigsten operationellen Risiken gehören, sollten die Methoden zum Informationssicherheitsmanagement und zum Management von Risiken mit den bereits etablierten Methoden und Managementsystemen abgestimmt werden, siehe hierzu auch BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz*.

4.2 Aufbau der Informationssicherheitsorganisation

In Abhängigkeit von der Institutionsgröße bieten sich verschiedene Möglichkeiten für die Aufbauorganisation des Informationssicherheitsmanagements an.

In den nachstehenden Abbildungen werden drei davon aufgezeigt. Die Abbildung 3 zeigt die Struktur für die IS-Organisation in einer großen Institution. Die Abbildung 4 zeigt den Aufbau in einer mittelgroßen Institution, in der das IS-Management-Team und der Sicherheitsbeauftragte zusammengefasst wurden. Die Abbildung 5 zeigt eine Struktur für die IS-Organisation in einer kleinen Institution, in der alle Aufgaben vom Informationssicherheitsbeauftragten wahrgenommen werden. Die Abbildung 6 zeigt eine Struktur der IS-Organisation, in der ein ICS-Bereich integriert ist.

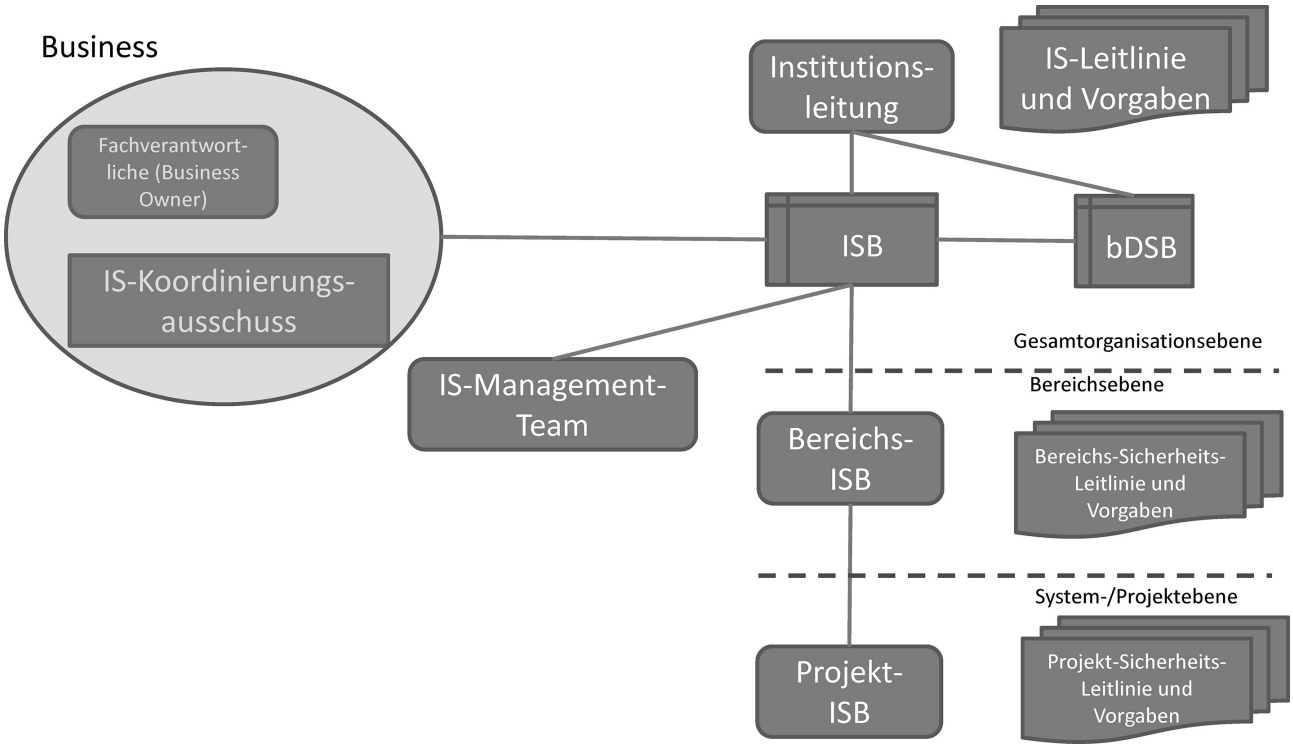


Abbildung 3: Aufbau einer IS-Organisation in einer großen Institution

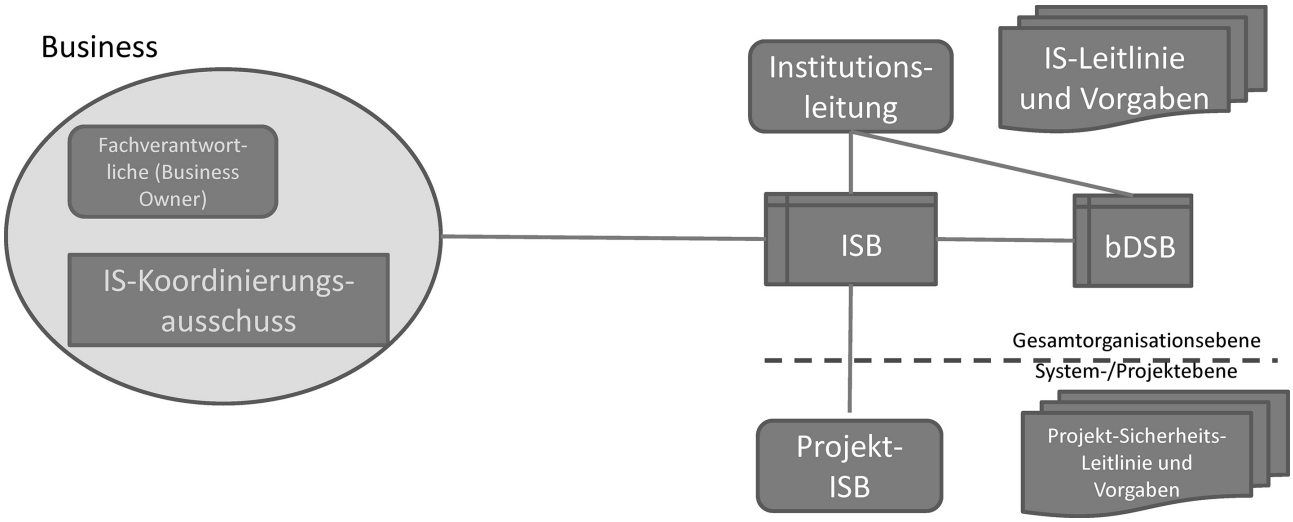


Abbildung 4: Aufbau der IS-Organisation in einer mittelgroßen Institution

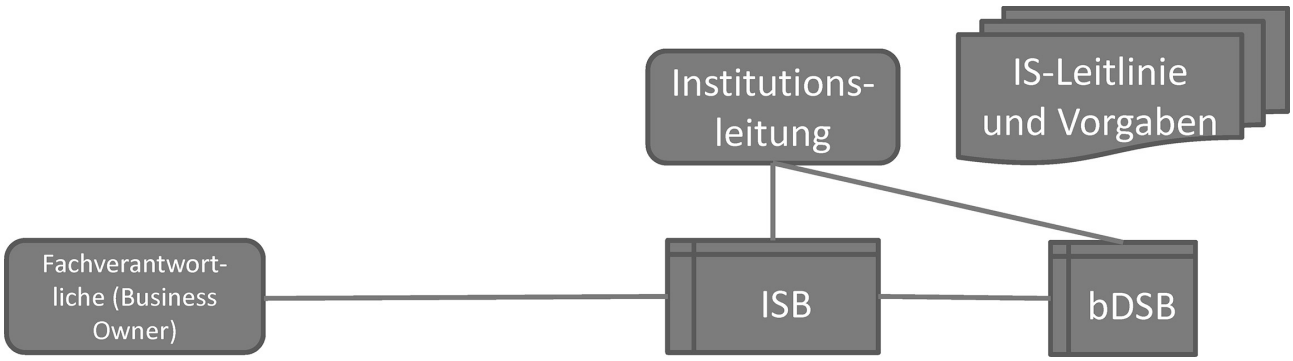


Abbildung 5: Aufbau der IS-Organisation in einer kleinen Institution

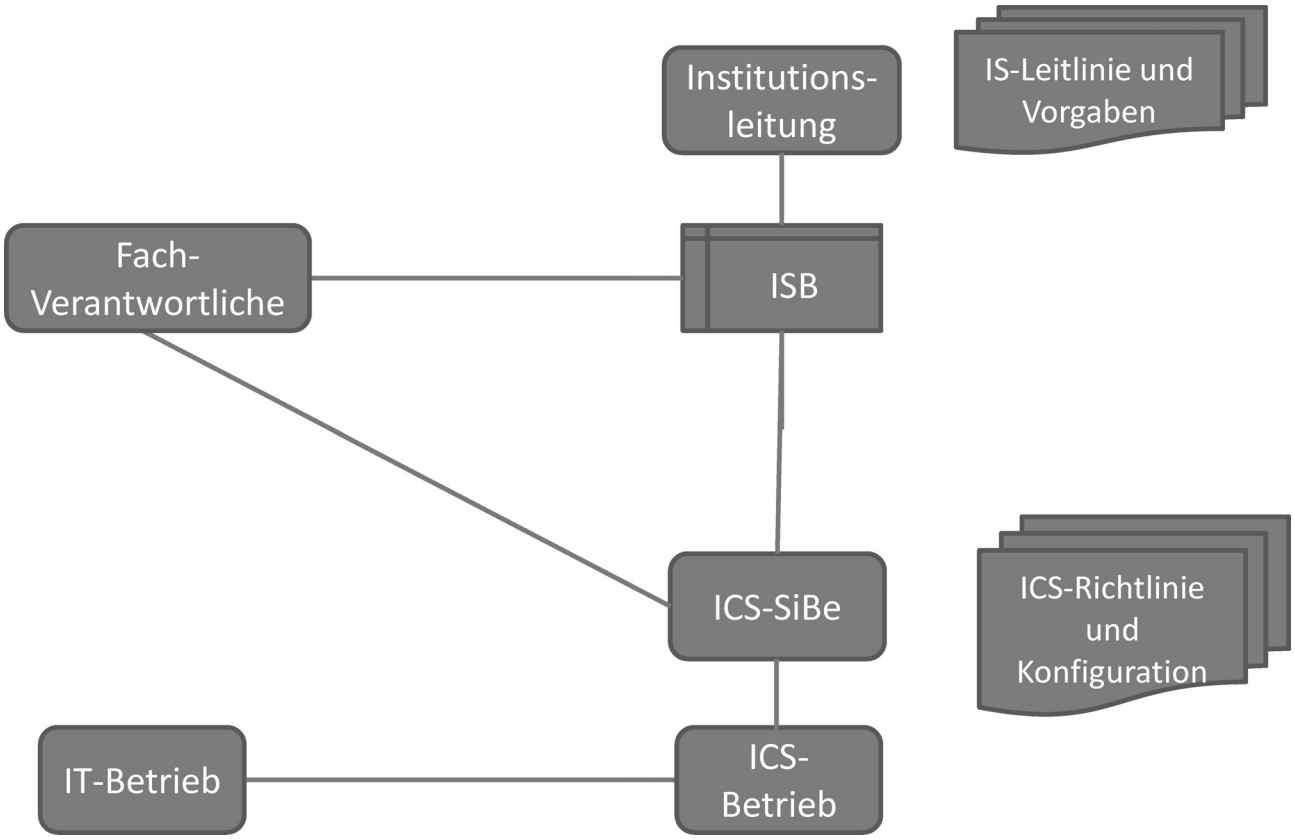


Abbildung 6: Aufbau der IS-Organisation mit integriertem ICS-Bereich

An dieser Stelle sei deutlich darauf hingewiesen, dass die in den Abbildungen dargestellten zentralen Rollen nicht unbedingt von verschiedenen Personen wahrgenommen werden müssen. Die personelle Ausgestaltung richtet sich nach der Größe der jeweiligen Institution, den vorhandenen Ressourcen und dem angestrebten Sicherheitsniveau. Die Ressourcenplanung für die Unterstützung der Informationssicherheit muss so erfolgen, dass das beschlossene Sicherheitsniveau auch tatsächlich erreicht werden kann.

4.3 Aufgaben, Verantwortungen und Kompetenzen in der IS-Organisation

Der Informationssicherheitsbeauftragte und das IS-Management-Team müssen klar definierte Aufgaben, Verantwortungsbereiche und Kompetenzen haben, die von der Leitungsebene festzulegen sind. Um ihre Aufgabe wahrnehmen zu können, sollten sie an allen relevanten Verfahren und Entscheidungen beteiligt werden. Die Rollen sind so in die Organisationsstruktur einzubinden, dass alle Beteiligten untereinander kommunizieren können. Außerdem muss geklärt sein, wer im Rahmen des Sicherheitsmanagements mit welchen internen und externen Stellen wann worüber kommuniziert sowie welche Kommunikationskanäle für die jeweiligen Ansprechpartner genutzt und wie diese geschützt werden (siehe hierzu auch Kapitel 5.2 *Informationsfluss im Informationssicherheitsprozess*).

Mit der Wahrnehmung der Aufgaben als Sicherheitsbeauftragte bzw. im IS-Management-Team sollte stets qualifiziertes Personal betraut werden. Bei Bedarf können unterstützend Aufgaben an weitere Rollen, wie beispielsweise

- Bereichs-ISB (Informationssicherheitsbeauftragter für einen Bereich, Abteilung, Außenstelle, o.Ä.),
- Projekt-ISB sowie
- ICS-ISB (Informationssicherheitsbeauftragter für den Bereich der industriellen Steuerung),

delegiert werden.

4.4 Der Informationssicherheitsbeauftragte

Informationssicherheit wird häufig vernachlässigt, sodass sie hinter dem Tagesgeschäft zurückfällt. Dadurch besteht bei unklarer Aufteilung der Zuständigkeiten die Gefahr, dass Informationssicherheit grundsätzlich zu einem „Problem anderer Leute" wird. Damit wird die Verantwortung für Informationssicherheit so lange hin- und hergeschoben, bis keiner sie mehr zu haben glaubt. Um dies zu vermeiden, sollte ein Hauptansprechpartner für alle Aspekte rund um die Informationssicherheit, ein Informationssicherheitsbeauftragter oder kurz ISB, ernannt werden, der die Aufgabe „Informationssicherheit" koordiniert und innerhalb der Institution vorantreibt. Ob es neben einem solchen weitere Personen mit Sicherheitsaufgaben gibt und wie die Informationssicherheit organisiert ist, hängt von der Art und Größe der Institution ab.

Die Rolle des Verantwortlichen für Informationssicherheit wird je nach Art und Ausrichtung der Institution anders genannt. Häufige Titel sind neben dem Informationssicherheitsbeauftragten auch Chief Information Security Officer (CISO) oder Informationssicherheitsmanager (ISM). In den IT-Grundschutz-Dokumenten wurde bislang die Bezeichnung IT-Sicherheitsbeauftragter (IT-SiBe) verwendet, da dieser Begriff in Unternehmen und Behörden lange Zeit der am weitesten verbreitete war. Mit dem Titel „Sicherheitsbeauftragter" werden dagegen häufig diejenigen Personen bezeichnet, die für Arbeitsschutz, Betriebssicherheit oder Werkschutz zuständig sind.

Aus diesen Titeln folgt aber auch häufig ein anderes Rollenverständnis. So macht der Titel des Informationssicherheitsbeauftragten statt des IT-Sicherheitsbeauftragten deutlich, dass diese Person sich um die Absicherung aller Arten von Informationen kümmert und nicht nur um IT-bezogene Aspekte. Informationssicherheit sollte aber immer ein Teil des operationellen Risikomanagements einer Institution sein. Aus diesem Grund ersetzt die Bezeichnung „Informationssicherheitsbeauftragter" (ISB) im IT-Grundschutz in diesem Zusammenhang die Bezeichnung „IT-Sicherheitsbeauftragter" (IT-SiBe).

Eng damit hängt auch die Frage zusammen, wo der Sicherheitsbeauftragte organisatorisch verankert ist. Es ist empfehlenswert, die Position des Informationssicherheitsbeauftragten direkt der obersten Leitungsebene zuzuordnen. Es ist davon abzuraten, den Sicherheitsbeauftragten in der IT-Abteilung zu verorten, da es hierbei zu Rollenkonflikten kommen kann.

Um einen Sicherheitsprozess erfolgreich planen, umsetzen und aufrechterhalten zu können, müssen die Verantwortlichkeiten klar definiert werden. Es müssen also Rollen definiert sein, die die verschiedenen Aufgaben im Hinblick auf das Erreichen der Informationssicherheitsziele wahrnehmen müssen. Zudem müssen Personen benannt sein, die qualifiziert sind und denen im ausreichenden Maße Ressourcen zur Verfügung stehen, um diese Rollen ausfüllen zu können.

Zuständigkeiten und Aufgaben

Der Informationssicherheitsbeauftragte ist zuständig für die Wahrnehmung aller Belange der Informationssicherheit innerhalb der Institution. Die Hauptaufgabe des ISB besteht darin, die Behörden- bzw. Unternehmensleitung bei deren Aufgabenwahrnehmung bezüglich der Informationssicherheit zu beraten und diese bei der Umsetzung zu unterstützen. Seine Aufgaben umfassen unter anderem:

- den Informationssicherheitsprozess zu steuern und an allen damit zusammenhängenden Aufgaben mitzuwirken,
- die Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit zu unterstützen,
- die Erstellung des Sicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte und System-Sicherheitsrichtlinien zu koordinieren sowie weitere Richtlinien und Regelungen zur Informationssicherheit zu erlassen,
- die Realisierung von Sicherheitsmaßnahmen zu initiieren und zu überprüfen,
- der Leitungsebene und dem IS-Management-Team über den Status quo der Informationssicherheit zu berichten,
- sicherheitsrelevante Projekte zu koordinieren,
- Sicherheitsvorfälle zu untersuchen und
- Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren und koordinieren.

Der ISB ist außerdem bei allen größeren Projekten, die deutliche Auswirkungen auf die Informationsverarbeitung haben könnten, zu beteiligen, um die Beachtung von Sicherheitsaspekten in den verschiedenen Projektphasen zu gewährleisten. So sollte der ISB bei der Planung und Einführung neuer Anwendungen und IT-Systeme ebenso beteiligt sein wie bei neuen ICS-Komponenten oder wesentlichen Änderungen der Infrastruktur.

Anforderungsprofil

Zur Erfüllung dieser Aufgaben ist es wünschenswert, dass der Informationssicherheitsbeauftragte über Wissen und Erfahrung auf den Gebieten der Informationssicherheit und IT verfügt. Ebenso sollte er Kenntnisse hinsichtlich der Geschäftsprozesse der Institution mitbringen. Da diese Aufgabe eine Vielzahl von Fähigkeiten erfordert, sollte bei der Auswahl des Weiteren darauf geachtet werden, dass die folgenden Qualifikationen vorhanden sind:

- Identifikation mit den Zielsetzungen der Informationssicherheit, Überblick über Aufgaben und Ziele der Institution.
- Kooperations- und Teamfähigkeit, aber auch Durchsetzungsvermögen (Kaum eine Aufgabe erfordert so viel Fähigkeit und Geschick im Umgang mit anderen Personen: Die Leitungsebene muss in zentralen Fragen des Sicherheitsprozesses immer wieder eingebunden werden. Entscheidungen müssen eingefordert werden und die Mitarbeiter müssen, eventuell mithilfe des Bereichs-Sicherheitsbeauftragten, in den Sicherheitsprozess eingebunden werden).
- Erfahrungen im Projektmanagement, idealerweise im Bereich der Systemanalyse und Kenntnisse über Methoden zur Risikoanalyse.
- Grundlegende Kenntnisse über die Prozesse und Fachaufgaben innerhalb der Institution und, soweit erforderlich, Grundkenntnisse in den Bereichen IT und ICS.

- Ein Informationssicherheitsbeauftragter muss zudem die Bereitschaft mitbringen, sich in neue Gebiete einzuarbeiten und Entwicklungen in der IT zu verfolgen. Er sollte sich so aus- und fortbilden, dass er die erforderlichen Fachkenntnisse für die Erledigung seiner Aufgaben besitzt.

Kooperation und Kommunikation

Die Zusammenarbeit mit den Mitarbeitern ebenso wie mit Externen verlangt viel Geschick, da diese zunächst von der Notwendigkeit der (für sie manchmal lästigen) Sicherheitsmaßnahmen überzeugt werden müssen. Ein ebenfalls sehr sensibles Thema ist die Befragung der Mitarbeiter nach sicherheitskritischen Vorkommnissen und Schwachstellen. Um den Erfolg dieser Befragungen zu garantieren, müssen die Mitarbeiter davon überzeugt werden, dass ehrliche Antworten nicht zu Problemen für sie selbst führen.

Die Kommunikationsfähigkeiten des Informationssicherheitsbeauftragten sind nicht nur gegenüber den Mitarbeitern gefordert. Genauso wichtig ist es, dass der ISB in der Lage ist, seine fachliche Meinung gegenüber der Behörden- oder Unternehmensleitung zu vertreten. Er muss so selbstbewusst und kommunikationsstark sein, um gelegentlich auch Einspruch gegen eine Entscheidung einzulegen, die mit den Sicherheitszielen nicht vereinbar ist.

Der Informationssicherheitsbeauftragte muss seine Kommunikationsfähigkeit derart einsetzen können, dass es in anderen Fachbereichen nicht zu Missverständnissen kommt. Hierzu ist es besonders wichtig, die jeweils anderen Sprachwelten und Kulturen zu verstehen und zu respektieren. So verwenden beispielsweise Ansprechpartner aus dem Bereich der industriellen Steuerung andere Begriffe für das IT-Equipment als IT-Experten.

Unabhängigkeit

Es ist empfehlenswert, die Position des Informationssicherheitsbeauftragten organisatorisch als Stabsstelle einzurichten, also als eine direkt der Leitungsebene zugeordnete Position, die von keinen anderen Stellen Weisungen bekommt. In jedem Fall muss der ISB das direkte und jederzeitige Vorspracherecht bei der Behörden- bzw. Unternehmensleitung haben, um diese über Sicherheitsvorfälle, -risiken und -maßnahmen informieren zu können. Er muss aber auch über das Geschehen in der Institution, soweit es einen Bezug zu seiner Tätigkeit hat, umfassend und frühzeitig unterrichtet werden.

Der Informationssicherheitsbeauftragte sollte nicht organisatorisch der IT-Abteilung zugeordnet sein. Die Erfahrung hat zeigt, dass dies häufig dazu führt, dass die Aufgabe der Informationssicherheit auf IT-Absicherung reduziert wird und der ganzheitliche Schutz von Informationen in den Hintergrund gerückt wird. Dadurch kann es vorkommen, dass Informationen so lange angemessen geschützt werden, wie sie ausschließlich auf IT-Systemen verarbeitet werden, aber diese dann beispielsweise nach dem Ausdrucken ungeschützt beim Drucker liegen bleiben. Ein anderes Problem ist der inhärente Aufgabenkonflikt. Es ist z. B. problematisch, wenn ein „aktiver" Administrator die Rolle des Informationssicherheitsbeauftragten zusätzlich zu seinen normalen Aufgaben wahrnimmt, da es mit hoher Wahrscheinlichkeit zu Interessenkonflikten kommen wird. Die Personalunion kann dazu führen, dass er als Informationssicherheitsbeauftragter Einspruch gegen Entscheidungen einlegen müsste, die ihm sein Leben als Administrator wesentlich erleichtern würden oder die gar von seinem Fachvorgesetzten stark favorisiert werden (siehe auch Kapitel 4.10 „Zusammenspiel mit anderen Organisationseinheiten und Managementdisziplinen").

Personalunion mit dem Datenschutzbeauftragten

Eine häufige Frage ist, ob die Position des Informationssicherheitsbeauftragten gleichzeitig vom Datenschutzbeauftragten wahrgenommen werden kann (zu dessen Aufgaben siehe unten). Die beiden Rollen schließen sich nicht grundsätzlich aus, es sind allerdings einige Aspekte im Vorfeld zu klären:

- Die Schnittstellen zwischen den beiden Rollen sollten klar definiert und dokumentiert werden. Außerdem sollten auf beiden Seiten direkte Berichtswege zur Leitungsebene existieren. Weiterhin sollte überlegt werden, ob konfliktträchtige Themen zusätzlich noch nachrichtlich an die Revision weitergeleitet werden sollten.
- Es muss sichergestellt sein, dass der Informationssicherheitsbeauftragte über ausreichend freie Ressourcen für die Wahrnehmung beider Rollen verfügt. Gegebenenfalls muss er durch entsprechendes Personal unterstützt werden.

Es darf nicht vergessen werden, dass auch der Informationssicherheitsbeauftragte einen qualifizierten Vertreter benötigt.

4.5 Das IS-Management-Team

Das IS-Management-Team unterstützt den Informationssicherheitsbeauftragten, indem es übergreifende Maßnahmen in der Gesamtorganisation koordiniert, Informationen zusammenträgt und Kontrollaufgaben durchführt. Die genaue Ausprägung hängt von der Größe der jeweiligen Institution, dem angestrebten Sicherheitsniveau und den vorhandenen Ressourcen ab. Im Extremfall besteht das IS-Management-Team nur aus zwei Personen, dem Informationssicherheitsbeauftragten, dem in diesem Fall sämtliche Aufgaben im Sicherheitsprozess obliegen, und seinem Stellvertreter.

Aufgaben des IS-Management-Teams sind insbesondere:

- Informationssicherheitsziele und -strategien zu bestimmen sowie die Leitlinie zur Informationssicherheit zu entwickeln,
- die Umsetzung der Sicherheitsleitlinie zu überprüfen,
- den Sicherheitsprozess zu initiieren, zu steuern und zu kontrollieren,
- bei der Erstellung des Sicherheitskonzepts mitzuwirken,
- zu überprüfen, ob die im Sicherheitskonzept geplanten Sicherheitsmaßnahmen wie beabsichtigt funktionieren sowie geeignet und wirksam sind,
- die Schulungs- und Sensibilisierungsprogramme für Informationssicherheit zu konzipieren sowie
- die Fachverantwortlichen, den IT-Betrieb, die Bereichs-ISBs, eventuell den ICS-ISB und die Leitungsebene in Fragen der Informationssicherheit zu beraten.

Zusammensetzung des Teams

Um seine Aufgaben erfüllen zu können, sollte sich das IS-Management-Team aus Personen zusammensetzen, die über Kenntnisse in Informationssicherheit und technische Kenntnisse über die in der Institution eingesetzten IT-, ICS- und IoT-Systeme verfügen sowie Erfahrungen mit Organisation und Verwaltung haben. Darüber hinaus sollte das IS-Management-Team die unterschiedlichen Aufgabenbereiche und Geschäftsprozesse einer Institution kennen. In großen Institutionen ist es sinnvoll, wenn die verschiedenen Fachbereiche einer Institution jeweils einen Vertreter im IS-Management-Team haben. Diese Person übernimmt die Vertretung im IS-Management-Team neben ihren Fachaufgaben, bringt die Expertise aus dem Fachbereich ein und wird dadurch gleichzeitig Ansprechpartner für Sicherheitsfragen der Mitarbeiter aus diesem Bereich.

4.6 Bereichs- und Projekt-Sicherheitsbeauftragte bzw. Beauftragter für IT-Sicherheit

Bei großen Institutionen kann es erforderlich sein, in den verschiedenen Bereichen eigene Sicherheitsbeauftragte einzusetzen.

Bereichs-Sicherheitsbeauftragter

Der Bereichs-Sicherheitsbeauftragte ist für alle Sicherheitsbelange der Geschäftsprozesse, Anwendungen und IT-Systeme in seinem Bereich (z. B. Abteilung oder Außenstelle) verantwortlich. Je nach Größe des zu betreuenden Bereiches kann die Aufgabe des Bereichs-Sicherheitsbeauftragten von einer Person übernommen werden, die bereits mit ähnlichen Aufgaben betraut ist, z. B. dem Bereichs-Beauftragten (falls vorhanden). Auf jeden Fall ist bei der Auswahl des Bereichs-Sicherheitsbeauftragten darauf zu achten, dass er die Aufgaben, Gegebenheiten und Arbeitsabläufe in dem von ihm zu betreuenden Bereich gut kennt.

Beauftragter für IT-Sicherheit

In großen Institutionen kann es auch einen Beauftragten für die IT-Sicherheit geben, der für die Sicherheit der IT zuständig ist. Der ISB gestaltet das Informationssicherheitsmanagement und erstellt die generellen Sicherheitsziele und -vorgaben, ein Beauftragter für die IT-Sicherheit sorgt dafür, dass diese technisch umgesetzt werden. Ein Beauftragter für die IT-Sicherheit ist somit typischerweise im IT-Betrieb tätig, während der ISB unmittelbar der Leitungsebene zuarbeitet.

Projekt-Sicherheitsbeauftragter

Für große Projekte sollte ein Projekt-Sicherheitsbeauftragter benannt werden, um sowohl den Sicherheitsbedarf innerhalb des Projektes zu klären als auch die sichere Einbindung der Projektergebnisse in die Geschäftsprozesse der Institution zu ermöglichen. Der Projekt-Sicherheitsbeauftragter kann ein Mitarbeiter des Projektes oder ein Mitglied des IS-Management-Teams sein. Die Verantwortung für die Informationssicherheit liegt immer beim Projektleiter bzw. bei der Leitungsebene. Der ISB bzw. der Projekt-Sicherheitsbeauftragte unterstützt die Projektleitung in Fragen der Informationssicherheit. Dementsprechend müssen auch die erforderlichen Ressourcen für die Informationssicherheit vonseiten der Projektleitung eingeplant und bereitgestellt werden.

Die verschiedenen Geschäftsprozesse, Anwendungen und IT-Systeme einer Institution haben oft verschiedene Sicherheitsanforderungen, die unter Umständen in spezifischen Sicherheitsleitlinien zusammengefasst sind und unterschiedlicher Sicherheitsmaßnahmen bedürfen. Ähnliches trifft für den Projekt-Sicherheitsbeauftragten zu, mit dem Unterschied, dass es sich bei den Aufgaben um projektspezifische, nicht jedoch um IT-systemspezifische handelt.

Als Aufgaben der Projekt-, IT- bzw. Bereichs-Sicherheitsbeauftragten sind die folgenden festzuhalten:

- die Vorgaben des ISB umsetzen,
- die Sicherheitsmaßnahmen gemäß der IT-System-Sicherheitsleitlinie oder anderer spezifischer Sicherheitsleitlinien umsetzen,
- projekt- oder IT-systemspezifische Informationen zusammenfassen und an den ISB weiterleiten,
- als Ansprechpartner der Mitarbeiter vor Ort dienen,
- an der Auswahl der Sicherheitsmaßnahmen zur Umsetzung der spezifischen Sicherheitsleitlinien mitwirken,
- Information über Schulungs- und Sensibilisierungsbedarf von Beschäftigten ermitteln,

- Protokolldateien regelmäßig kontrollieren und auswerten sowie
- eventuell auftretende sicherheitsrelevante Zwischenfälle an den ISB melden.

Folgende Qualifikationen sollten vorhanden sein:

- detaillierte IT-Kenntnisse, da diese die Gespräche mit Mitarbeitern vor Ort erleichtern und bei der Suche nach Sicherheitsmaßnahmen für die speziellen IT-Systeme von Nutzen sind, sowie
- Kenntnisse im Projektmanagement, die bei der Organisation von Benutzerbefragungen und der Erstellung von Plänen zur Umsetzung und der Kontrolle von Sicherheitsmaßnahmen hilfreich sind.

4.7 Der ICS-Informationssicherheitsbeauftragte (ICS-ISB)

Institutionen mit industriellen Steuerungskomponenten (ICS) sollten aufgrund gesetzlicher und organisatorischer Maßnahmen einen Verantwortlichen für die Umsetzung von Anforderungen der Informationssicherheit für diesen Bereich benennen.

Industrielle Steuerungssysteme bringen zahlreiche Sicherheitsanforderungen mit sich, die sich grundlegend von denen der allgemeinen Büro-IT unterscheiden. Im ICS-Bereich werden IT-Systeme und Anwendungen oftmals über einen sehr langen Zeitraum eingesetzt. Der Lebenszyklus dieser Objekte beträgt häufig mehr als zehn Jahre.

Innerhalb von ICS-Bereichen kommen aber auch vermehrt noch Anwendungen und IT-Systeme aus dem Bereich der Büro-IT zum Einsatz. Diese werden jedoch für ihren Anwendungszweck länger als die in Büroumgebungen übliche Zeitdauer verwendet.

Um die speziellen Anforderungen im Bereich der industriellen Steuerung abzudecken und um die Sicherheitsorganisation aus dem Bereich der industriellen Steuerung in das Gesamt-ISMS einzubinden, sollte die Institution einen ICS-Informationssicherheitsbeauftragten (ICS-ISB) benennen. Dieser sollte Mitglied im IS-Management-Team sein. Außerdem sollte er im IS-Koordinierungsausschuss (siehe Kapitel 4.8 *IS-Koordinierungsausschuss*) vertreten sein. Zwar betrifft das Thema der industriellen Steuerung nicht alle Bereiche, aber aufgrund möglicher Veränderungen in der Büro-IT können Synergien für die produzierenden Bereiche ausgenutzt werden.

Je nach Größe der Institution kann es sinnvoll sein, die Aufgaben für das Gesamt-ISMS und das ISMS im ICS-Bereich auf verschiedene personelle Ressourcen aufzuteilen.

Die Sicherheitsorganisation der industriellen Steuerung sollte in die Sicherheitsorganisation der gesamten Institution eingebunden und entsprechend betrieben werden. Um Synergien zu nutzen und Fehlplanungen sowie Risiken zu vermeiden, muss eine enge Kooperation zwischen dem ICS-ISB und dem ISB stattfinden. Weitere Ansprechpartner innerhalb der Institution sind insbesondere die Mitarbeiter der Haustechnik und die IT-Experten.

Welche Struktur für eine Sicherheitsorganisation im Bereich ICS geeignet ist, hängt stark von den vorhandenen Strukturen und eingespielten Prozessen innerhalb einer Institution ab. Grundlegend muss die Kommunikation zwischen allen beteiligten Parteien sichergestellt werden. Alle Parteien müssen ein grundlegendes Verständnis für die jeweiligen Besonderheiten des anderen Bereichs aufbringen. Nur durch ein vorangegangenes Verständnis für die Kultur und Sprache der jeweiligen Bereiche können Missverständnisse vermieden werden.

Die Aufgaben des ICS-Informationssicherheitsbeauftragten sind folgendermaßen festzuhalten:

- die allgemeingültigen Sicherheitsvorgaben der Informationssicherheitsleitlinie und weiterer Richtlinien im Bereich ICS umsetzen,
- gemeinsame Ziele aus dem Bereich der industriellen Steuerung und dem Gesamt-ISMS verfolgen und Projekte aktiv unterstützen,
- für den ICS-Bereich Risikoanalysen durchführen, die den Vorgaben des Risikomanagements entsprechen,
- Sicherheitsrichtlinien und Konzepte für den ICS-Bereich unter Einbeziehung der Anforderungen aus Safety und Security erstellen und schulen,
- eng mit dem Informationssicherheitsbeauftragten kooperieren,
- als Ansprechpartner für ICS-Sicherheit für die Mitarbeiter vor Ort und in der gesamten Institution dienen,
- ICS-Sicherheitsmaßnahmen erstellen und bei der Umsetzung mitwirken,
- notwendige Dokumente zur ICS-Sicherheit erstellen und diese kommunizieren,
- Informationen über Schulungs- und Sensibilisierungsbedarf der Beschäftigten im ICS-Bereich ermitteln und Aktivitäten initiieren sowie
- Sicherheitsvorfälle im ICS-Bereich zusammen mit dem Informationssicherheitsbeauftragten bearbeiten.

Folgende Qualifikationen sollten beim ICS-ISB vorhanden sein:

- spezielle Kenntnisse zu den Prozessen innerhalb der Institution und der industriellen Steuerung,
- ausreichende IT-Kenntnisse, um Fragen der Mitarbeiter vor Ort, der IT-Experten und weiterer Parteien umfassend beantworten zu können,
- Kenntnisse zu Bedrohungen und Schwachstellen innerhalb der industriellen Steuerung,
- Kenntnisse zu Gefährdungen für die Büro-IT, die innerhalb des ICS-Bereichs eingesetzt wird,
- Kenntnisse zum Projektmanagement sowie
- Kenntnisse zu den Themen Change Management und Notfallmanagement.

4.8 IS-Koordinierungsausschuss

Der IS-Koordinierungsausschuss ist in der Regel keine Dauereinrichtung in einer Institution, sondern wird bei Bedarf (z. B. zur Planung größerer Projekte) einberufen. Er hat die Aufgabe, das Zusammenspiel zwischen dem IS-Management-Team, den Fachverantwortlichen, dem Sicherheitsbeauftragten und der Behörden- bzw. Unternehmensleitung zu koordinieren.

Ebenso wie den IS-Koordinierungsausschuss gibt es in vielen Institutionen einen IT-Koordinierungsausschuss. Auch dieser ist keine Dauereinrichtung, sondern seine Aufgabe besteht darin, das Zusammenspiel zwischen den Vertretern der IT-Anwender, dem ISB und der Behörden- bzw. Unternehmensleitung zu koordinieren.

Es bietet sich an, die beiden Koordinierungsausschüsse, insoweit dies möglich ist, zusammenarbeiten zu lassen und sie auch personell weitgehend identisch zu besetzen.

Zusammensetzung des IS-Koordinierungsausschusses

Der IS-Koordinierungsausschuss sollte die unterschiedlichen Aufgabenbereiche einer Institution widerspiegeln. Im IS-Koordinierungsausschuss sollten mindestens folgende Rollen vertreten sein: ein IT-Verantwortlicher, der Informationssicherheitsbeauftragte und Vertreter der Anwender. Da häufig auch personenbezogene Daten betroffen sind, sollte der Datenschutzbeauftragte ebenfalls Mitglied des IS-Koordinierungsausschusses sein. Wenn die Institution einen ICS-Informationssicherheitsbeauftragten hat, sollte auch dieser im IS-Koordinierungsausschuss vertreten sein. Gibt es in der Institution bereits ein ähnliches Gremium, könnten dessen Aufgaben entsprechend erweitert werden. Um die Bedeutung der Informationssicherheit zu unterstreichen, ist es jedoch ratsam, einen IS-Koordinierungsausschuss einzurichten und diesen regelmäßig einzuberufen.

4.9 Der Datenschutzbeauftragte

Der Datenschutz wird oft nachrangig behandelt, da er vermeintlich die effektive Informationsverarbeitung behindert, obwohl er in Deutschland und in vielen anderen Ländern auf gesetzlichen Vorschriften beruht und Verletzungen des damit verbundenen informationellen Selbstbestimmungsrechts empfindliche Geldbußen und Freiheitsstrafen nach sich ziehen können.

Oft werden die Aufgaben des Datenschutzbeauftragten Personen übertragen, die bereits eine andere Rolle innehaben, mit der in der neuen Funktion auch eine Interessenkollision auftreten kann, indem sie sich beispielsweise in ihrer ursprünglichen Funktion selbst kontrollieren (z. B. Leiter IT).

Um dies zu vermeiden, sollte ein kompetenter und qualifizierter Ansprechpartner für Datenschutzfragen ernannt werden, der alle Aspekte des Datenschutzes innerhalb der Institution begleitet und für eine angemessene Umsetzung und ausreichende Kontrolle sorgt. In dieser Funktion arbeitet er eng mit dem Informationssicherheitsbeauftragten zusammen, gehört zum IS-Koordinierungsausschuss, ist weisungsunabhängig und berichtet direkt der Behörden- bzw. Unternehmensleitung.

Bei angemessener Verwirklichung wird der Datenschutz Arbeitsabläufe im Ergebnis eher fördern als erschweren. Wenn nämlich eine Behörde bzw. ein Unternehmen zu viele personenbezogene Daten sammelt, personenbezogene Daten zu spät löscht oder unberechtigt übermittelt, verstößt sie nicht nur gegen Datenschutzrecht, sondern verursacht auch einen erhöhten Verwaltungsaufwand und Mehrkosten. Vor allem ist der Datenschutz ein wichtiges Element eines bürger- und kundenfreundlichen Verhaltens, weil er die Verfahrensabläufe transparent macht.

Jede Institution sollte einen Datenschutzbeauftragten ernennen. In vielen Bereichen ist die Bestellung eines Datenschutzbeauftragten sogar gesetzlich vorgeschrieben. Auch in Institutionen, die keinen Datenschutzbeauftragten benannt haben, muss die Einhaltung der datenschutzrechtlichen Anforderungen sichergestellt sein. Dies kann auch durch das IS-Management-Team oder die interne Revision erfolgen.

Anforderungsprofil

Zum Datenschutzbeauftragten kann nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Zur Aufgabenerfüllung gehören technische, organisatorische und rechtliche Kenntnisse. Als Methodik zur effektiven und vollständigen Aufgabenerfüllung empfehlen die deutschen Datenschutzaufsichtsbehörden die Anwendung des Standard-Datenschutzmodells [SDM]. Der Datenschutzbeauftragte muss die jeweiligen gesetzlichen Regelungen, bereichsspezifische datenschutzrechtliche Regelungen und die für die Institution einschlägigen Spezialvorschriften kennen und sicher anwenden können. Wichtige Rechtsnormen für den Datenschutz sind in Deutschland insbesondere das Bundesdatenschutzgesetz und die EU-Datenschutz-Grundver-

ordnung. Der Datenschutzbeauftragte sollte ferner gute Kenntnisse der Organisation und vertiefte Kenntnisse der Informationstechnik besitzen. Soweit ihm die fachliche Qualifikation in Teilbereichen noch fehlt, ist ihm Gelegenheit zu geben, sich entsprechend weiterzubilden. Mit den Aufgaben und der Arbeitsweise seiner Behörde bzw. seines Unternehmens sollte der Datenschutzbeauftragte möglichst aus eigener Erfahrung gut vertraut sein, um seinen Kontroll- und Beratungsaufgaben nachkommen zu können.

Der Datenschutzbeauftragte muss nicht ausschließlich mit diesen Funktionen betraut sein. Je nach Art und Umfang der personenbezogenen Datenverarbeitung und der damit verbundenen Datenschutzprobleme kann es angebracht sein, ihm daneben weitere Aufgaben zu übertragen. Dies wird besonders bei kleineren Institutionen in Betracht kommen. Besonders ist darauf zu achten, dass keine Interessenkonflikte oder Abhängigkeiten entstehen, die seine Aufgabenerfüllung gefährden. Möglich ist auch die Zusammenlegung der Funktionen des Datenschutzbeauftragten mit denen des Informationssicherheitsbeauftragten (zu den Rahmenbedingungen siehe auch Kapitel 4.4 *Der Informationssicherheitsbeauftragte*).

Einbeziehungspflicht

Der Datenschutzbeauftragte muss das direkte und jederzeitige Vortragsrecht bei der Behörden- bzw. Unternehmensleitung haben und über das Geschehen in der Behörde bzw. im Unternehmen, soweit es einen Bezug zu seiner Tätigkeit hat, umfassend und frühzeitig unterrichtet werden. Er ist an datenschutzrelevanten Vorgängen zu beteiligen und Planungen, die den Umgang mit personenbezogenen Daten betreffen, sind ihm bekannt zu geben. Bei Bedarf muss er von anderen Mitarbeitern mit weitergehenden rechtlichen oder technischen Kenntnissen unterstützt werden.

Zuständigkeiten und Aufgaben

Der Datenschutzbeauftragte soll dazu beitragen, dass seine Institution den Erfordernissen des Datenschutzes umfassend Rechnung trägt. Er hat die Einhaltung der Vorschriften des Datenschutzes in allen Bereichen zu überwachen. Er nimmt seine Aufgaben im Wesentlichen durch Beratung und Kontrollen wahr. Seine vorrangige Aufgabe ist die Beratung. Für die Mitarbeiter sollte der Datenschutzbeauftragte Ansprechpartner in allen Fragen des Datenschutzes sein, an den sie sich jederzeit vertrauensvoll wenden können. Bei Schwachstellen und Versäumnissen sollte er zunächst gemeinsam mit den Beteiligten nach konstruktiven Lösungen suchen.

Der Datenschutzbeauftragte hilft der Behörden- bzw. Unternehmensleitung, ihre Verantwortung für die Wahrung des Persönlichkeitsschutzes wahrzunehmen und Zwischenfälle zu vermeiden, die dem Ansehen der Institution abträglich wären. Er sollte auch Kontakt zum Personal- bzw. Betriebsrat halten. Eine gute Zusammenarbeit ist nicht nur aufgrund der Sensibilität der Personaldatenverarbeitung wünschenswert.

Der spezielle Zuschnitt der Aufgaben des Datenschutzbeauftragten richtet sich im Einzelfall nach den zu erfüllenden Aufgaben, aber auch nach der Größe, dem Aufbau und der Gliederung der jeweiligen Behörde bzw. des Unternehmens.

4.10 Zusammenspiel mit anderen Organisationseinheiten und Managementdisziplinen

In den meisten Institutionen gibt es neben dem Informationssicherheitsmanagement auch andere Bereiche, die Aufgaben im Bereich der Informationssicherheit wahrnehmen oder vergleichbare Aufgaben haben, sodass es sinnvoll ist, ein koordiniertes Vorgehen und Schnittstellen abzustimmen. Diese Bereiche sind häufig als getrennte Disziplinen und teilweise auch in anderen Organisationseinheiten organisiert. Gemeinsam ist diesen Bereichen, dass sie alle unter verschiedenen Blickwinkeln das Ziel verfolgen, Werte der Institution zu schützen. Daher führen viele dieser Bereiche bereits „Schutz" im Namen. Beispielsweise gehören hierzu neben dem Informationssicherheitsmanagement die Themenfelder Datenschutz, Objektschutz, Personenschutz, Geheimschutz, Notfallmanagement oder Risikomanagement. So kann es neben dem Informationssicherheitsbeauftragten nicht nur einen Datenschutzbeauftragten geben, sondern außerdem noch einen Geheimschutzbeauftragten, einen Notfallbeauftragten oder einen Revisor. In Institutionen mit einem Produktionsbereich ist auch die Zusammenarbeit mit den Verantwortlichen für die Produkt- und Anlagensicherheit wichtig.

Zusammenarbeit mit dem IT-Betrieb

Viele Teilaufgaben des Sicherheitsmanagements hängen unmittelbar mit Aufgaben des IT-Betriebs zusammen. Der ISB erstellt Vorgaben für den sicheren Betrieb von IT-Systemen und Netzen, der IT-Betrieb muss diese umsetzen. Daher müssen das Sicherheitsmanagement und der IT-Betrieb eng zusammenarbeiten und sich regelmäßig über Vorgehensweisen abstimmen, ebenso wie über aktuelle Gefährdungen und neu umzusetzende Sicherheitsanforderungen. In größeren Institutionen kann es daher sinnvoll sein, als Ansprechpartner des ISB im IT-Betrieb einen Beauftragten für IT-Sicherheit zu ernennen. Dieser wird häufig als IT-Sicherheitsbeauftragter, IT-Sicherheitsmanager oder auch IT-Sicherheitskoordinator bezeichnet.

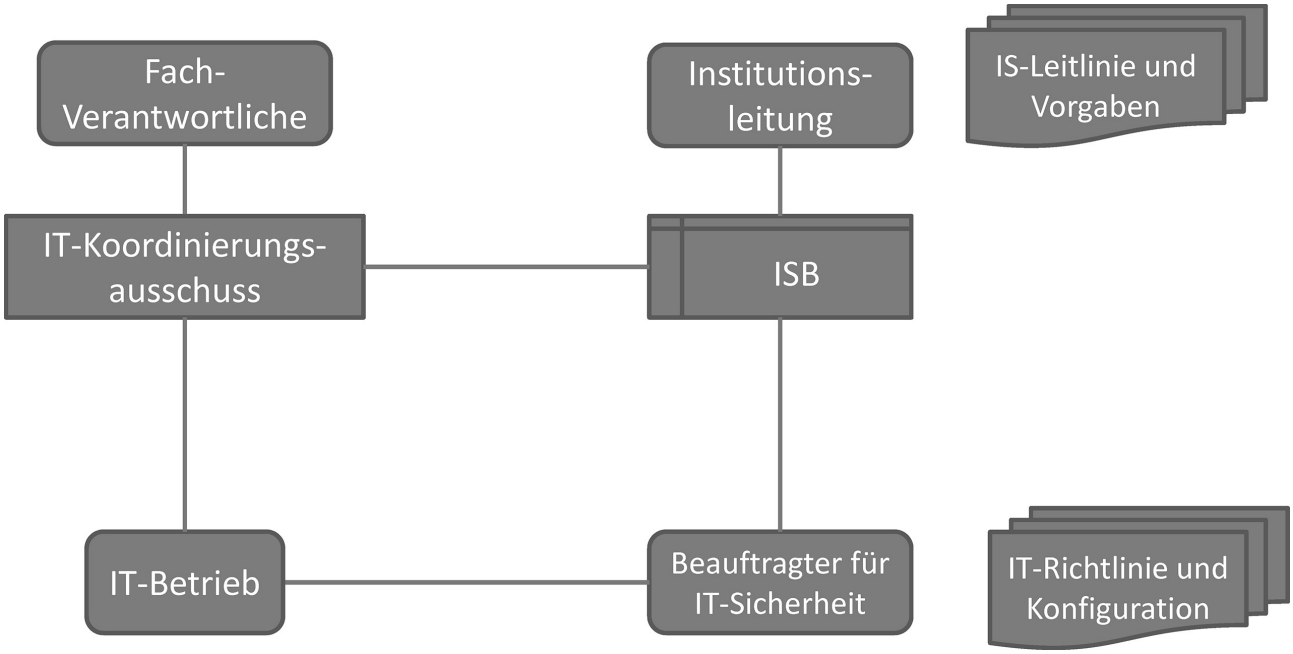


Abbildung 7: IS-Organisation und IT-Betrieb

Rollenkonflikte vermeiden

Bei der Ausgestaltung der Rollen und der Verteilung der Aufgaben ist darauf zu achten, welche Aufgaben in Personalunion wahrgenommen werden können und wo es zu Rollenkonflikten kommen könnte. Aus der Sicht des Informationssicherheitsmanagements ist zu klären, inwieweit der ISB weitere Rollen übernehmen kann, wie z. B. die des Notfallbeauftragten.

Diese Rollen schließen sich nicht grundsätzlich aus. Ausschlaggebend sind jedoch Faktoren wie die Größe und Ausrichtung der Institution, die Durchdringung der Geschäftsprozesse mit IT und die Ausprägung des Sicherheitsmanagements.

Grundsätzlich sind bei der Übernahme weiterer Aufgaben folgende Aspekte im Vorfeld zu klären:

- Die Schnittstellen zwischen den verschiedenen Rollen sollten klar definiert und dokumentiert werden.
- Beim Eintreten konfliktträchtiger Themen sollte eine Instanz benannt sein, die diese klären kann, z. B. die Innenrevision.
- Es muss sichergestellt werden, dass Personen mit mehreren Rollen ausreichend qualifiziert sind und genügend Ressourcen für ihre Aufgaben zur Verfügung haben.

Es gibt aber auch Rollen, die sich nicht ohne Weiteres mit den Aufgaben des Informationssicherheitsmanagements kombinieren lassen. Dazu können z. B. Rollen wie jene des Revisors oder Auditors gehören, auch das hängt aber immer vom konkreten Aufgabenumfeld ab. Grundsätzlich besteht bei einer kontrollierenden Tätigkeit immer das Problem, dass die Kontrollierenden nichts überprüfen sollten, was sie selbst konzeptioniert haben.

4.11 Einbindung externer Sicherheitsexperten

Unter Umständen kann es erforderlich sein, externe Sicherheitsexperten in der internen Sicherheitsorganisation einzusetzen. Wenn wesentliche Rollen wie der ISB nicht durch interne Mitarbeiter wahrgenommen werden können, müssen hierfür qualifizierte Externe beauftragt werden. Die notwendigen Qualifikationen sind in den vorhergehenden Abschnitten dieses Kapitels beschrieben.

Insbesondere in kleinen Unternehmen oder Behörden kann es unter Umständen zweckmäßig sein, die Rolle des Informationssicherheitsbeauftragten nicht durch einen eigenen Mitarbeiter zu besetzen, sondern hierfür auf die Dienstleistung eines externen ISB zurückzugreifen.

In der Praxis fehlt den internen Sicherheitsexperten häufig die Zeit, um alle sicherheitsrelevanten Einflussfaktoren und Rahmenbedingungen (z. B. gesetzliche Anforderungen oder technische Fragen) zu analysieren. Teilweise fehlen ihnen auch die entsprechenden Grundlagen. Auch in diesen Fällen ist es sinnvoll, auf externe Experten zurückzugreifen. Dies muss von den internen Sicherheitsexperten dokumentiert werden, damit die Leitungsebene die erforderlichen Ressourcen bereitstellt.

Aktionspunkte zu 4 Organisation des Sicherheitsprozesses
• Rollen für die Gestaltung des Informationssicherheitsprozesses festlegen • Aufgaben und Verantwortungsbereiche den Rollen zuordnen • Personelle Ausstattung der Rollen festlegen • IS-Organisation dokumentieren • Informationssicherheitsmanagement in die organisationsweiten Abläufe und Prozesse integrieren • Wenn erforderlich, externe Experten hinzuziehen

5 Dokumentation im Sicherheitsprozess

Vor und während des Sicherheitsprozesses wird eine Vielzahl verschiedener Dokumente und Beschreibungen erstellt. Hierbei sollte immer darauf geachtet werden, dass der Aufwand für die Erstellung von Dokumentationen in einem angemessenen Rahmen bleibt. Die Dokumentation des Sicherheitsprozesses sollte so aussagekräftig sein, dass auch später noch nachvollziehbar ist, was zu früheren Zeitpunkten entschieden und umgesetzt wurde.

Dieses Kapitel beschreibt idealtypische Anforderungen und Methoden bei der Dokumentation des Sicherheitsprozesses. Abhängig von der gewählten IT-Grundschutz-Vorgehensweise und den vorhandenen Rahmenbedingungen kann und sollte der Dokumentationsprozess angepasst werden. Insbesondere bei der Basis-Absicherung sollte der Dokumentationsprozess möglichst einfach und zweckmäßig gehalten werden.

Wenn eine spätere Zertifizierung des ISMS angestrebt ist, müssen einige Dokumente zwingend erstellt werden (siehe Kapitel 11 *Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz*). Davon abgesehen, sollte der Dokumentationsaufwand möglichst minimiert werden. Wenn es im IT-Grundschutz heißt, dass etwas dokumentiert werden muss, ist es hierfür meistens nicht erforderlich, eigenständige Dokumente zu erstellen. Im Allgemeinen reicht es, die notwendigen Informationen an geeigneter Stelle zu notieren, beispielsweise in einem Wiki, in vorhandenen Texten oder Tabellen.

5.1 Klassifikation von Informationen

Um Informationen angemessen schützen zu können, muss deren Bedeutung für die Institution klar sein. Um sich innerhalb einer Institution, aber auch mit anderen Institutionen einfacher darüber austauschen zu können, welchen Wert bestimmte Arten von Informationen haben, wird ein Klassifikationsschema benötigt, in dem beschrieben ist, welche Abstufungen der Wertigkeit es gibt und wie die verschiedenen Stufen gegeneinander abgegrenzt sind.

Eine sinnvolle Vorgehensweise ist es daher, ein Klassifikationsschema zu erarbeiten, das es allen Mitarbeitern ermöglicht, daraus für jede Art der Information die korrekte Einstufung abzuleiten, ohne dass diese dafür explizit gekennzeichnet werden muss. Das Klassifikationsschema sollte nicht zu kompliziert gewählt sein, sodass es einfach verständlich und leicht anwendbar ist.

Es bietet es sich an, von den Grundwerten der Informationssicherheit auszugehen und Informationen in Bezug auf ihre Vertraulichkeit, Integrität und Verfügbarkeit zu klassifizieren. Je nach Institution können hier auch weitere oder andere Parameter verwendet werden, beispielsweise wenn diese in der Institution bereits in anderen Zusammenhängen verwendet wurden. Ein Nachteil davon, das Klassifikationsschema zu erweitern, ist, dass die Klassifizierung komplexer wird. Damit wird es für die Mitarbeiter schwieriger, die Abgrenzung zwischen den einzelnen Stufen nachzuvollziehen und das Schema anzuwenden. Ein weiterer Nachteil ist, dass es somit schwieriger wird, ein gemeinsames Verständnis über die Klassifizierung von Informationen mit anderen Institutionen aufzubauen.

Um die Vertraulichkeit zu klassifizieren, wird häufig zwischen *offen*, *intern*, *vertraulich* und *streng vertraulich* abgestuft. Bei der Verfügbarkeit kann beispielsweise eine Klassifikation über die zu erwartende bzw. die tolerierbare Dauer bis zur Wiederherstellung bei einem Ausfall getroffen werden, etwa *eine Stunde*, *ein Tag*, *eine Woche*, *ein Monat*. Schwieriger ist es, die Integrität zu klassifizieren, etwa in *essenziell*, *wichtig* und *normal*. Kriterien können hierfür beispielsweise die möglichen Auswirkungen bei Integritätsverlust und deren Schweregrad sein oder der betriebene Aufwand zur Sicherstellung der Integrität.

In einfachen Fällen, etwa auch im Kontext der Basis-Absicherung, kann anfangs bereits eine zweistufige Klassifizierung ausreichend sein, indem beispielsweise nur zwischen internen („alles im Intranet") und öffentlichen Informationen unterschieden wird. In diesem Fall empfiehlt es sich, die für die Veröffentlichung vorgesehenen Informationen, aber auch nur diese, als solche zu klassifizieren („offen").

Diese Klassifikation ist eine wesentliche Voraussetzung, um später adäquate Sicherheitsmaßnahmen auszuwählen und anzuwenden.

Kennzeichnung: Es ist erstrebenswert, alle Informationen bereits bei ihrer Generierung zu kennzeichnen, um diese konsequent während ihres gesamten Lebenszyklus angemessen schützen zu können. Dies ist aber erfahrungsgemäß schwierig. Die Erfahrung hat gezeigt, dass ein Klassifikationsschema einfach aufzubauen ist, aber es sich als schwierig herausstellt, dieses im laufenden Betrieb am Leben zu erhalten, sodass es von allen Mitarbeitern konsequent und einheitlich angewendet wird. Außerdem ist zu berücksichtigen, dass sich die Klassifikation im Lebenszyklus der Informationen ändern kann.

Ein positiver Nebeneffekt der Klassifizierung von Daten ist, dass dabei auffällt, welche Daten überflüssig oder veraltet sind bzw. nicht genutzt werden. Eine konsequente Klassifikation hilft demnach, den Datenmüll zu reduzieren.

Um einen funktionierenden Prozess zur Klassifikation von Informationen aufzubauen und zu betreiben, sollten dafür geeignete Rollen eingerichtet und deren Aufgaben festgelegt werden.

Die nachfolgende Tabelle zeigt ein umfangreiches Beispiel zu möglichen Rollen, um notwendige Aufgaben zu verdeutlichen. Auch hier können in der Praxis geeignete Anpassungen vorgenommen werden. Es sollte immer mindestens die Rolle eines Verantwortlichen für den Klassifikationsprozess geben sowie die Rollen derjenigen, die diesen Prozess einhalten bzw. umsetzen.

Rolle	**deutsche Rollenbezeichnung**	**Wer kann die Rolle übernehmen?**	**Aufgaben**
Data Creator	Ersteller	jeder Mitarbeiter	• erzeugt Daten • Erst-Klassifikation
Data Owner	Fachverantwortlicher	Fachverantwortlicher/ Linienvorgesetzer	• konkretisiert Regelungen zur Klassifikation in seinem Bereich • klärt Einstufungsfragen mit Erstellern • überwacht Klassifikationsprozess seitens der Ersteller
Data User	Benutzer	jeder Mitarbeiter	• benutzt Daten • beachtet Regeln zur Klassifikation • gibt Feedback zu Einstufungshöhen

Rolle	deutsche Rollenbezeichnung	Wer kann die Rolle übernehmen?	Aufgaben
Data Auditor	Klassifikationsverantwortlicher	Anforderungsmanager/Compliance Manager	• erstellt institutionsweite Klassifikationsstrategie und -vorgaben • stellt Hilfsmittel und Erläuterungen zur Verfügung • klärt Einstufungsfragen mit Fachverantwortlichen und Benutzern • überwacht Klassifikationsprozess seitens der Fachverantwortlichen • stimmt sich ab mit Risikomanagement, ISB, Datenschutzbeauftragter

Tabelle 1: Aufgaben und Prozesse bei der Klassifizierung von Daten

Ein typisches Beispiel für ein Klassifikationsschema ist die im staatlichen Geheimschutz benutzte Einteilung in:

- VS – NUR FÜR DEN DIENSTGEBRAUCH
- VS – VERTRAULICH
- GEHEIM
- STRENG GEHEIM

Dieses Schema bezieht sich allerdings auf den kleinen Bereich der Verschlusssachen (VS), also der im öffentlichen Interesse geheimhaltungsbedürftigen Informationen oder Gegenstände. Es lässt daher große Lücken bei der Vielzahl an Informationen, die typischerweise in einem Unternehmen oder in einer Behörde anfallen, die aber ebenfalls geschützt werden müssen. In Institutionen, in denen Verschlusssachen nur einen geringen Anteil der verarbeiteten Daten darstellen, ist es daher sinnvoll, für den großen Anteil der geschäftsrelevanten und teilweise geschäftskritischen Informationen ein eigenes Klassifikationsschema zu entwickeln.

Aktionspunkte zu 5.1 Klassifikation von Informationen
• Klassifikationsschema erstellen, das eine korrekte, unkomplizierte und nachvollziehbare Einstufung von Informationen ermöglicht

5.2 Informationsfluss im Informationssicherheitsprozess

In den verschiedenen Schritten des Informationssicherheitsprozesses entsteht eine Vielzahl an unterschiedlichen Berichten, Konzepten, Richtlinien, Meldungen über sicherheitsrelevante Ereignisse und an weiteren Dokumenten zur Informationssicherheit der Institution. Die Dokumente müssen aussagekräftig und für die jeweilige Zielgruppe verständlich sein. Da nicht alle diese Informationen für die Leitungsebene geeignet sind, ist es eine Aufgabe des ISB, diese Informationen zu sammeln, zu verarbeiten und entsprechend kurz und übersichtlich aufzubereiten.

Dieses Kapitel beschreibt umfassend die wesentlichen Aspekte bezüglich einer angemessenen Dokumentation sowie eines angemessenen Informationsflusses. Die Berücksichtigung dieser Aspekte unterstützt bei der Erstellung einer guten Dokumentation. Sie sind bewährt und empfehlenswert und müssen den Gegebenheiten der Institution angepasst werden. Dies gilt insbesondere im Kontext der Basis-Absicherung. Im Rahmen einer Zertifizierung werden sie verbindlich, ansonsten sind sie als „Best Practices" zu verstehen.

5.2.1 Berichte an die Leitungsebene

Damit die Unternehmens- bzw. Behördenleitung die richtigen Entscheidungen bei der Steuerung und Lenkung des Informationssicherheitsprozesses treffen kann, benötigt sie Eckdaten zum Stand der Informationssicherheit. Diese Eckpunkte sollten in Managementberichten aufbereitet werden, die unter anderem folgende Punkte abdecken:

- Status und Umsetzungsgrad des Sicherheitskonzepts
- Ergebnisse von Audits und Datenschutzkontrollen (siehe auch Datenschutz-Grundverordnung [DSGVO])
- Berichte über Sicherheitsvorfälle
- Berichte über bisherige Erfolge und Probleme beim Informationssicherheitsprozess
- Berichte über die Reduzierung bestehender Umsetzungsdefizite und der damit verbundenen Risiken (Risikobehandlungsplan, siehe BSI-Standard 200-3)

Die Leitungsebene muss vom ISB regelmäßig in angemessener Form über die Ergebnisse der Überprüfungen und den Status des Sicherheitsprozesses informiert werden. Dabei sollten Erfolge, Probleme und Verbesserungsmöglichkeiten aufgezeigt werden. Die Leitungsebene nimmt die Managementberichte zur Kenntnis und veranlasst eventuell notwendige Maßnahmen.

Ebenso erarbeitet der Sicherheitsbeauftragte das Sicherheitskonzept und sorgt für dessen Umsetzung und regelmäßige Aktualisierung. Die Freigabe des Sicherheitskonzepts erfolgt durch die Leitungsebene.

5.2.2 Dokumentation im Informationssicherheitsprozess

Aus zahlreichen Gründen ist die Dokumentation des IS-Prozesses auf allen Ebenen entscheidend für dessen Erfolg. Nur durch eine ausreichende Dokumentation

- werden getroffene Entscheidungen nachvollziehbar,
- sind Prozesse wiederholbar und standardisierbar,
- können Schwächen und Fehler erkannt und zukünftig vermieden werden.

Abhängig vom Gegenstand und vom Verwendungszweck einer Dokumentation können folgende Arten von Dokumentationen unterschieden werden:

Dokumente für das Sicherheitsmanagement (Zielgruppe: Sicherheitsmanagement)

Im Rahmen der verschiedenen Aktivitäten des Informationssicherheitsmanagements entstehen Konzepte, Richtlinien, Berichte und weitere Dokumente. Nur durch eine ausreichende Dokumentation werden getroffene Entscheidungen nachvollziehbar, Handlungen wiederholbar und Schwächen erkannt, sodass diese in Zukunft vermieden werden können.

Die Menge und Ausprägung der Dokumentation hängt von den Notwendigkeiten der jeweiligen Institutionen ab und kann sehr unterschiedlich sein. Beispiele für zu erstellende Dokumente sind:

- Sicherheitskonzept mit den Berichten zur Risikoanalyse,
- Schulungs- und Sensibilisierungskonzept,
- Audit- oder Revisionsberichte.

Technische Dokumentation und Dokumentation von Arbeitsabläufen (Zielgruppe: Experten)

Hier wird der aktuelle Stand von Geschäftsprozessen und der damit verbundenen IT-Systeme und Anwendungen beschrieben. Oft ist der Detaillierungsgrad technischer Dokumentationen ein Streitthema. Ein pragmatischer Ansatz ist, dass andere Personen mit vergleichbarer Expertise in diesem Bereich die Dokumentation nachvollziehen können müssen und dass der Administrator zwar auf sein Wissen, aber nicht auf sein Gedächtnis angewiesen sein muss, um die Systeme und Anwendungen wiederherzustellen. Bei Sicherheitsübungen und bei der Behandlung von Sicherheitsvorfällen sollte die Qualität der vorhandenen Dokumentationen bewertet und die gewonnenen Erkenntnisse zur Verbesserung genutzt werden. Zu solcher Art von Dokumentationen gehören unter anderem:

- Installations- und Konfigurationsanleitungen,
- Anleitungen für den Wiederanlauf nach einem Sicherheitsvorfall,
- Dokumentation von Test- und Freigabeverfahren,
- Anweisungen für das Verhalten bei Störungen und Sicherheitsvorfällen.

Anleitungen für Mitarbeiter (Zielgruppe: Mitarbeiter)

Das Dokument, das die grundlegenden Aussagen zum Umgang mit Informationssicherheit in der Institution enthält, ist die Leitlinie zur Informationssicherheit.

Daneben müssen die umzusetzenden Sicherheitsmaßnahmen für die Mitarbeiter verständlich in Form von Richtlinien dokumentiert werden. Die Mitarbeiter müssen über die Existenz und Bedeutung dieser Richtlinien informiert und entsprechend geschult sein. Diese Gruppe von Dokumentationen umfasst beispielsweise:

- Arbeitsabläufe und organisatorische Vorgaben,
- Richtlinien zur Nutzung des Internets,
- Verhalten bei Sicherheitsvorfällen.

Aufzeichnung von Managemententscheidungen (Zielgruppe: Leitungsebene)

Grundlegende Entscheidungen zum Informationssicherheitsprozess und zur Sicherheitsstrategie müssen aufgezeichnet werden, damit diese jederzeit nachvollziehbar und wiederholbar sind.

Gesetze und Regelungen (Zielgruppe: Leitungsebene)

Für die Informationsverarbeitung können eine Vielzahl unterschiedlicher Gesetze, Regelungen und Anweisungen relevant sein. Es sollte dokumentiert werden, welche Gesetze, Regelungen und Anweisungen im vorliegenden Fall besondere Anforderungen an Geschäftsprozesse, den IT-Betrieb oder an die Informationssicherheit stellen und welche konkreten Konsequenzen sich daraus ergeben.

Referenzdokumente für die Zertifizierung (Zielgruppe: Institutionen mit dem Ziel der Zertifizierung)

Strebt eine Institution eine Zertifizierung an, so müssen verschiedene Dokumente für die Auditierung erstellt und aktualisiert werden. Diese Dokumente werden den Auditoren und der Zertifizierungsstelle im BSI überreicht, bewertet und darauf aufbauend die Entscheidung für oder gegen ein Zertifikat getroffen. Die erforderlichen Dokumente für die Zertifizierung werden im Internet in der Liste der Referenzdokumente gepflegt. Dazu gehören beispielsweise Richtlinien zur Risikoanalyse, zur Lenkung von Dokumenten und Aufzeichnungen, zur Auditierung des Managementsystems für Informationssicherheit und zur Lenkung von Korrektur- und Vorbeugungsmaßnahmen.

Dokumentation im ICS-Bereich (Zielgruppe: Anwender)

Viele der Dokumente zur Informationssicherheit aus dem IT-Bereich können für den Bereich der industriellen Steuerung übernommen werden. Einige der Dokumente aus dem IT-Bereich lassen sich jedoch nicht ohne Weiteres für den Bereich der industriellen Steuerung übertragen. Hier müssen entsprechend der Anforderungen Dokumente für den ICS-Bereich neu erstellt, modifiziert oder geändert werden. Häufig ist es sinnvoll, für den Bereich der industriellen Steuerung eine abgeleitete Leitlinie für die Informationssicherheit und eigene Richtlinien und Arbeitsanweisungen zu erstellen. Zu beachten ist, dass alle abgeleiteten Dokumente in das ISMS der Institution integriert werden sollten.

Es muss sichergestellt werden, dass alle Dokumentationen auf dem aktuellen Stand gehalten werden. Dafür muss die Dokumentation in den Änderungsprozess einbezogen werden.

5.2.3 Anforderungen an die Dokumentation

Eine angemessene Dokumentation des Informationssicherheitsprozesses sollte eine Reihe von Anforderungen bezüglich Kennzeichnung, Detailtiefe, Aktualisierungen, Medium, Sicherheit und Datenschutz erfüllen. Diese werden nachfolgend detailliert beschrieben.

Mindestanforderung an die Kennzeichnung der Dokumente zum Sicherheitsmanagement

Die Dokumente, die im Rahmen des Sicherheitsmanagements erstellt, bearbeitet und verwaltet werden, müssen aussagekräftig und für die jeweilige Zielgruppe verständlich sein. Es sollte, soweit sinnvoll, ein einheitlicher Aufbau der Dokumente genutzt werden. Dies dient dem besseren Verständnis und der einfacheren Handhabung. Die Dokumente müssen so gekennzeichnet sein, dass sie im Bedarfsfall schnell gefunden und zugeordnet werden können. Daher müssen mindestens folgende Angaben vorhanden sein:

- Eindeutige Bezeichnung (aussagekräftiger Titel),
- Ersteller / Autor / Dokumenteninhaber,
- Funktion des Erstellers,
- Versionsnummer,
- letzte Überarbeitung, nächste geplante Überarbeitung,
- freigegeben am / durch,
- Klassifizierung (vertrauliche Inhalte müssen klassifiziert, als solche gekennzeichnet und die Dokumente sicher verwahrt werden) und
- berechtigte Rollen (Verteilerkreis).

Optional können folgende Informationen mit aufgenommen werden:

- Quellenangaben,
- Aufbewahrungszeitraum und
- eine Änderungsübersicht.

Externe Dokumente, die für das Sicherheitsmanagement relevant sind, müssen ebenfalls angemessen gekennzeichnet und verwaltet werden.

Detailtiefe

Für die Detailtiefe der einzelnen Dokumente gilt das Prinzip „dem Ziel und Zweck angemessen". Strategiedokumente, wie die Leitlinie, sollten kurz und prägnant, jedoch aussagekräftig gehalten werden. Die bei der Konzeption anfallenden Dokumente sollten detaillierte Informationen enthalten, um die daraus abgeleiteten Entscheidungen nachvollziehen zu können. Alle Entscheidungen sowie die Informationen, auf denen die Entscheidungen basieren, müssen dokumentiert werden.

Für Richtlinien und Handlungsanweisungen für Mitarbeiter gilt in besonderem Maße, dass sie klar und verständlich gehalten werden müssen. Oftmals sind für bestimmte Bereiche einfache Checklisten ausreichend. Diese ermöglichen einen schnellen Überblick und helfen dabei, nichts zu vergessen und die Reihenfolge einzelner Schritte einzuhalten.

Änderungsmanagement

Alle Dokumente zum Sicherheitsmanagement sollen regelmäßig aktualisiert werden. Dafür empfiehlt es sich, ein Änderungsmanagement-Verfahren aufzusetzen, mit dem alle Änderungen erfasst, bewertet, freigegeben und nachvollzogen werden können. Dazu sind für alle Dokumente klare schriftliche Änderungsmanagement-Anweisungen vorzugeben. Das Verfahren sollte des Weiteren festlegen, wie Anwender Änderungsvorschläge einbringen können und wie diese dann beurteilt und gegebenenfalls berücksichtigt werden. Das Änderungsmanagement des Sicherheitsmanagements ist in das übergreifende Änderungsmanagement der Institution zu integrieren.

Für die Aktualisierung der einzelnen Dokumente sollten Intervalle vorgegeben werden. Für den überwiegenden Teil der Dokumente hat sich eine jährliche Überprüfung bewährt.

Die Mechanismen, die das Änderungsmanagement anstoßen, sind in die entsprechenden Prozesse (z. B. Personalverwaltung, Hausverwaltung, Inventarisierung) zu integrieren. Der Sicherheitsbeauftragte ist steuernd tätig. Die Verantwortung für die Aktualisierungen und Durchführung der Änderungsanforderungen für ein einzelnes Dokument trägt der jeweilige Dokumenteneigentümer.

Dokumentationsmedium

Dokumente zum Sicherheitsmanagement müssen nicht immer in Papierform vorliegen. Zur Dokumentation können auch lokale oder internetbasierte Software Tools genutzt werden. Diese speichern alle nötigen Informationen und sind von verschiedenen Standorten aus sowie kollaborativ nutzbar.

Das Dokumentationsmedium sollte je nach Bedarf, Phase (Planung, Umsetzung oder Prüfung) oder Teilaufgabe gewählt werden. Auch die Zielpersonen der Dokumente und deren Vertrautheit mit den unterschiedlichen Medien sollte in die Überlegung eingeschlossen werden. Während die einen die Arbeit mit Papier bevorzugen, ist für die anderen das einfache Suchen oder Filtern in elektronischen Dokumenten unverzichtbar.

Sicherheit und Datenschutz

Da die Dokumente zum Sicherheitsmanagement sowohl sensitive Daten über die Institution als auch personenbezogene Daten beinhalten, muss die Informationssicherheit und der Datenschutz gewährleistet werden. Neben der Verfügbarkeit sind auch die Integrität und insbesondere die Vertraulichkeit der Dokumente zu garantieren. Die verschiedenen Dokumente des Sicherheitsmanagements sollten in Bezug auf ihre Vertraulichkeit eingestuft, entsprechend gekennzeichnet und durch geeignete Maßnahmen geschützt werden.

Die jeweils berechtigten Empfänger sollten in den Dokumenten genannt werden. Der Zugriff auf die Dokumente ist auf die Personen zu beschränken, die die enthaltenen Informationen für ihre Tätigkeit benötigen („Need-to-know-Prinzip"). Eine sinnvolle Modularisierung der Dokumente ist daher empfehlenswert. Diese ermöglicht eine auf die Empfänger ausgerichtete Verteilung der Informationen. Es sollte in der Institution einen Überblick über die Anzahl der klassifizierten Dokumente, deren Art (z. B. Papier oder DVD) und deren Verteilung geben, wie auch über deren korrekte und vollständige Aktualisierung und Vernichtung bzw. Rücknahme.

5.2.4 Informationsfluss und Meldewege

Über die verschiedenen Aktivitäten im Rahmen des Sicherheitsmanagements müssen alle Betroffenen zeitnah informiert werden. Allerdings ist es auch nicht sinnvoll, Detailinformationen über den Sicherheitsprozess beliebig zu streuen. Daher muss geklärt sein, welche Personen mit welchen internen und externen Stellen wann über welche Details des Sicherheitsprozesses kommunizieren. Zudem muss festgelegt werden, welche Kommunikationskanäle für die jeweiligen Ansprechpartner genutzt und wie diese geschützt werden.

Für die Aufrechterhaltung des Informationssicherheitsprozesses ist die zeitnahe Aktualisierung der Meldewege und der Festlegungen für den Informationsfluss von elementarer Bedeutung. Darüber hinaus bieten die Ergebnisse aus durchgeführten Übungen, Tests und Audits auch eine nützliche Grundlage für die Verbesserung des Informationsflusses.

Grundsätzliche Festlegungen zum Informationsfluss und zu den Meldewegen in Bezug auf den Informationssicherheitsprozess sollten in einer entsprechenden Richtlinie dokumentiert und von der Leitungsebene verabschiedet werden. In der *Richtlinie zum Informationsfluss und zu den Meldewegen* sollten insbesondere die für den Informationssicherheitsprozess kritischen Informationsflüsse geregelt werden. Dabei ist zwischen Hol- und Bringschuld zu unterscheiden.

Nutzung von Synergieeffekten für den Informationsfluss

Viele Institutionen haben bereits Prozesse für die Bereitstellung von Dienstleistungen oder den IT-Betrieb definiert. Häufig gelingt es, Synergieeffekte zu nutzen und Aspekte der Informationssicherheit in bereits bestehende Prozesse einzugliedern. Beispielsweise könnten Meldewege für IT-Sicherheitsvorfälle in den IT-Betrieb integriert werden oder die Kapazitätsplanung um Aspekte der Notfallvorsorge erweitert werden.

Viele Informationen, die aus Sicherheitsgründen erhoben werden, können auch zu anderen Zwecken genutzt werden. Ebenso haben Sicherheitsmaßnahmen auch andere positive Nebeneffekte, besonders die Optimierung von Prozessen zahlt sich aus. Beispielsweise sind die Bestimmung von Informationseigentümern oder die Einstufung von Informationen nach einheitlichen Bewertungskriterien für viele Bereiche einer Institution relevant. Ein Überblick über die Abhängigkeit der Geschäftsprozesse von IT- bzw. ICS-Systemen und Anwendungen ist ebenfalls nicht nur für das Sicherheitsmanagement

sinnvoll. Zum Beispiel kann dadurch häufig auch eine exakte Zuordnung von IT-Kosten, die oftmals als Gemeinkosten umgelegt werden, auf einzelne Geschäftsprozesse oder Produkte erfolgen.

Aktionspunkte zu 5.2 Informationsfluss im Informationssicherheitsprozess

- Grundsätzliche Festlegungen zum Informationsfluss und zu den Meldewegen in Bezug auf den Informationssicherheitsprozess in einer entsprechenden Richtlinie dokumentieren und der Leitungsebene zur Verabschiedung vorlegen
- Leitungsebene über die Ergebnisse von Überprüfungen und den Status des Informationssicherheitsprozesses informieren
- Gegebenenfalls Entscheidungen über erforderliche Korrekturmaßnahmen einholen
- Alle Teilaspekte des gesamten Informationssicherheitsprozesses nachvollziehbar dokumentieren und die Dokumentation auf dem aktuellen Stand halten
- Bei Bedarf die Qualität der Dokumentation bewerten und gegebenenfalls nachbessern oder aktualisieren
- Meldewege, die den Informationssicherheitsprozess betreffen, auf dem aktuellen Stand halten
- Synergien zwischen dem Informationssicherheitsprozess und anderen Managementprozessen ausfindig machen

6 Erstellung einer Sicherheitskonzeption nach der Vorgehensweise Basis-Absicherung

Die Erstellung der Sicherheitskonzeption für die Institution erfolgt nach der Vorgehensweise Basis-Absicherung, wenn die folgenden Voraussetzungen erfüllt sind:

- ein Informationssicherheitsprozess wurde initiiert,
- die Sicherheitsleitlinie und Informationssicherheitsorganisation wurden definiert,
- eine Übersicht der vorhandenen Assets der Institution wurde erstellt,
- die Basis-Absicherung wurde als IT-Grundschutz-Vorgehensweise ausgewählt.

Im Hinblick auf die Sicherheitskonzeption sollten für die Komponenten von Geschäftsprozessen, Anwendungen und IT-Systemen organisatorische, personelle, infrastrukturelle und technische Anforderungen aus dem IT-Grundschutz-Kompendium erfüllt werden. Diese sind in Bausteine strukturiert, sodass sie modular aufeinander aufsetzen.

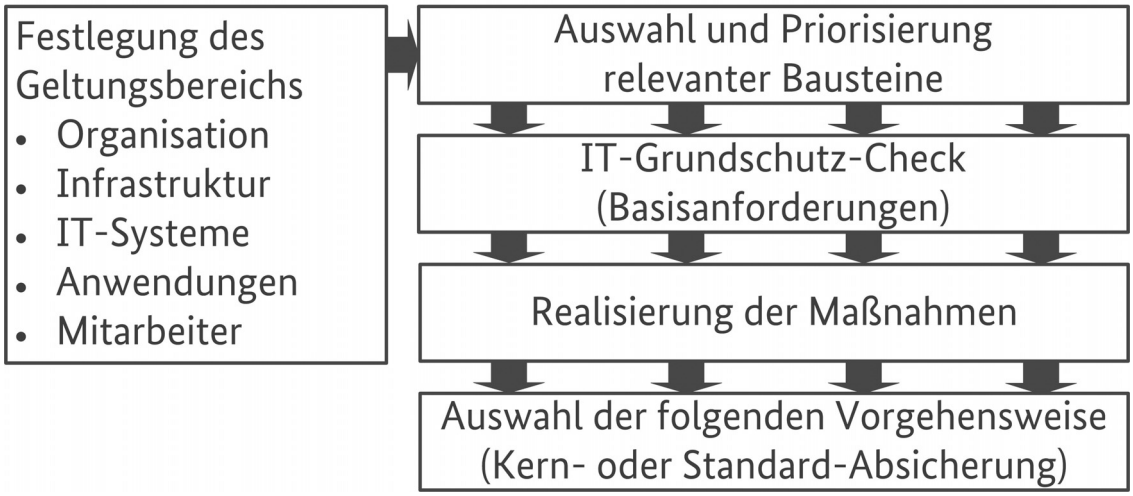


Abbildung 8: Basis-Absicherung

Die Erstellung einer Sicherheitskonzeption nach Basis-Absicherung gliedert sich in folgende Aktionsfelder, die anschließend noch näher vorgestellt werden sollen:

- Festlegung des Geltungsbereichs:
  Es muss der Informationsverbund festgelegt werden, für den die Sicherheitskonzeption erstellt und umgesetzt werden soll.
- Auswahl und Priorisierung:
  Der betrachtete Informationsverbund muss mithilfe der vorhandenen Bausteine aus dem IT-Grundschutz-Kompendium nachgebildet werden.
- IT-Grundschutz-Check:
  In diesem Schritt wird überprüft, ob die Basis-Anforderungen nach dem IT-Grundschutz bereits ganz oder teilweise umgesetzt sind und welche Sicherheitsmaßnahmen noch fehlen.
- Realisierung:
  Für die bisher nicht erfüllten Basis-Anforderungen müssen geeignete Sicherheitsmaßnahmen festgelegt und umgesetzt werden.

- Auswahl der folgenden Vorgehensweise:
  Die Basis-Absicherung dient als Einstiegsvorgehensweise. Es muss daher festgelegt werden, zu welchem Zeitpunkt und mit welcher IT-Grundschutz-Vorgehensweise das Sicherheitsniveau angehoben werden soll.

Im Unterschied zur Standard-Absicherung sind die Aktionsfelder bei der Basis-Absicherung kein geschlossener Zyklus, sondern eine Einstiegsvorgehensweise, die mit der Standard-Absicherung fortgeführt werden kann (eventuell mit der Kern-Absicherung als Zwischenschritt).

6.1 Festlegung des Geltungsbereichs für die Basis-Absicherung

Bei der Erstellung einer Sicherheitskonzeption muss als Erstes festgelegt werden, welchen Bereich der Institution sie abdecken soll (Geltungsbereich).

Der Geltungsbereich kann die gesamte Institution umfassen oder auch nur einzelne Bereiche. Auf jeden Fall muss der Geltungsbereich klar abgegrenzt und sinnvoll in sich abgeschlossen sein, mit wenigen, eindeutig definierten Schnittstellen. So könnte eine Institution beispielsweise für eine neu hinzugekommene Abteilung mit ihren Geschäftsprozessen und Assets zunächst die Basis-Absicherung umsetzen. Vertiefende Informationen zur Abgrenzung des Geltungsbereichs sind im Kapitel 3.4.3 *Festlegung des Geltungsbereichs und Inhalt der Sicherheitsleitlinie* zu finden.

Informationsverbund

Der Geltungsbereich für die Erstellung der Sicherheitskonzeption wird im Folgenden „Informationsverbund" genannt. Ein Informationsverbund umfasst die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei als Ausprägung die gesamte Informationsverarbeitung einer Institution oder auch einzelne Bereiche umfassen, die nach organisatorischen oder technischen Strukturen (z. B. Abteilungsnetz) oder gemeinsamen Geschäftsprozessen bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind. Für die Erstellung der Sicherheitskonzeption werden auf Grundlage der bereits während der Vorarbeiten erfolgten Ersterfassung (siehe Kapitel 3.2.4 *Ersterfassung der Prozesse, Anwendungen und IT-Systeme*) die relevanten Bestandteile des betrachteten Informationsverbunds identifiziert.

6.2 Auswahl und Priorisierung für die Basis-Absicherung

Der nächste Schritt besteht darin, den betrachteten Informationsverbund mithilfe der in der Ersterfassung identifizierten Prozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen und Räume und den vorhandenen Bausteinen aus dem IT-Grundschutz-Kompendium nachzubilden. Das Ergebnis ist ein IT-Grundschutz-Modell des Informationsverbunds, das aus verschiedenen, gegebenenfalls auch mehrfach verwendeten Bausteinen besteht und durch die Verwendung der Bausteine die sicherheitsrelevanten Aspekte des Informationsverbunds beinhaltet.

6.2.1 Modellierung nach IT-Grundschutz

Um einen im Allgemeinen komplexen Informationsverbund nach IT-Grundschutz zu modellieren, müssen die passenden Bausteine des IT-Grundschutz-Kompendiums ausgewählt und umgesetzt werden. Um die Auswahl zu erleichtern, sind die Bausteine im IT-Grundschutz-Kompendium zunächst in prozess- und systemorientierte Bausteine aufgeteilt. Ein Überblick über die Struktur des IT-Grund-

schutz-Kompendiums mit den System- und Prozessbausteinen ist in Kapitel 8.3.1 *Das IT-Grundschutz-Kompendium* zu finden.

Die Modellierung nach IT-Grundschutz besteht nun darin, für die Bausteine einer jeden Schicht zu entscheiden, ob und wie sie zur Abbildung des Informationsverbunds herangezogen werden können. Je nach betrachtetem Baustein können die Zielobjekte dieser Abbildung von unterschiedlicher Art sein: einzelne Geschäftsprozesse oder Komponenten, Gruppen von Komponenten, Gebäude, Liegenschaften, Organisationseinheiten usw. Können einzelne Zielobjekte nicht unmittelbar mit den vorhandenen Bausteinen abgebildet werden, muss gewährleistet sein, dass ähnliche, verallgemeinerte Bausteine berücksichtigt werden.

6.2.2 Reihenfolge der Baustein-Umsetzung

Um grundlegende Risiken abzudecken und eine ganzheitliche Informationssicherheit aufzubauen, müssen die essenziellen Sicherheitsanforderungen frühzeitig erfüllt und entsprechende Sicherheitsmaßnahmen umgesetzt werden. Daher wird im IT-Grundschutz eine Reihenfolge für die umzusetzenden Bausteine vorgeschlagen.

Im IT-Grundschutz-Kompendium wird im Kapitel *Schichtenmodell und Modellierung* beschrieben, wann ein einzelner Baustein sinnvollerweise eingesetzt werden soll und auf welche Zielobjekte er anzuwenden ist. Zudem sind die Bausteine danach gekennzeichnet, ob sie vor- oder nachrangig umgesetzt werden sollten.

Diese Kennzeichnung zeigt nur die sinnvolle zeitliche Reihenfolge für die Umsetzung der jeweiligen Anforderungen der Bausteine auf und stellt keine Gewichtung der Bausteine untereinander dar. Grundsätzlich müssen alle für den jeweiligen Informationsverbund relevanten Bausteine des IT-Grundschutz-Kompendiums umgesetzt werden.

Die Kennzeichnung der Bausteine stellt des Weiteren nur eine Empfehlung dar, in welcher Reihenfolge die verschiedenen Bausteine sinnvoll umgesetzt werden könnten. Jede Institution kann hier eine abweichende, für sich sinnvolle Reihenfolge festlegen.

6.2.3 Zuordnung von Bausteinen

Die Zuordnung von Bausteinen zu Zielobjekten sollte in Form einer Tabelle mit folgenden Spalten dokumentiert werden:

- Vollständiger Titel des Bausteins (z. B. SYS.3.1 *Laptop*)
- Zielobjekt: Dieses kann z. B. die Identifikationsnummer einer Komponente oder einer Gruppe umfassen bzw. der Name eines Gebäudes oder einer Organisationseinheit sein.
- Ansprechpartner: Diese Spalte dient zunächst nur als Platzhalter. Der Ansprechpartner wird nicht im Rahmen der Modellierung, sondern erst bei der Planung des eigentlichen Soll-Ist-Vergleichs im IT-Grundschutz-Check ermittelt.
- Reihenfolge: Es sollte die Umsetzungsreihenfolge (R1, R2, R3) des Bausteins eingetragen werden.
- Hinweise: In dieser Spalte können Randinformationen und Begründungen für die Modellierung dokumentiert werden.

6.2.4 Ermittlung konkreter Maßnahmen aus Anforderungen

Über die Modellierung wurden die Bausteine des IT-Grundschutz-Kompendiums ausgewählt, die für die einzelnen Zielobjekte des betrachteten Informationsverbunds umzusetzen sind. In den Bausteinen

werden die Anforderungen aufgeführt, die typischerweise für diese Komponenten geeignet und angemessen sind.

Für die Erstellung eines Sicherheitskonzepts oder für ein Audit müssen jetzt die einzelnen Anforderungen bearbeitet und zur Erfüllung geeignete Sicherheitsmaßnahmen formuliert werden, hierbei unterstützen die zu vielen Bausteinen zugehörigen Umsetzungshinweise. Vertiefende Informationen hierzu sind in Kapitel 8.3.6 *Anpassung der Baustein-Anforderungen* zu finden.

6.3 IT-Grundschutz-Check für Basis-Absicherung

Schon bevor eine IT-Grundschutz-Vorgehensweise ausgewählt wurde, wurden während der Vorarbeiten in der Erstaufnahme (siehe Kapitel 3.2.4 *Ersterfassung der Prozesse, Anwendungen und IT-Systeme*) die geschäftskritischen Informationen und Kernprozesse der Institution ermittelt und die betroffenen Anwendungen, IT-Systeme, Netze und Räume erfasst. Der betrachtete Informationsverbund wurde mithilfe der vorhandenen Bausteine aus dem IT-Grundschutz-Kompendium nachgebildet. Die Auswahl und Priorisierung der IT-Grundschutz-Bausteine (wie im vorherigen Kapitel beschrieben) wird nun als Prüfplan benutzt, um anhand eines Soll-Ist-Vergleichs herauszufinden, welche Basis-Anforderungen ausreichend oder nur unzureichend erfüllt sind.

Bei dem hier anzuwendenden IT-Grundschutz-Check für die Basis-Absicherung müssen lediglich die Basis-Anforderungen erfüllt sein. Für eine Standard- oder Kern-Absicherung ist innerhalb dieser Vorgehensweisen ein separater IT-Grundschutz-Check durchzuführen, bei dem die Standard-Anforderungen der betreffenden Bausteine hinzukommen. Um Mehraufwände zu vermeiden und Synergieeffekte erzielen zu können, sollten die Ergebnisse des für die Basis-Absicherung durchzuführenden IT-Grundschutz-Checks so aufbereitet sein, dass sie direkt in die Standard- oder Kern-Absicherung integriert werden können.

Unabhängig von der IT-Grundschutz-Vorgehensweise besteht der IT-Grundschutz-Check aus drei unterschiedlichen Schritten. Im ersten Schritt werden die organisatorischen Vorbereitungen getroffen, insbesondere die relevanten Ansprechpartner für den Soll-Ist-Vergleich werden ausgewählt. Im zweiten Schritt wird der eigentliche Soll-Ist-Vergleich mittels Interviews und Stichproben durchgeführt. Im letzten Schritt werden die erzielten Ergebnisse des Soll-Ist-Vergleichs einschließlich der erhobenen Begründungen dokumentiert.

Organisatorische Vorarbeiten für den IT-Grundschutz-Check

Zunächst sollten alle hausinternen Papiere, die die sicherheitsrelevanten Abläufe regeln, gesichtet werden. Diese Dokumente können bei der Ermittlung des Umsetzungsgrades hilfreich sein.

Die geeigneten Interviewpartner müssen identifiziert werden. Für jeden Baustein, der für die Modellierung des Informationsverbunds herangezogen wurde, sollte ein Hauptansprechpartner festgelegt werden. Bei den Anforderungen in den Bausteinen werden die Rollen genannt, die für die Umsetzung der Anforderungen zuständig sind. Hieraus können die geeigneten Ansprechpartner für die jeweilige Thematik in der Institution identifiziert werden. Für die Bausteine der Schicht APP *(Anwendungen)* sind dies beispielsweise die Betreuer der einzelnen Anwendungen.

Als Nächstes sollte festgestellt werden, ob und in welchem Umfang externe Stellen an der Ermittlung des Umsetzungsstatus beteiligt werden müssen. Dies kann beispielsweise bei Firmen, die Teile von Geschäftsprozessen oder des IT-Betriebes als outgesourcte Dienstleistungen übernehmen, erforderlich sein.

Für die anstehenden Interviews sollte ein Terminplan erstellt werden. Ein besonderes Augenmerk gilt hier der Terminkoordination mit Personen aus anderen Organisationseinheiten oder anderen Institutionen. Außerdem erscheint es sinnvoll, schon vorab Ausweichtermine abzustimmen.

Durchführung des Soll-Ist-Vergleichs

Bei der Erhebung des erreichten Sicherheitsstatus werden die Sicherheitsanforderungen des jeweiligen Bausteins der Reihe nach durchgearbeitet. Diese können vollständig, teilweise oder nicht erfüllt sein. Als Umsetzungsstatus ist daher jeweils eine der folgenden Aussagen möglich:

„entbehrlich"	Die Erfüllung der Anforderung ist in der vorgeschlagenen Art nicht notwendig, weil die Anforderung im betrachteten Informationsverbund nicht relevant ist (z. B. weil Dienste nicht aktiviert wurden).
„ja"	Zu der Anforderung wurden geeignete Maßnahmen vollständig, wirksam und angemessen umgesetzt.
„teilweise"	Die Anforderung wurde nur teilweise umgesetzt.
„nein"	Die Anforderung wurde noch nicht erfüllt, also geeignete Maßnahmen sind größtenteils noch nicht umgesetzt.

Es ist sinnvoll, bei den Interviews nicht nur die Bausteintexte, sondern auch die Umsetzungshinweise oder andere ergänzende Materialien griffbereit zu haben. Den Befragten sollte der Zweck des IT-Grundschutz-Checks kurz vorgestellt werden. Es bietet sich an, mit den Anforderungsüberschriften fortzufahren und die Anforderung kurz zu erläutern. Dem Gesprächspartner sollte die Möglichkeit gegeben werden, auf die bereits umgesetzten Anforderungen und Maßnahmen einzugehen und danach noch offene Punkte zu besprechen.

Zum Abschluss jedes Bausteins sollte den Befragten das Ergebnis (Umsetzungsstatus der Anforderungen: entbehrlich/ja/teilweise/nein) mitgeteilt und diese Entscheidung erläutert werden.

Dokumentation der Ergebnisse

Die Ergebnisse des IT-Grundschutz-Checks sollten so dokumentiert werden, dass sie für alle Beteiligten nachvollziehbar sind und als Grundlage für die Umsetzungsplanung der defizitären Anforderungen und Maßnahmen genutzt werden können. Es sollten geeignete Hilfsmittel verwendet werden, die bei der Erstellung und Aktualisierung aller im Sicherheitsprozess erforderlichen Dokumente unterstützen, beispielsweise spezielle IT-Grundschutz-Tools oder selbst entwickelte Tabellen. Als Hilfsmittel stehen auch auf der IT-Grundschutz-Website entsprechende Formulare für die jeweiligen Bausteine zur Verfügung.

Die Ergebnisse des Soll-Ist-Vergleichs sollten tabellarisch erfasst werden. Dabei sollten zu jeder Anforderung des jeweiligen Bausteins folgende Informationen festgehalten werden:

- Umsetzungsgrad (entbehrlich/ja/teilweise/nein)
- Verantwortliche: Welche Mitarbeiter sind für die vollständige Umsetzung einer defizitären Anforderung verantwortlich? Bis wann ist diese umzusetzen?
- Bemerkungen: Ein solches Feld ist wichtig, um getroffene Entscheidungen später nachvollziehen zu können. Bei Anforderungen, deren Umsetzung entbehrlich erscheint, ist hier die Begründung zu nennen. Bei Anforderungen, die noch nicht oder nur teilweise umgesetzt sind, sollte in diesem Feld dokumentiert werden, welche Maßnahmen noch umgesetzt werden müssen. In dieses Feld sollten auch alle anderen Bemerkungen eingetragen werden, die bei der Beseitigung von Defiziten hilfreich oder im Zusammenhang mit der Anforderung zu berücksichtigen sind.

- Defizite/Kostenschätzung: Für Anforderungen, die nicht oder nur teilweise erfüllt wurden, ist das damit verbundene Risiko in geeigneter Form zu ermitteln und zu dokumentieren. Des Weiteren sollte geschätzt werden, welchen finanziellen und personellen Aufwand die Beseitigung der Defizite erfordert.

Diese Schritte werden detailliert im Kapitel 8.4 *IT-Grundschutz-Check* beschrieben.

6.4 Realisierung

In diesem Kapitel wird beschrieben, wie für die Basis-Absicherung aus den Anforderungen die Sicherheitsmaßnahmen abgeleitet und wie diese dann geplant, durchgeführt, begleitet und überwacht werden können. Es liegen die Ergebnisse des IT-Grundschutz-Checks, also des Soll-Ist-Vergleichs, vor.

Generell müssen für die Basis-Absicherung alle identifizierten Basis-Anforderungen erfüllt werden. Auch für die Erfüllung der Basis-Anforderungen stehen in der Regel nur beschränkte Ressourcen an Geld und Personal zur Verfügung. Das primäre Ziel der nachfolgend beschriebenen Schritte ist es daher, eine möglichst effiziente Erfüllung der vorgesehenen Basis-Anforderungen zu erreichen (eine vollständige Beschreibung für alle IT-Grundschutz-Vorgehensweisen ist im Kapitel 9 „Umsetzung der Sicherheitskonzeption" zu finden):

- Sichtung der Untersuchungsergebnisse
  In einer Gesamtsicht sollten zuerst die fehlenden oder nur teilweise erfüllten Basis-Anforderungen ausgewertet werden.
- Konsolidierung der Basis-Anforderungen
  In diesem Schritt werden zunächst die noch zu erfüllenden Basis-Anforderungen konsolidiert.
- Kosten- und Aufwandsschätzung
  Es sollte für jede zu erfüllende Basis-Anforderung festgehalten werden, welche Investitionskosten und welcher Personalaufwand dafür notwendig sind.
- Festlegung der Umsetzungsreihenfolge der Basis-Anforderungen
  Wenn das vorhandene Budget oder die personellen Ressourcen nicht ausreichen, um die fehlenden Basis-Anforderungen sofort erfüllen zu können, muss eine Umsetzungsreihenfolge festgelegt werden.
- Festlegung der Aufgaben und der Verantwortung
  Es muss festgelegt werden, wer bis wann welche Basis-Anforderungen erfüllen muss.
- Realisierungsbegleitende Basis-Anforderungen
  Überaus wichtig ist es, notwendige realisierungsbegleitende Basis-Anforderungen, wie beispielsweise Schulungen, rechtzeitig zu konzipieren und für die Realisierung mit einzuplanen.

6.5 Auswahl einer folgenden Vorgehensweise

Informationssicherheit muss gelebt werden. Um das Sicherheitsniveau aufrechtzuerhalten und kontinuierlich verbessern zu können, müssen nicht nur die erforderlichen Sicherheitsmaßnahmen umgesetzt und fortlaufend aktualisiert werden, sondern auch der gesamte Prozess der Informationssicherheit muss regelmäßig auf seine Wirksamkeit und Effizienz hin überprüft werden.

Die Basis-Absicherung ist eine IT-Grundschutz-Vorgehensweise für den Einstieg, um zunächst zeitnah die wichtigsten Sicherheitsempfehlungen für den ausgewählten Einsatzbereich identifizieren und umsetzen zu können. Ziel ist es daher, mittelfristig ein vollständiges Sicherheitskonzept gemäß der Stan-

dard-Absicherung zu erstellen. Als Zwischenschritt könnte nach der Basis-Absicherung und vor der Standard-Absicherung die nun erstellte Sicherheitskonzeption um die Kern-Absicherung ergänzt werden.

Nachdem die Basis-Absicherung realisiert wurde, sollte zeitnah entschieden werden, wann mit dem notwendigen Verbesserungsprozess begonnen wird. In Abhängigkeit der Sicherheitsansprüche und der verfügbaren Ressourcen ist zu entscheiden, ob im nächsten Schritt eine Sicherheitskonzeption nach der Standard- oder der Kern-Absicherung erstellt werden soll. Informationen zur Auswahl sind in Kapitel 3.3 *Entscheidung für Vorgehensweise* zu finden.

7 Erstellung einer Sicherheitskonzeption nach der Vorgehensweise Kern-Absicherung

Der IT-Grundschutz des BSI bietet einen ganzheitlichen Schutz aller geschäftsrelevanten Informationen einer Institution. Für Institutionen, die noch großen Handlungsbedarf im Bereich der Informationssicherheit haben, kann es zielführend sein, sich anfangs auf die Absicherung der essenziellen Assets zu beschränken und erst nachfolgend ein breites Sicherheitskonzept umzusetzen. Dieses Kapitel beschreibt, wie vorzugehen ist, wenn als Vorgehensweise Kern-Absicherung ausgewählt wurde.

Nachdem ein Informationssicherheitsprozess initiiert, die wesentlichen Rahmenbedingungen sowie die zu schützenden Prozesse, Anwendungen und IT-Systeme identifiziert wurden und eine Vorgehensweise ausgewählt wurde, wird die Sicherheitskonzeption für die Institution erstellt. Zu diesem Zweck werden im IT-Grundschutz-Kompendium für typische Komponenten von Geschäftsprozessen, Anwendungen, IT-Systemen und anderen Objekten organisatorische, personelle, infrastrukturelle und technische Standardsicherheitsanforderungen gestellt. Diese sind in Bausteinen strukturiert, sodass sie modular aufeinander aufsetzen.

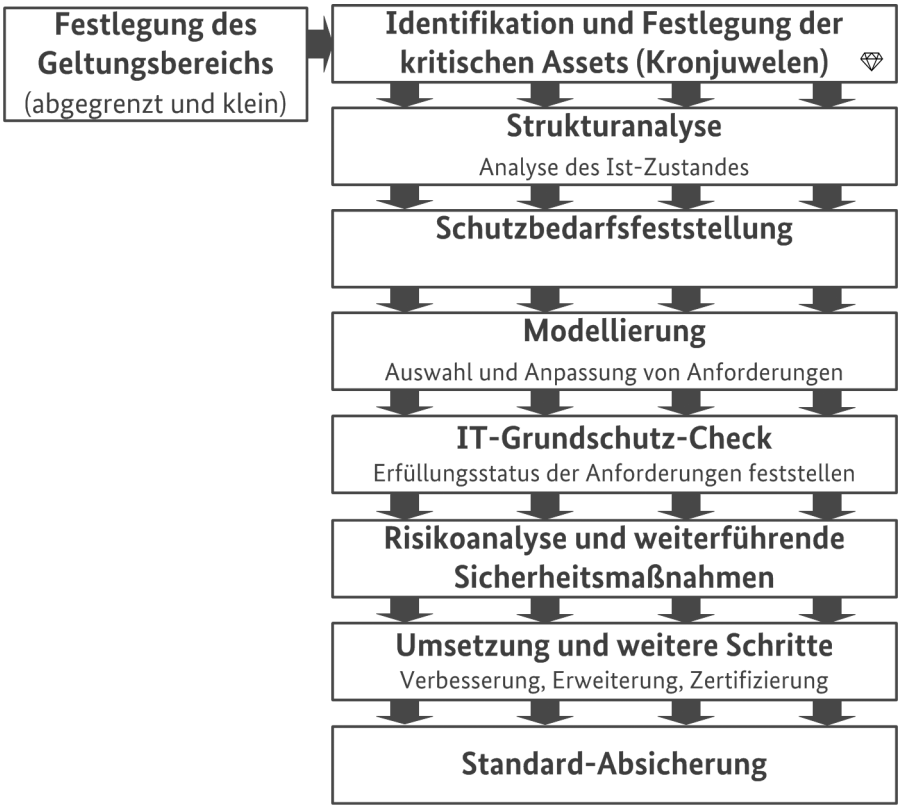


Abbildung 9: Kern-Absicherung

7.1 Die Methodik der Kern-Absicherung

Die Vorgehensweise Kern-Absicherung des IT-Grundschutzes konzentriert sich auf den Schutz von besonders schützenswerten Assets, den sogenannten „Kronjuwelen". Bei der Anwendung der Kern-Absicherung erfolgt ein Soll-Ist-Vergleich zwischen den im IT-Grundschutz-Kompendium aufgestellten und den bereits in der Institution erfüllten Anforderungen für die Absicherung dieser Kronjuwelen. Dabei nicht oder nur unzureichend erfüllte Anforderungen zeigen die Sicherheitsdefizite auf, die es durch entsprechende Maßnahmen zu beheben gilt.

Das mittels der Kern-Absicherung erstellte Sicherheitskonzept ist die Basis für ein umfangreicheres Sicherheitskonzept, wie es mit der Standard-Absicherung (siehe Kapitel 8) erstellt und etabliert werden kann.

Da sich die Kern-Absicherung auf die besonders schützenswerten Assets konzentriert, ist hier grundsätzlich von einem erhöhten Schutzbedarf auszugehen. Daher müssen die in den relevanten Bausteinen des IT-Grundschutz-Kompendiums aufgeführten Basis- und Standard-Anforderungen komplett umgesetzt werden. Darauf aufbauend muss bei erhöhtem Schutzbedarf eine Risikoanalyse unter Berücksichtigung von Kosten- und Wirksamkeitsaspekten durchgeführt werden, damit die relevanten Risiken im Bereich der Kronjuwelen ganzheitlich behandelt werden können. Dabei dürfen die in den Bausteinen exemplarisch aufgeführten Anforderungen für einen erhöhten Schutzbedarf als Grundlage herangezogen werden, um entsprechende individuelle Maßnahmen zu ergänzen.

Hierzu ist im BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz* eine im Vergleich zu traditionellen Risikoanalyse-Methoden einfachere Vorgehensweise beschrieben.

Die Kern-Absicherung, bei der der Schutz von Kronjuwelen im Fokus steht, ist kein allein stehendes Projekt, sondern Teil des Sicherheitsprozesses. Die Kern-Absicherung kann nur dann als Projekt betrachtet werden, wenn sie anschließend in die Standard-Absicherung integriert wird. Solange dies nicht der Fall ist, muss regelmäßig der Prozess der Kern-Absicherung überprüft und verbessert werden.

Die Erstellung einer Sicherheitskonzeption für eine Kern-Absicherung nach dem IT-Grundschutz gliedert sich grob in folgende Bereiche:

- Festlegung des Geltungsbereichs für die Kern-Absicherung
- Identifikation und Festlegung der kritischen Assets (Kronjuwelen)
- Strukturanalyse
- Schutzbedarfsfeststellung
- Modellierung: Auswahl und Anpassung von Anforderungen
- IT-Grundschutz-Check
- Risikoanalyse und weiterführende Sicherheitsmaßnahmen
- Umsetzung und weitere Schritte

7.2 Festlegung des Geltungsbereichs für die Kern-Absicherung

Die ganzheitliche Umsetzung von Informationssicherheit, wie dies mit der Standard-Absicherung erfolgt, ist in einem einzelnen großen Schritt oft ein zu ehrgeiziges Ziel. Viele kleine Schritte und ein langfristiger, kontinuierlicher Verbesserungsprozess ohne hohe Investitionskosten zu Beginn sind oft erfolgversprechender. Daher konzentriert sich die Kern-Absicherung auf die besonders schützenswerten Assets und Ressourcen der Institution. Von diesem ausgewählten und beschränkten Bereich der Institution ausgehend, sollte dann kontinuierlich die Sicherheit innerhalb der gesamten Institution verbessert werden.

Zunächst muss daher dieser Bereich festgelegt werden, für den die Sicherheitskonzeption erstellt und umgesetzt werden soll. Dieser umfasst unter anderem alle (Teil-)Geschäftsprozesse, Anwendungen, IT-Systeme, Infrastrukturen, die für die Bearbeitung der besonders kritischen Geschäftsprozesse und Informationen benötigt werden. Dazu gehören unter Umständen auch ICS-Systeme. Der betrachtete Geltungsbereich für die Sicherheitskonzeption wird im IT-Grundschutz generell als „Informationsver-

bund“ bezeichnet. Die Kern-Absicherung betrachtet somit einen bewusst eingeschränkten Informationsverbund.

Bei der Kern-Absicherung ist es besonders wichtig, den Informationsverbund nicht nur klar abzugrenzen, sondern ihn auch möglichst klein zu halten. Jedes weitere Zielobjekt, das einem Informationsverbund hinzugefügt wird, erhöht die Komplexität der Absicherung. Daher kann es in Zweifelsfällen zielführender sein, die kritischen Objekte in kleinen, überschaubaren Bereichen zu betreiben, die vom Rest der Institution abgeschottet sind. Beispielsweise ist es sinnvoller, geschäftskritische Informationen in getrennten IT-Umgebungen zu verarbeiten und dafür Unbequemlichkeiten in Kauf zu nehmen, statt die im höchsten Maße schutzbedürftigen Geschäftsprozesse mit vielen Anwendungen aus der gewohnten Büroumgebung zu verknüpfen und damit alle mit ihnen vernetzten Komponenten auf dem dann erforderlichen hohen Sicherheitsniveau absichern zu müssen.

7.3 Identifikation und Festlegung der kritischen Assets (Kronjuwelen)

Als Kronjuwelen werden diejenigen Geschäftsprozesse und die Informationen bezeichnet, die am wichtigsten für den Erhalt der Institution sind. Es ist wichtig, die mögliche Menge der schützenswerten Daten gezielt einzugrenzen.

Zu den kritischen Assets gehören üblicherweise:

- Informationen, die wesentlich zur erfolgreichen Durchführung von essenziellen Geschäftsprozessen sind.
- Informationen und Geschäftsprozesse, die ein deutlich erhöhtes Gefährdungspotenzial bezüglich der Informationssicherheit innehaben. Dies betrifft Vertraulichkeit, Integrität und Verfügbarkeit.
- Informationen und Geschäftsprozesse, deren Diebstahl, Zerstörung, Kompromittierung oder Beeinträchtigung einen existenzbedrohenden Schaden für die Institution bedeutet und die vorrangig geschützt werden sollen.

Die folgenden weiteren Charakteristika für Kronjuwelen helfen bei der Identifikation und Eingrenzung der kritischen Assets:

- Als Kronjuwelen werden Informationen oder Geschäftsprozesse bezeichnet, nicht Dienstleistungen, Anwendungen, IT-Systeme oder ähnliche Objekte.
- Die Menge der Informationen und Geschäftsprozesse mit deutlich erhöhtem Schutzbedarf ist überschaubar bzw. umfasst nur einen kleinen Anteil aller Geschäftsprozesse der Institution. Nur wenige Assets ragen in ihrer Bedeutung für die Fachaufgaben bzw. Geschäftstätigkeit deutlich aus der Masse heraus und können einen großen Schaden für die Institution verursachen.
- Kronjuwelen können auch in Formen vorliegen, die nicht auf den ersten Blick offensichtlich sind: dies mögen einzelne Dateien, Datensammlungen, strukturierte oder unstrukturierte Informationen bis hin zu handschriftlichen Notizen oder Gesprächen sein, kann aber auch das Wissen und die Fähigkeiten einzelner Mitarbeiter betreffen.
- Kronjuwelen sind häufig die Informationen, für die es wünschenswert erscheint, das vorhandene Klassifikationsschema um noch höhere Kategorien zu erweitern.
- Es ist davon auszugehen, dass der Schutzbedarf der Kronjuwelen und aller damit verknüpften Ressourcen im Informationsverbund mindestens als „hoch“ einzuordnen ist.

- Der Schutzbedarf von Kronjuwelen kann sich mit der Zeit verändern. Typische Beispiele sind hier Informationen über Produktneuerungen oder Jahresabschlussberichte.
- Es muss bei Kronjuwelen häufig zwischen verschiedenen „Besitzern" der Information unterschieden werden. Diese können unterschiedliche Rollen und Verantwortlichkeiten haben. Insbesondere betrifft dies „Zuständigkeit" (Responsibility) versus „Rechenschaftspflicht" (Accountability).
- Der Schutzbedarf von Kronjuwelen kann sogar als so hoch eingestuft werden, dass die Sicherheitsbeauftragten nicht die Berechtigungen bekommen, diese selbst einzusehen, aber den Auftrag haben, sie zu schützen.
- Es sind alle elementaren Gefährdungen des IT-Grundschutz-Kompendiums relevant, häufig liegt ein besonderer Fokus auf den Angreifern. Darüber dürfen aber Ursachen wie Umwelteinflüsse oder menschliche Fehlhandlungen nicht vergessen werden.

Die Festlegung, bei welchen Assets es sich um Kronjuwelen handelt, erfolgt typischerweise durch die Leitungsebene. Die Entscheidung, bestimmte Informationen als Kronjuwelen einzustufen, führt unmittelbar dazu, dass adäquate Sicherheitsmaßnahmen für diese ergriffen werden müssen. Diese sind natürlich entsprechend dem herausragenden Schutzbedarf der Kronjuwelen folgend umfangreich und damit tendenziell aufwendig und teuer. Fachverantwortliche, Sicherheitsbeauftragte und andere Instanzen können vorschlagen, diese Informationen als Kronjuwelen einzustufen, die Entscheidung muss jedoch letztlich vonseiten der Leitungsebene erfolgen.

Jede Institution sollte zur besseren Einordnung für sich selbst individuelle Beispiele für Kronjuwelen erarbeiten. Zudem sollten auch Beispiele zur Abgrenzung von Kronjuwelen zu wichtigen Informationen erstellt werden. Nachfolgend sind einige typische Beispiele für Kronjuwelen aus der Praxis aufgeführt:

- Details über anstehende geschäftliche Entscheidungen, z. B. Strategiepapiere für Firmenaufkäufe, Finanzierungspläne.
- Details über Produktentwicklungen, z. B. Hintergrundmaterial zu Patentanträgen, Designentwürfen usw.
- Informationen über Standorte geschützter Pflanzen, gefährdeter Personen oder geheimer Anlagen.
- Administrative Zugriffsdaten für Server (wenn nicht auffindbar, ist kein schneller Zugriff möglich).
- Kryptomaterial, z. B. Masterschlüssel für institutionsweit eingesetzte kryptografische Verfahren.
- Baupläne oder Rezepturen für Produkte.

Anmerkung: Das geheime Familienrezept einer Koffeinbrause ist ein in der Öffentlichkeit immer wieder thematisiertes Beispiel für ein „Kronjuwel". Wird dies offenbart (Verlust der Vertraulichkeit), würde das einen großen Pressewirbel auslösen, aber die Existenz der Firma nicht gefährden, sondern eventuell sogar zur Produktwerbung beitragen. In diesem Kontext wird auch deutlich, dass manche Kronjuwelen zu „heiß" sein könnten, um für einen Angreifer oder Konkurrenten wertvoll zu sein. Eine unbemerkte Änderung der Rezeptur (Verlust der Integrität) könnte aber zu einem schweren Imageschaden führen. Der vollständige Verlust der Rezeptur würde schließlich zu einem Produktionsstillstand führen und wäre damit das schwerwiegendste Problem.

Es kann Kronjuwelen geben, bei denen nicht ein einzelner Prozess oder ein Objekt im Fokus steht, sondern wo die Kronjuwelen durch die Kumulation wichtiger geschäftskritischer Werte entstehen.

Beispiel:

Wenn bei einem Buchverlag der streng vertrauliche Entwurf des letzten Bands einer Erfolgsreihe an die Öffentlichkeit gelangt, ist das ein schwerwiegender Sicherheitsvorfall. Werden allerdings alle Daten der für das Geschäftsjahr geplanten Bestseller vernichtet und somit deren Veröffentlichung verhindert, kann dieser Vorfall für den Verlag zu einer wirtschaftlichen Katastrophe führen.

Es kann somit Kronjuwelen geben, bei denen nicht ein einzelner Prozess oder ein einziges Objekt die höchste Verfügbarkeit aufweisen muss, sondern wo die Verfügbarkeit der Produktionskette oder sogar der Schutzeinrichtungen selbst abzusichern ist. Ein Beispiel hierfür sind die Prozesse zur Energieerzeugung in einem Kernkraftwerk.

7.4 Strukturanalyse

Für die Erstellung eines Sicherheitskonzepts und insbesondere für die Anwendung des IT-Grundschutz-Kompendiums ist es erforderlich, das Zusammenspiel der Geschäftsprozesse, der Anwendungen und der vorliegenden Informationstechnik zu analysieren und zu dokumentieren. Aufgrund der heute üblichen starken Vernetzung von IT-Systemen bietet sich ein Netztopologieplan als Ausgangsbasis für die weitere technische Analyse an. Die folgenden Aspekte müssen berücksichtigt werden:

- die für die Kern-Absicherung im eingeschränkten Informationsverbund betriebenen Anwendungen und die dadurch gestützten Geschäftsprozesse,
- die organisatorischen und personellen Rahmenbedingungen für diesen Informationsverbund,
- im Informationsverbund eingesetzte vernetzte und nicht vernetzte IT-Systeme,
- die Kommunikationsverbindungen zwischen den IT-Systemen und nach außen,
- die vorhandene Infrastruktur.

Die einzelnen Schritte der Strukturanalyse werden im Detail in Kapitel 8.1 dieses Dokuments in Form einer Handlungsanweisung beschrieben.

7.5 Schutzbedarfsfeststellung

Zweck der Schutzbedarfsfeststellung ist es, zu ermitteln, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich hierfür eine Einteilung in die drei Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“. Grundsätzlich ist bei den Assets, die durch eine Kern-Absicherung geschützt werden sollen, von einem Schutzbedarf der Kategorien „hoch“ und „sehr hoch“ auszugehen. Trotzdem muss der Schutzbedarf dieser wenigen, besonders geschäftskritischen Assets dediziert eingeschätzt werden.

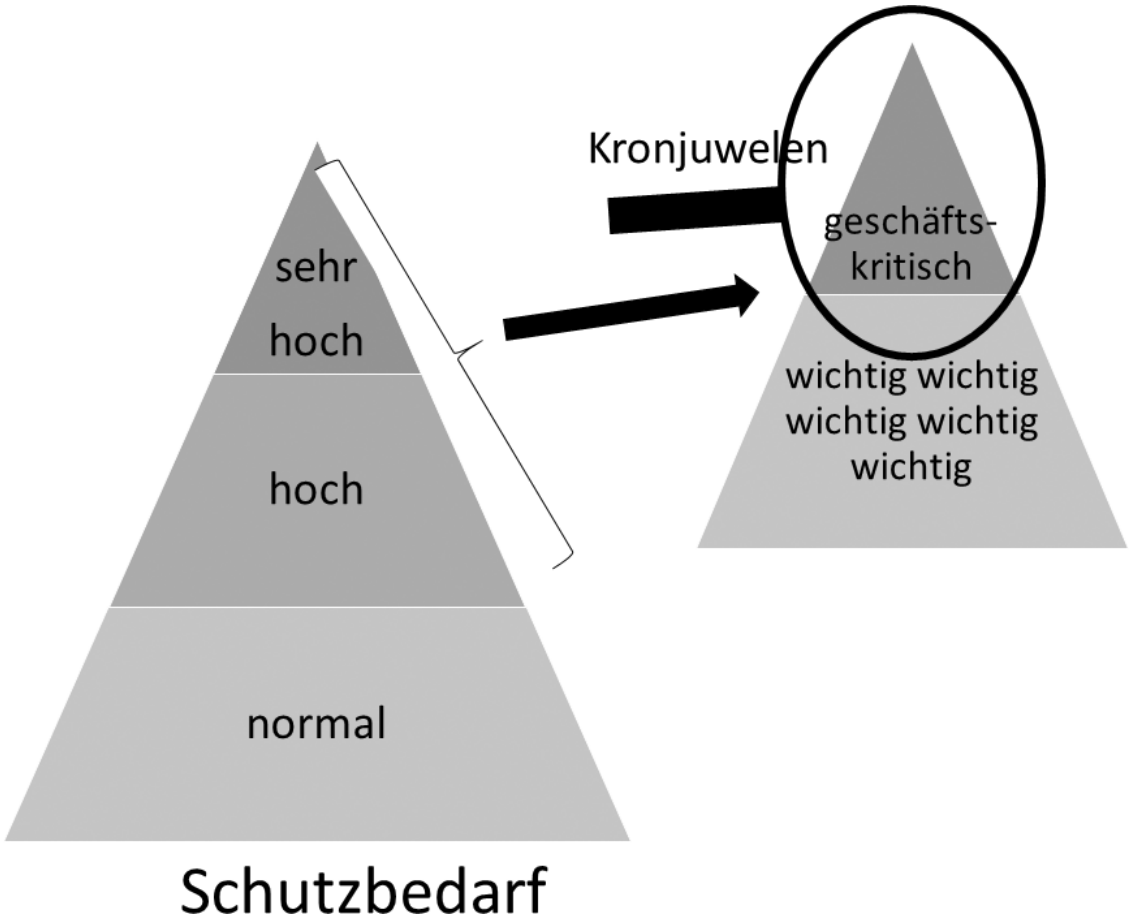


Abbildung 10: Schutzbedarf und Kronjuwelen

Neben den als Kronjuwelen identifizierten Assets gibt es typischerweise weitere Assets mit hohem oder sehr hohem Schutzbedarf, die auch angemessen zu schützen sind.

Die einzelnen Schritte der Schutzbedarfsfeststellung werden im Detail in Kapitel 8.2 dieses Dokuments erläutert, wobei zu beachten ist, dass bei der Kern-Absicherung der Fokus auf einem hohen und sehr hohen Schutzbedarf liegt.

7.6 Modellierung: Auswahl und Anpassung von Anforderungen

Die Voraussetzung für die Anwendung des IT-Grundschutz-Kompendiums auf einen Informationsverbund sind detaillierte Unterlagen über seine Struktur und den Schutzbedarf der darin enthaltenen Zielobjekte. Diese Informationen sollten über die zuvor beschriebenen Arbeitsschritte ermittelt werden. Um geeignete Sicherheitsmaßnahmen für den vorliegenden Informationsverbund identifizieren zu können, müssen anschließend die Bausteine des IT-Grundschutz-Kompendiums auf die Zielobjekte und Teilbereiche abgebildet werden.

Dieser Vorgang der Modellierung wird in Kapitel 8.3 näher erörtert.

7.7 IT-Grundschutz-Check

Der IT-Grundschutz-Check ist ein Organisationsinstrument, das einen schnellen Überblick über das vorhandene Sicherheitsniveau bietet. Mithilfe von Interviews wird der Status quo eines bestehenden (nach dem IT-Grundschutz modellierten) Informationsverbunds in Bezug auf den Grad der Erfüllung der Sicherheitsanforderungen des IT-Grundschutzes ermittelt. Als Ergebnis liegt ein Katalog vor, in dem für jede relevante Anforderung der Erfüllungsstatus „ja", „teilweise", „nein" oder „entbehrlich" (mit Begründung, nicht möglich bei Basis-Anforderungen) erfasst ist. Durch die Identifizierung von noch nicht oder nur teilweise erfüllten Anforderungen werden Verbesserungsmöglichkeiten für die Sicherheit der betrachteten Geschäftsprozesse und der Informationstechnik aufgezeigt.

Kapitel 8.4 beschreibt einen Aktionsplan für die Durchführung eines IT-Grundschutz-Checks. Dabei wird sowohl den organisatorischen Aspekten als auch den fachlichen Anforderungen bei der Projektdurchführung Rechnung getragen.

7.8 Risikoanalyse und weiterführende Sicherheitsmaßnahmen

Die Erfüllung der Standard-Anforderungen nach IT-Grundschutz bietet im Normalfall einen angemessenen und ausreichenden Schutz. Bei einem hohen oder sehr hohen Schutzbedarf, wie er im Rahmen der Kern-Absicherung regelmäßig auftritt, ist zu prüfen, ob sich zusätzliche Sicherheitsanforderungen ergeben und damit zusätzliche oder ersatzweise höherwertige Sicherheitsmaßnahmen erforderlich sind. Dies gilt auch, wenn besondere Einsatzbedingungen vorliegen oder wenn Komponenten verwendet werden, die nicht mit den existierenden Bausteinen des IT-Grundschutz-Kompendiums abgebildet werden können. Dann ist zu entscheiden, ob für die jeweils betroffenen Bereiche eine Risikoanalyse durchgeführt werden muss, um angemessene Sicherheitsmaßnahmen zu identifizieren.

Eine Methode für Risikoanalysen ist die im BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz* beschriebene Vorgehensweise. In Kapitel 8.5 wird diese Methode überblicksartig dargestellt. Die erfolgreiche Durchführung einer Risikoanalyse hängt entscheidend von den Fachkenntnissen des Projektteams ab. Daher ist es häufig sinnvoll, fachkundiges externes Personal hinzuzuziehen.

7.9 Umsetzung und weitere Schritte

Die identifizierten und konsolidierten Sicherheitsmaßnahmen für die Kern-Absicherung müssen im Anschluss umgesetzt werden. Was hierbei zu beachten ist, wird in Kapitel 9 *Umsetzung der Sicherheitskonzeption* ausführlich diskutiert.

Zu den Aufgaben eines ISMS gehört es nicht nur, im betrachteten Informationsverbund die Informationssicherheit aufrechtzuerhalten, sondern diese sollte auch fortlaufend verbessert werden (siehe Kapitel 10). Für die Kern-Absicherung bedeutet dies, dass natürlich regelmäßig überprüft werden muss, ob die getroffenen Sicherheitsvorkehrungen noch der aktuellen Gefährdungslage entsprechen. Des Weiteren sollte überlegt werden, ob nach der erfolgreichen Absicherung der Kronjuwelen nicht auch noch weitere Bereiche der Institution angemessen geschützt werden sollten. Hierfür kann beispielsweise auf weitere Bereiche die Basis- oder die Standard-Absicherung angewendet werden oder auch der Informationsverbund der Kern-Absicherung erweitert werden.

Wenn die Kern-Absicherung in einem abgegrenzten Informationsverbund erfolgreich umgesetzt wurde, kann dies auch über eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz nach innen und außen hin demonstriert werden. Welche Schritte hierfür notwendig sind und welche Bedingungen für eine erfolgreiche Zertifizierung erfüllt werden müssen, wird in Kapitel 11 *Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz* näher ausgeführt.

8 Erstellung einer Sicherheitskonzeption nach der Vorgehensweise der Standard-Absicherung

Eines der Ziele der Standard-Absicherung des IT-Grundschutzes ist es, eine pragmatische und effektive Vorgehensweise zur Erzielung eines normalen Sicherheitsniveaus anzubieten, das auch als Basis für ein höheres Sicherheitsniveau dienen kann.

Nachdem ein Informationssicherheitsprozess initiiert, die Sicherheitsleitlinie und Informationssicherheitsorganisation definiert wurden, wird die Sicherheitskonzeption für die Institution erstellt. Als Grundlage hierfür finden sich in den Bausteinen des IT-Grundschutz-Kompendiums Sicherheitsanforderungen nach dem jeweiligen Stand der Technik für typische Komponenten von Geschäftsprozessen, Anwendungen, IT-Systemen usw. Diese sind in Bausteinen strukturiert, sodass sie modular aufeinander aufsetzen.

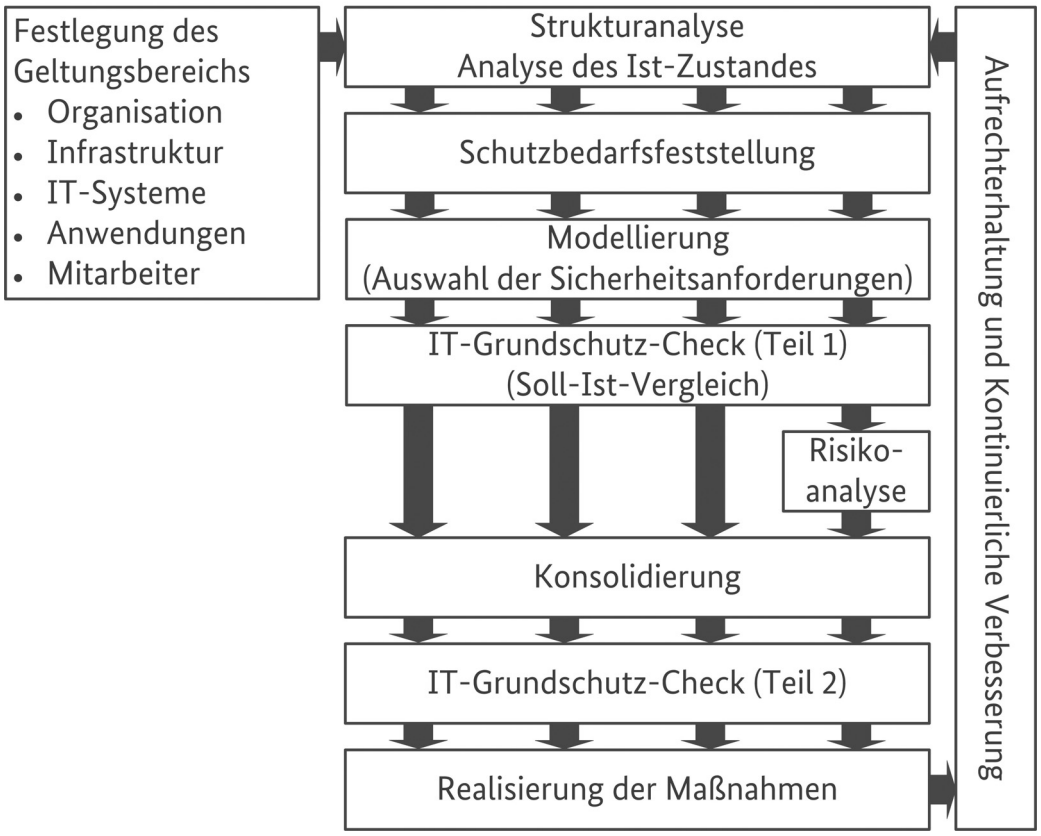


Abbildung 11: Erstellung der Sicherheitskonzeption bei der Standard-Absicherung

Die Durchführung einer Standard-Absicherung nach IT-Grundschutz gliedert sich in die nachfolgenden Aktionsfelder:

Festlegung des Geltungsbereichs

Bei der Entscheidung für die weitere Vorgehensweise (siehe Kapitel 3.3) wurde auch der Geltungsbereich festgelegt, für den die Sicherheitskonzeption erstellt und umgesetzt werden soll. Dies können beispielsweise bestimmte Organisationseinheiten einer Institution sein. Es könnten aber auch Bereiche sein, die definierte Geschäftsprozesse oder Fachaufgaben bearbeiten, inklusive der dafür notwendigen Infrastruktur. Im IT-Grundschutz wird der Geltungsbereich für die Sicherheitskonzeption auch als „Informationsverbund" bezeichnet. Die Bestandteile des betrachteten Informationsverbunds sind

die mit den passenden Bausteinen des IT-Grundschutz-Kompendiums abzusichernden Komponenten.

Strukturanalyse

Für die Erstellung eines Sicherheitskonzepts nach der Vorgehensweise Standard-Absicherung und insbesondere für die Anwendung des IT-Grundschutz-Kompendiums ist es erforderlich, das Zusammenspiel der Geschäftsprozesse, der Anwendungen und der vorliegenden Informationstechnik zu analysieren und zu dokumentieren. Aufgrund der heute üblichen starken Vernetzung von IT-Systemen, die sich auch auf die Bereiche ICS und IoT erstreckt, bietet sich ein Netztopologieplan als Ausgangsbasis für die weitere technische Analyse an. Die folgenden Aspekte müssen berücksichtigt werden:

- im Informationsverbund betriebene Anwendungen und die dadurch gestützten Geschäftsprozesse,
- die organisatorischen und personellen Rahmenbedingungen für den Informationsverbund,
- im Informationsverbund eingesetzte vernetzte und nicht vernetzte IT-Systeme, ICS- und IoT-Komponenten,
- die Kommunikationsverbindungen dazwischen und nach außen,
- die vorhandene Infrastruktur.

Die einzelnen Schritte der Strukturanalyse werden im Detail in Kapitel 8.1 dieses Dokuments in Form einer Handlungsanweisung beschrieben.

Schutzbedarfsfeststellung

Zweck der Schutzbedarfsfeststellung ist es, zu ermitteln, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Hierfür hat sich eine Einteilung in die drei Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ bewährt.

Die einzelnen Schritte der Schutzbedarfsfeststellung werden in Kapitel 8.2 ausführlicher verhandelt.

Auswahl von Anforderungen und Anpassung von Maßnahmen (Modellierung)

Die Voraussetzung für die Anwendung des IT-Grundschutz-Kompendiums auf einen Informationsverbund sind detaillierte Unterlagen über seine Struktur und den Schutzbedarf der darin enthaltenen Zielobjekte. Diese Informationen sollten über die zuvor beschriebenen Arbeitsschritte ermittelt werden. Um geeignete Sicherheitsanforderungen und darüber umzusetzende Maßnahmen für den vorliegenden Informationsverbund identifizieren zu können, müssen anschließend die Bausteine des IT-Grundschutz-Kompendiums auf die Zielobjekte und Teilbereiche abgebildet werden.

Dieser Vorgang der Modellierung wird in Kapitel 8.3 detailliert besprochen.

IT-Grundschutz-Check

Der IT-Grundschutz-Check ist ein Organisationsinstrument, das einen schnellen Überblick über das vorhandene Sicherheitsniveau bietet. Mithilfe von Interviews wird der Status quo eines bestehenden (nach IT-Grundschutz modellierten) Informationsverbunds in Bezug auf den Umsetzungsgrad der Sicherheitsanforderungen des IT-Grundschutz-Kompendiums ermittelt. Als Ergebnis liegt ein Katalog

vor, in dem für jede relevante Anforderung der Umsetzungsstatus „entbehrlich", „ja", „teilweise" oder „nein" erfasst ist. Durch die Identifizierung von noch nicht oder nur teilweise erfüllten Anforderungen werden Verbesserungsmöglichkeiten für die Sicherheit der betrachteten Geschäftsprozesse und der Informationstechnik aufgezeigt.

Kapitel 8.4 beschreibt einen Aktionsplan für die Durchführung eines IT-Grundschutz-Checks. Dabei wird sowohl den organisatorischen Aspekten als auch den fachlichen Anforderungen bei der Projektdurchführung Rechnung getragen.

Risikoanalyse

Durch die Umsetzung der Sicherheitsanforderungen der Standard-Absicherung wird im Normalfall für einen Informationsverbund ein angemessener und ausreichender Schutz erzielt. Bei einem hohen oder sehr hohen Schutzbedarf kann es jedoch sinnvoll sein, zu prüfen, ob zusätzlich oder ersatzweise höherwertige Sicherheitsmaßnahmen erforderlich sind. Dies gilt auch, wenn besondere Einsatzbedingungen vorliegen oder wenn Komponenten verwendet werden, die nicht mit den existierenden Bausteinen des IT-Grundschutz-Kompendiums abgebildet werden können. In diesen Fällen ist eine Risikoanalyse durchzuführen. Sie sollte in regelmäßigen Abständen aktualisiert werden, damit auch geänderte Gefährdungslagen schnell erkannt werden können.

Eine Methode für Risikoanalysen ist die im BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz* beschriebene Vorgehensweise. In Kapitel 8.5 wird diese Methode überblicksartig dargestellt. Die erfolgreiche Durchführung einer Risikoanalyse hängt entscheidend von den Fachkenntnissen des Projektteams ab. Daher ist es häufig sinnvoll, fachkundiges externes Personal hinzuzuziehen.

Reihenfolge der Bearbeitung

Die verschiedenen Aktivitäten, die zur Erstellung einer Sicherheitskonzeption erforderlich sind, also Strukturanalyse, Schutzbedarfsfeststellung, Modellierung eines Informationsverbunds, IT-Grundschutz-Check, Risikoanalyse, müssen nicht zwingend nacheinander abgearbeitet werden. Diese Aktionsfelder können, soweit dies je nach vorhandenen Rahmenbedingungen und Größe des Sicherheitsteams möglich ist, auch unabhängig und zeitgleich durchgeführt werden.

8.1 Strukturanalyse

Die Strukturanalyse dient der Vorerhebung von Informationen, die für die weitere Vorgehensweise in der Erstellung eines Sicherheitskonzepts nach IT-Grundschutz benötigt werden. Dabei geht es um die Erfassung der Bestandteile (Geschäftsprozesse, Informationen, Anwendungen, IT- und ICS-Systeme, Räume, Kommunikationsnetze), die zur Betrachtung des Geltungsbereichs benötigt werden.

Hinweis:

Häufig sind die Geschäftsprozesse noch nicht, nicht durchgängig oder nicht aktuell erfasst. Dann müssen zuerst die relevanten Geschäftsprozesse identifiziert werden, z. B. durch eine Auswertung von Geschäftsverteilungsplänen, Aufgabenbeschreibungen oder anderen organisationsbeschreibenden Papieren.

Dazu müssen die für die Institution wesentlichen Geschäftsprozesse sowie die geschäftskritischen Informationen und Anwendungen ermittelt und die betroffenen IT-, ICS- oder IoT-Systeme, Räume und Netze erfasst werden. Die klassische Vorgehensweise ist, zuerst die Anwendungen und ausgehend davon die weiteren betroffenen Objekte zu ermitteln. Dieser Ansatz hat den Nachteil, dass es häufig schwierig ist,

abstrakte Anwendungen losgelöst von konkreten technischen Komponenten zu erfassen. Daher kann es in einigen Fällen zweckmäßig sein, abweichend von der hier dargestellten Reihenfolge zunächst die IT- und ICS-Systeme zu erheben, da sich die Anwendungen häufig anhand der betrachteten Systeme leichter ermitteln lassen.

Zu beachten ist, dass die Objekte und Daten, die im Rahmen einer Strukturanalyse erfasst werden, meist nicht nur für den Sicherheitsprozess, sondern auch für betriebliche Aspekte und die Verwaltung erforderlich sind. Es sollte daher geprüft werden, ob bereits Datenbanken oder Übersichten gepflegt werden, die im Rahmen der Strukturanalyse als Datenquellen genutzt werden könnten. In vielen Institutionen werden beispielsweise Datenbanken für die Inventarisierung, das Konfigurationsmanagement oder die Gestaltung von Geschäftsprozessen betrieben. Dadurch können sich Synergien ergeben.

Die Strukturanalyse gliedert sich in folgende Teilaufgaben:

- Erfassung der zum Geltungsbereich zugehörigen Geschäftsprozesse, Anwendungen und Informationen
- Netzplanerhebung
- Erhebung von IT-, ICS- und IoT-Systemen und ähnlichen Objekten
- Erfassung der Räume und Gebäude (für den ICS-Bereich sind auch die produzierenden Räumlichkeiten zu berücksichtigen)

Bei allen Teilaufgaben ist zu beachten, dass es häufig nicht zweckmäßig ist, jedes Objekt einzeln zu erfassen. Stattdessen sollten ähnliche Objekte zu Gruppen zusammengefasst werden.

8.1.1 Komplexitätsreduktion durch Gruppenbildung

Die Strukturanalyse liefert wichtige Grunddaten für den gesamten Sicherheitsprozess. Der Informationsverbund setzt sich meist aus vielen Einzelobjekten zusammen, die bei der Konzeption berücksichtigt werden müssen. Wenn alle logischen und technischen Objekte einzeln erfasst werden, besteht jedoch die Gefahr, dass die Ergebnisse der Strukturanalyse aufgrund der Datenmenge und der Komplexität nicht handhabbar sind. Ähnliche Objekte sollten deshalb sinnvoll zu Gruppen zusammengefasst werden.

Bei technischen Komponenten hat eine konsequente Gruppenbildung zudem den Vorteil, dass die Administration wesentlich vereinfacht wird, wenn es nur wenige Grundkonfigurationen gibt. Durch eine möglichst hohe Standardisierung innerhalb eines Informationsverbunds wird außerdem die Zahl potenzieller Sicherheitslücken reduziert und die Sicherheitsmaßnahmen für diesen Bereich können ohne Unterscheidung verschiedenster Schwachstellen umgesetzt werden. Dies kommt nicht nur der Informationssicherheit zugute, sondern spart auch Kosten.

Objekte können dann ein und derselben Gruppe zugeordnet werden, wenn die Objekte alle

- vom gleichen Typ sind,
- ähnliche Aufgaben haben,
- ähnlichen Rahmenbedingungen unterliegen und
- den gleichen Schutzbedarf aufweisen.

Bei technischen Objekten bietet sich eine Gruppenbildung außerdem immer dann an, wenn sie

- ähnlich konfiguriert sind,

- ähnlich in das Netz eingebunden sind (z. B. im gleichen Netzsegment) und
- ähnlichen administrativen und infrastrukturellen Rahmenbedingungen unterliegen,
- ähnliche Anwendungen bedienen und
- den gleichen Schutzbedarf aufweisen.

Aufgrund der genannten Voraussetzungen für die Gruppenbildung kann bezüglich der Informationssicherheit davon ausgegangen werden, dass eine Stichprobe aus einer Gruppe in der Regel den Sicherheitszustand der Gruppe repräsentiert.

Wichtigstes Beispiel für die Gruppierung von Objekten ist sicherlich die Zusammenfassung von Clients. In der Regel gibt es in einer Institution eine große Anzahl von Clients, die sich jedoch gemäß obigem Schema in eine überschaubare Anzahl von Gruppen aufteilen lassen. Auch in produzierenden und gewerblichen Bereichen ist es empfehlenswert, Objekte zu gruppieren, wenn diese vergleichbar konfiguriert und eingesetzt werden (z. B. Handscanner, Arbeitsplatz-PCs). Dies gilt analog auch für Räume und andere Objekte. In großen Informationsverbünden, wo aus Gründen der Redundanz oder des Durchsatzes viele Server die gleiche Aufgabe wahrnehmen, können durchaus auch Server zu Gruppen zusammengefasst werden.

Zunehmend werden IT-Systeme virtualisiert. Da hierbei typischerweise viele virtuelle Maschinen (VMs) auf einem Virtualisierungsserver betrieben werden, ist eine sinnvolle Strukturanalyse bei virtualisierten Infrastrukturen oder Cloud Computing nur durch geeignete Gruppenbildung möglich. Für die Gruppenbildung gelten bei Virtualisierung dieselben Regeln wie für physische Zielobjekte. Prinzipiell können auch solche VMs zu einer Gruppe zusammengefasst werden, die auf verschiedenen physischen IT-Systemen laufen, wenn sie ähnliche Aufgaben erfüllen, gleichartig konfiguriert sind und denselben Schutzbedarf aufweisen.

In der Regel bestehen Cloud Computing-Plattformen aus homogenen Hard- und Software-Komponenten. Aufgrund der Homogenität kann eine Vielzahl von Aufgaben automatisiert und zentral durchgeführt werden. Eine Gruppenbildung, beispielsweise anhand des Schutzbedarfs, ist beim Cloud Computing zwingend erforderlich.

Die Teilaufgaben der Strukturanalyse werden nachfolgend beschrieben und durch ein begleitendes Beispiel erläutert. Eine ausführliche Version des Beispiels findet sich in den Hilfsmitteln zum IT-Grundschutz auf den einzelnen Webseiten bzw. auf der BSI-Website. Bei allen Teilaufgaben sollten jeweils Objekte zu Gruppen zusammengefasst werden, wenn dies sinnvoll und zulässig ist.

Aktionspunkte zu 8.1.1 Komplexitätsreduktion durch Gruppenbildung
• Bei allen Teilaufgaben der Strukturanalyse gleichartige Objekte zu Gruppen zusammenfassen
• Typ und Anzahl der jeweils zusammengefassten Objekte vermerken

8.1.2 Erfassung der Geschäftsprozesse und der zugehörigen Informationen

Eine der Hauptaufgaben des Sicherheitsmanagements ist es, der Leitungsebene die Informationssicherheitsrisiken aufzuzeigen und damit Transparenz zu schaffen, wo Entscheidungs- oder Handlungsbedarf erforderlich ist. Hierzu muss sich der ISB einen Überblick über die für die Institution wesentlichen Geschäftsprozesse bzw. Fachaufgaben verschaffen und darstellen, was Informationssicherheitsrisiken bzw. IT-Risiken für diese Geschäftsprozesse bedeuten.

Somit erscheint es sinnvoll, einen Bezug zwischen den Geschäftsprozessen und der Wertschöpfung einer Institution und den zu schützenden Informationen sowie der verwendeten IT bzw. den verwendeten Anwendungen herzustellen. Hierfür müssen die Geschäftsprozesse und deren Abhängigkeit von den wichtigsten Anwendungen dokumentiert werden.

Auf Basis des definierten Informationsverbunds sind in einem ersten Schritt die dort enthaltenen zentralen Geschäftsprozesse oder Fachaufgaben zu erfassen und zu dokumentieren. Hierbei ist darauf zu achten, dass eine sinnvolle Granularität gewählt wird. Dies bedeutet, dass nicht nur ein einzelner Hauptprozess, wie z. B. das Personalmanagement, sondern auch die zugehörigen wichtigsten Subprozesse, wie z. B. Personalgewinnung, Mitarbeiterverwaltung, Personalentwicklung usw. erfasst werden, sofern diese Bestandteil des Informationsverbunds sind. Eine zu detaillierte Dokumentation z. B. durch eine Auflistung von nachgelagerten Prozessen sollte jedoch vermieden werden. Auch im ICS-Bereich müssen für die Strukturanalyse die Geschäftsprozesse mit den zugehörigen Informationen erfasst werden. Hier ist insbesondere darauf zu achten, dass neben dem Kernprozess der Produktion auch weitere Nebenprozesse, wie z. B. die logistischen Prozesse für den Warenfluss und die Instandhaltung, berücksichtigt werden.

Die einzelnen Prozesse sind wie folgt zu erfassen:

- eindeutiger Bezeichner
- Name
- Prozessverantwortlicher/Fachabteilung
- kurze Beschreibungen des Prozesses oder der Fachaufgabe und der dort verarbeiteten Informationen
- wichtige, für den Prozess benötigte Anwendung(en)

Um die wesentlichen Geschäftsprozesse zu identifizieren, kann in vielen Institutionen auf bestehende Prozesslandkarten zurückgegriffen werden. Wenn die Geschäftsprozesse noch nicht, nicht durchgängig oder nicht aktuell erfasst wurden, sollten zunächst Geschäftsverteilungspläne, Aufgabenbeschreibungen oder andere organisationsbeschreibende Papiere ausgewertet werden, um die relevanten Geschäftsprozesse zu identifizieren. Daneben kann das Verfahrensverzeichnis des Datenschutzbeauftragten ein weiterer Startpunkt für die Erfassung der Prozesse, Fachaufgaben und nachfolgenden Anwendungen sein, auch wenn dies lediglich die Verfahren und Anwendungen abbildet, die personenbezogene Daten verarbeiten. Sollten noch keine Prozessbeschreibungen vorliegen, sind kurze Workshops oder Interviews mit den Fachverantwortlichen zu empfehlen.

Es kann durchaus sinnvoll sein, die Erhebung der Prozesse und Fachaufgaben mit der Erhebung der Anwendungen zu koppeln, um damit redundante Fragen insbesondere in den Fachabteilungen zu vermeiden.

Aktionspunkte zu 8.1.2 Erfassung der Geschäftsprozesse und der zugehörigen Informationen
• Überblick über die Geschäftsprozesse erstellen
• Geschäftsprozesse mit eindeutigen Nummern oder Kürzeln kennzeichnen
• Zusammenhang zwischen Geschäftsprozessen und Anwendungen darstellen

8.1.3 Erfassung der Anwendungen und der zugehörigen Informationen

Ausgehend von jedem Geschäftsprozess bzw. jeder Fachaufgabe, die im Informationsverbund enthalten ist, müssen in dieser Phase die damit zusammenhängenden Anwendungen und die damit verarbeiteten Informationen identifiziert werden. Anwendungen dienen der IT-technischen Unterstützung von Geschäftsprozessen und Fachaufgaben in Behörden und Unternehmen.

Die geeignete Granularität für die betrachteten Anwendungen muss in jeder Institution individuell gewählt werden. Ziel sollte dabei sein, eine optimale Transparenz und Effizienz bei der Strukturanalyse und der Schutzbedarfsfeststellung zu erreichen. Auch die im IT-Grundschutz-Kompendium betrachteten Bausteine aus der Schicht der Anwendungen können für diesen Schritt Aufschluss geben.

Zur weiteren Reduzierung des Aufwands kann die Strukturanalyse des Informationsverbunds auf die Anwendungen und Informationen beschränkt werden, die für die betrachteten Geschäftsprozesse oder Fachaufgaben erforderlich sind. Dabei sollte darauf geachtet werden, dass zumindest diejenigen Anwendungen und Informationen berücksichtigt werden, die aufgrund der Anforderungen der betrachteten Geschäftsprozesse oder Fachaufgaben ein Mindestniveau an

- Geheimhaltung (Vertraulichkeit) oder
- Korrektheit und Unverfälschtheit (Integrität) oder
- Verfügbarkeit

erfordern.

Bei der Erfassung der Anwendungen sollten auch die Benutzer bzw. die für die Anwendung Verantwortlichen sowie die für den Geschäftsprozess Verantwortlichen befragt werden, wie sie das erforderliche Sicherheitsniveau einschätzen.

Aufgrund der steigenden Komplexität von Anwendungen ist es jedoch oft für die Fachverantwortlichen nicht klar, welche Abhängigkeiten zwischen einem Geschäftsprozess oder einer Fachaufgabe zu einer konkreten Anwendung bestehen. Es sollte also für jede einzelne Fachaufgabe festgestellt werden, welche Anwendungen für ihre Abwicklung notwendig sind und auf welche Daten dabei zugegriffen wird. In einer gemeinsamen Sitzung der Fachabteilung, der Verantwortlichen der einzelnen Anwendungen und der unterstützenden IT-Abteilung können diese Abhängigkeiten erfasst werden. Beispielsweise können Bestellungen nicht abschließend bearbeitet werden, wenn keine Informationen über den Lagerbestand zur Verfügung stehen.

Falls abweichend von der hier vorgeschlagenen Reihenfolge zuerst die IT-Systeme erfasst wurden, ist es häufig hilfreich, die Anwendungen an erster Stelle orientiert an den IT-Systemen zusammenzutragen. Aufgrund ihrer Breitenwirkung sollte dabei mit den Servern begonnen werden. Um ein möglichst ausgewogenes Bild zu bekommen, kann anschließend diese Erhebung aufseiten der Clients und Einzelplatz-Systeme vervollständigt werden. Abschließend sollte noch festgestellt werden, welche Netzkoppelelemente welche Anwendungen unterstützen. Für die Erfassung der Anwendungen auf einem Standard-Client hat sich in der Praxis bewährt, seitens der unterstützenden IT-Abteilung die Standard-Software der Clients als Paket zu betrachten. So wird die Standard-Software nicht vergessen. Oftmals wird diese als selbstverständlich angesehen und deren Anwendung wird in Interviews nicht mehr explizit genannt (z. B. die E-Mail-Anwendung oder Bürokommunikation).

Ausgehend von den Anwendungen können die zugehörigen Geschäftsprozesse auch im Nachgang erfasst werden (siehe Kapitel 8.1.2). Der Verantwortliche und die Benutzer der Anwendung sollten ebenfalls erfasst werden, um Ansprechpartner für Sicherheitsfragen leichter identifizieren bzw. betroffene Benutzergruppen schnell erreichen zu können.

Bei der Erfassung der Anwendungen ist es empfehlenswert, auch Datenträger und Dokumente zu betrachten und diese ähnlich wie Anwendungen zu behandeln. Sofern sie nicht fest mit einer Anwendung oder einem IT-System verknüpft sind, müssen Datenträger und Dokumente gesondert in die Strukturanalyse integriert werden. Natürlich ist es dabei nicht zweckmäßig, alle Datenträger einzeln zu erfassen. Zum einen sollten nur Datenträger und Dokumente mit einem Mindestschutzbedarf betrachtet und zum anderen sollten möglichst Gruppen gebildet werden. Beispiele für Datenträger und Dokumente, die im Rahmen der Strukturanalyse gesondert erfasst werden sollten, sind

- Archiv- und Back-up-Datenträger,
- Datenträger für den Austausch mit externen Kommunikationspartnern,
- Massenspeicher für den mobilen Einsatz (z. B. USB-Sticks oder externe Festplatten),
- Notfallhandbücher, die in ausgedruckter Form vorgehalten werden,
- Mikrofilme,
- wichtige Verträge mit Partnern und Kunden.

Es darf nicht vergessen werden, virtualisierte Anwendungen im Rahmen der Strukturanalyse mit zu erfassen.

Zur Dokumentation der Ergebnisse bietet sich die Darstellung in tabellarischer Form oder die Nutzung entsprechender Software-Produkte an.

Beispiel: RECPLAST GmbH

Im Folgenden wird anhand einer fiktiven Institution, der RECPLAST GmbH, beispielhaft dargestellt, wie die erfassten Anwendungen dokumentiert werden können. Zu beachten ist, dass die Struktur der RECPLAST GmbH im Hinblick auf die Informationssicherheit keineswegs optimal ist. Sie dient lediglich dazu, die Vorgehensweise bei der Anwendung des IT-Grundschutzes zu illustrieren. In diesem Dokument werden anhand der RECPLAST GmbH die einzelnen Aktivitäten zur Erstellung einer Sicherheitskonzeption erläutert. Das komplette Beispiel findet sich unter den Hilfsmitteln zum IT-Grundschutz.

Die RECPLAST GmbH ist eine fiktive Institution mit ca. 500 Mitarbeitern, von denen 130 an Bildschirmarbeitsplätzen arbeiten. Räumlich ist die RECPLAST GmbH aufgeteilt in zwei Standorte innerhalb Bonns, wo unter anderem die administrativen und produzierenden Aufgaben wahrgenommen werden, und drei Vertriebsstandorte in Deutschland.

Um die Geschäftsprozesse zu optimieren, sind alle Arbeitsplätze vernetzt worden. Die Außenstelle in Bonn ist über eine angemietete Standleitung an die Zentrale angebunden. Die Vertriebsstandorte sind mit abgesicherten Verbindungen über das Internet an die Zentrale angebunden. Alle für die Aufgabenerfüllung und die Informationssicherheit wesentlichen Richtlinien und Vorschriften sowie Formulare und Textbausteine sind ständig für jeden Mitarbeiter über das Intranet abrufbar. Alle relevanten Arbeitsergebnisse werden in eine zentrale Datenbank eingestellt. Entwürfe werden ausschließlich elektronisch erstellt, weitergeleitet und unterschrieben. Die Realisierung und Betreuung aller benötigten Funktionalitäten übernimmt eine IT-Abteilung in Bonn.

Die Geschäftsprozesse der RECPLAST werden elektronisch gepflegt und sind nach einem zweistufigen Schema benannt. Hinter dem Kürzel GP wird die Nummer des Hauptprozesses angegeben, zum Beispiel GP002. Ein Geschäftsprozess sollte immer beschrieben werden, damit ein einheitliches Verständnis für die Abgrenzung eines Prozesses vorhanden ist. Optional kann eine Prozessart erfasst werden. Diese dient lediglich zur Übersicht, welche Prozesse für eine Institution hauptsächlich zum Fortbestand beitragen. Die Unterstützungsprozesse sind jedoch ebenso wichtig, diese sind jedoch eher für den allgemeinen Betrieb einer Institution erforderlich.

Nachfolgend ist ein Auszug aus der Erfassung der Geschäftsprozesse und der dazugehörigen Informationen für die RECPLAST GmbH abgebildet:

A.1 Geschäftsprozesse der RECPLAST GmbH				
Bezeichnung	**Beschreibung des Prozesses**	**Prozess-Art**	**Prozessverant-wortlicher**	**Mitarbeiter**
GP001	**Produktion:** Die Produktion der Kunststoffartikel umfasst alle Phasen von der Materialbereitstellung bis hin zur Einlagerung des produzierten Materials. Hierzu gehören innerhalb der Produktion die internen Transportwege, die Produktion und Fertigung der verschiedenen Komponenten und das Verpacken der Teile.	Kerngeschäft	Leiter Produktion	Alle Mitarbeiter
GP002	**Angebotswesen:** In der Angebotsabwicklung werden die Kundenanfragen für Produkte verarbeitet. Im Regelfall werden Kundenanfragen formlos per E-Mail oder Fax geschickt. Die Angebote werden elektronisch erfasst und ein schriftliches Angebot per Post an den Kunden versendet.	Unterstützender Prozess	Leiter Angebotswesen	Vertrieb
GP003	**Auftragsabwicklung:** Kunden schicken die Bestellungen im Regelfall per Fax oder E-Mail. Alle Belege müssen ausgedruckt und elektronisch erfasst werden. Eine Auftragsbestätigung erhält der Kunde nur, wenn er dies ausdrücklich wünscht oder der Produktionsprozess von der üblichen Produktionszeit abweicht.	Kerngeschäft	Leiter Auftrags-abwicklung	Vertrieb
GP004	**Einkaufsabteilung:** In der Einkaufsabteilung werden alle erforderlichen Artikel bestellt, die nicht für den Produktionsprozess erforderlich sind. In dieser Abteilung werden externe Projekte verhandelt, IT-Verträge gestaltet und Verbrauchsmaterial im organisatorischen Umfeld (Papier, Toner, etc.) beschafft.	Unterstützender Prozess	Leiter Einkaufsabteilung	Einkauf

A.1 Geschäftsprozesse der RECPLAST GmbH				
Bezeichnung	**Beschreibung des Prozesses**	**Prozess-Art**	**Prozessverant-wortlicher**	**Mitarbeiter**
GP005	**Disposition:** In der Disposition werden alle für die Produktion benötigten Materialien (Kunststoffe, Schrauben, Tüten, etc.) beschafft. Hierzu liegen normalerweise Rahmenverträge vor. Geplant wird in diesem Umfeld anhand von Jahresplanmengen und verschiedenen Bestellwerten.	Kerngeschäft	Leiter Disposition	Disposition, Produktion

Abbildung 12: Auszug aus den Geschäftsprozessen der RECPLAST GmbH

Strukturanalyse der Anwendungen

Der zuständige Informationssicherheitsbeauftragte der RECPLAST GmbH erfasst in der Strukturanalyse neben den Geschäftsprozessen auch alle weiteren Objekte, die zur Institution selbst gehören. Dazu zählen auch die Anwendungen, die zur Aufrechterhaltung der bereits erfassten Geschäftsprozesse benötigt werden.

Nachfolgend wird ein Auszug aus der Erfassung der Anwendungen und der zugehörigen Informationen für das fiktive Beispiel RECPLAST dargestellt:

A.1 Strukturanalyse der RECPLAST GmbH									
Bezeichnung	**Beschreibung des Zielobjektes / der Gruppe der Zielobjekte**	**Plattform / Baustein**	**Ort**	**Gebäude**	**Raum**	**Anzahl**	**Status**	**Benutzer**	**Verantwortlich / Administrator**
A003	**Textverarbeitung, Tabellenkalkulation:** Alle geschäftlichen Informationen werden in einem Office-Produkt verarbeitet, Geschäftsbriefe, Analysen oder Präsentationen	Office-Produkt 2010	-	-	-	130	in Betrieb	Alle Mitarbeiter	IT-Betrieb
A004	**Chat-Anwendung:** Eine Chat-Anwendung soll den Kontakt zwischen den Mitarbeitern vereinfachen. Die E-Mails werden standardmäßig nur zwei Mal pro Tag abgerufen. Diese Anwendung wird als virtualisierte Anwendung eingesetzt.	Standardsoftware	-	-	-	130	in Betrieb	Alle Mitarbeiter	IT-Betrieb
A008	**Active Directory:** Diese Anwendung soll dem IT-Betrieb die Arbeit erleichtern und doppelte Benutzereingaben reduzieren.	Active Directory	Bonn	BG	Büro	5	Test	Administratoren	IT-Betrieb

Abbildung 13: Auszug aus der Strukturanalyse der RECPLAST GmbH (Anwendungen)

Der Zusammenhang zwischen den Geschäftsprozessen und den Anwendungen muss immer dargestellt werden. Diese Zuordnung sollte idealerweise mit Tools durchgeführt werden, um bei der üblichen Vielzahl von Prozessen und Anwendungen die Übersichtlichkeit und Aktualität zu gewährleisten.

Am Beispiel der RECPLAST GmbH wird nachfolgend dargestellt, dass für einen Prozess normalerweise mehrere Anwendungen eingesetzt werden:

A.1 Zuordnungen Geschäftsprozesse zu Anwendungen der RECPLAST GmbH

Geschäftsprozess / Anwendung	A001	A002	A003	A004	A005	A006	A007	A008	A009	A010
GP001	x					x	x			x
GP002					x	x	x		x	
GP003					x	x	x		x	
GP004			x	x		x	x	x	x	
GP005			x			x	x	x	x	

Abbildung 14: Zuordnung der Geschäftsprozesse zu den Anwendungen der RECPLAST GmbH

Aktionspunkte zu 8.1.3 Erfassung der Anwendungen und der zugehörigen Informationen

- Unter Einbeziehung der Verantwortlichen bzw. der Nutzer der Anwendungen herausfinden, welche Anwendungen für die betrachteten Geschäftsprozesse erforderlich sind
- Übersicht über die Anwendungen erstellen und mit eindeutigen Nummern oder Kürzeln kennzeichnen

8.1.4 Netzplanerhebung

Einen geeigneten Ausgangspunkt für die weitere technische Analyse stellt ein Netzplan (beispielsweise in Form eines Netztopologieplans) dar. Ein Netzplan ist eine grafische Übersicht über die im betrachteten Bereich der Informations- und Kommunikationstechnik eingesetzten Komponenten und deren Vernetzung. Netzpläne oder ähnliche grafische Übersichten sind auch aus betrieblichen Gründen in den meisten Institutionen vorhanden. Im Einzelnen sollte der Plan in Bezug auf die Informationssicherheit mindestens folgende Objekte darstellen:

- IT-Systeme, d.h. Client- und Server-Computer, aktive Netzkomponenten (wie Switches, Router, WLAN Access Points), Netzdrucker usw.
- ICS- und IoT-Komponenten mit Netzanschluss, d. h. Clients, Handscanner, Industriedrucker, Geräte mit speicherprogrammierbarer Steuerung (SPS), Schaltschränke usw.
- Netzverbindungen zwischen diesen Systemen, d. h. LAN-Verbindungen (wie Ethernet), WLAN, Backbone-Techniken (wie ATM) usw.
- Verbindungen des betrachteten Bereichs nach außen, d. h. Einwahlzugänge über ISDN oder Modem, Internetanbindungen über analoge Techniken oder Router, Funkstrecken oder Mietleitungen zu entfernten Gebäuden oder Liegenschaften usw.

Zu jedem der dargestellten Objekte gehört weiterhin ein Minimalsatz von Informationen, die einem zugeordneten Katalog zu entnehmen sind. Für jedes IT-System und sonstige Geräte sollten zumindest

- eine eindeutige Bezeichnung (beispielsweise der vollständige Hostname oder eine Identifikationsnummer),
- Typ und Funktion (beispielsweise Datenbank-Server für Anwendung X),
- die zugrunde liegende Plattform (d. h. Hardware-Plattform und Betriebssystem),
- der Standort (beispielsweise Gebäude- und Raumnummer),
- der zuständige Administrator,
- die vorhandenen Kommunikationsschnittstellen (z. B. Internetanschluss, Bluetooth, WLAN Adapter) sowie
- die Art der Netzanbindung und die Netzadresse

vermerkt sein. Bei Außenanbindungen oder drahtlosen Kommunikationsverbindungen (WLAN, UMTS, LTE,...) sollten zusätzlich Details zum externen Netz (z. B. Internet, Geschäftspartner, Name des Providers für die Datenübertragung sowie die Art der Leitung, z. B. MPLS, Leased Line, VPN) aufgenommen werden.

Virtuelle IT-Systeme (virtuelle Switches, virtuelle Server usw.) und virtuelle Netzverbindungen, beispielsweise virtuelle LANs (VLANs) oder virtuelle private Netze (VPNs), sollten ebenfalls in einem Netzplan dargestellt werden. Hierbei sind virtuelle IT-Systeme gemäß ihrem Typ und Einsatzzweck genauso wie physische IT-Systeme zu behandeln. Darüber hinaus muss die Zuordnung von virtuellen IT-Systemen zu physischen Host-Systemen nachvollziehbar sein. Um die Übersichtlichkeit zu verbessern, ist es bei zunehmender Größe eines Netzes sinnvoll, den Netzplan in mehrere Teilnetzpläne aufzuteilen.

Eine Cloud-Infrastruktur setzt sich aus einer Vielzahl von Elementen zusammen. Neben den physischen (mit CPU, Arbeitsspeicher und anderer Hardware) und gegebenenfalls virtuellen Servern zählen noch Netze und Speicherlösungen dazu. Die aufgezählten Bereiche verfügen in der Regel über eine Verwaltungssoftware.

Für den Bereich „Netze" sollten die eingesetzten Netzmanagement-Tools eine automatische Erzeugung von Netzplänen unterstützen. Neben physischen sollten auch virtuelle IT-Systeme (z. B. virtuelle Switches, virtuelle Router, virtuelle Sicherheitsgateways) automatisch abgebildet werden können.

Der ICS-Bereich kann als eigenständiges Netz betrieben werden. Bei der Erfassung der Netzverbindungen sollten dabei auch die Schnittstellen erfasst werden (Auflistung der erlaubten und gesperrten Schnittstellen). Auch die Internetanbindung aus dem ICS-Bereich heraus sollte erfasst werden. Die Trennung der Netze zwischen dem Office-Bereich und dem ICS-Bereich sollte im Netzplan dargestellt werden.

Es empfiehlt sich, Bereiche mit unterschiedlichem Schutzbedarf zu kennzeichnen. Der Netzplan sollte möglichst in elektronischer Form erstellt und gepflegt werden. Hat die Informationstechnik in der Institution einen gewissen Umfang überschritten, bietet es sich an, bei der Erfassung und Pflege des Netzplans auf geeignete Hilfsprogramme zurückzugreifen, da die Unterlagen eine erhebliche Komplexität aufweisen können und einem ständigen Wandel unterzogen sind.

Aktualisierung des Netzplans

Da die IT-Struktur in der Regel ständig an die Anforderungen der Institution angepasst wird und die Pflege des Netzplans entsprechende Ressourcen bindet, ist der Netzplan der Institution nicht immer

auf dem aktuellen Stand. Vielmehr werden in der Praxis oftmals nur größere Änderungen an der IT-Struktur einzelner Bereiche zum Anlass genommen, den Plan zu aktualisieren.

Im Hinblick auf die Verwendung des Netzplans für die Strukturanalyse besteht demnach der nächste Schritt darin, den vorliegenden Netzplan (bzw. die Teilpläne, wenn der Gesamtplan aus Gründen der Übersichtlichkeit aufgeteilt wurde) mit der tatsächlich vorhandenen IT-Struktur abzugleichen und gegebenenfalls auf den neuesten Stand zu bringen. Hierzu sind die IT-Verantwortlichen und Administratoren der einzelnen Anwendungen und Netze zu konsultieren. Falls Programme für ein zentralisiertes Netz- und Systemmanagement eingesetzt werden, sollte auf jeden Fall geprüft werden, ob diese Programme bei der Erstellung eines Netzplans Unterstützung anbieten. Zu beachten ist jedoch, dass Funktionen zur automatischen oder halbautomatischen Erkennung von Komponenten temporär zusätzlichen Netzverkehr erzeugen. Es muss sichergestellt sein, dass dieser Netzverkehr nicht zu Beeinträchtigungen des IT-Betriebs führt. Ebenso sollte das Ergebnis von automatischen bzw. halbautomatischen Erkennungen stets dahingehend geprüft werden, ob wirklich alle relevanten Komponenten ermittelt wurden.

Der Bereich der industriellen Steuerung sollte ebenfalls in den Netzplan integriert werden. Ansprechpartner sind neben den IT-Verantwortlichen und Administratoren auch die Mitarbeiter der Haustechnik.

Ein bereinigter Netzplan ist auch an anderen Stellen hilfreich. So kann dieser genutzt werden, um Dritten schnell die Geschäftsprozess- und IT-Strukturen innerhalb der Institution darzustellen, da in einem bereinigten Netzplan der Detaillierungsgrad auf das notwendige Maß reduziert wird. Auch für eine Zertifizierung ist ein bereinigter Netzplan eine sinnvolle Grundlage.

Beispiel: RECPLAST GmbH

Die Netzpläne in der RECPLAST GmbH werden in der IT-Abteilung mit einem Tool verwaltet. Die Darstellung aller Netzpläne ist sehr detailliert und oftmals für Dritte sehr unübersichtlich. Die RECPLAST GmbH nutzt deshalb für die Darstellung der erfassten Zielobjekte einen bereinigten Netzplan.

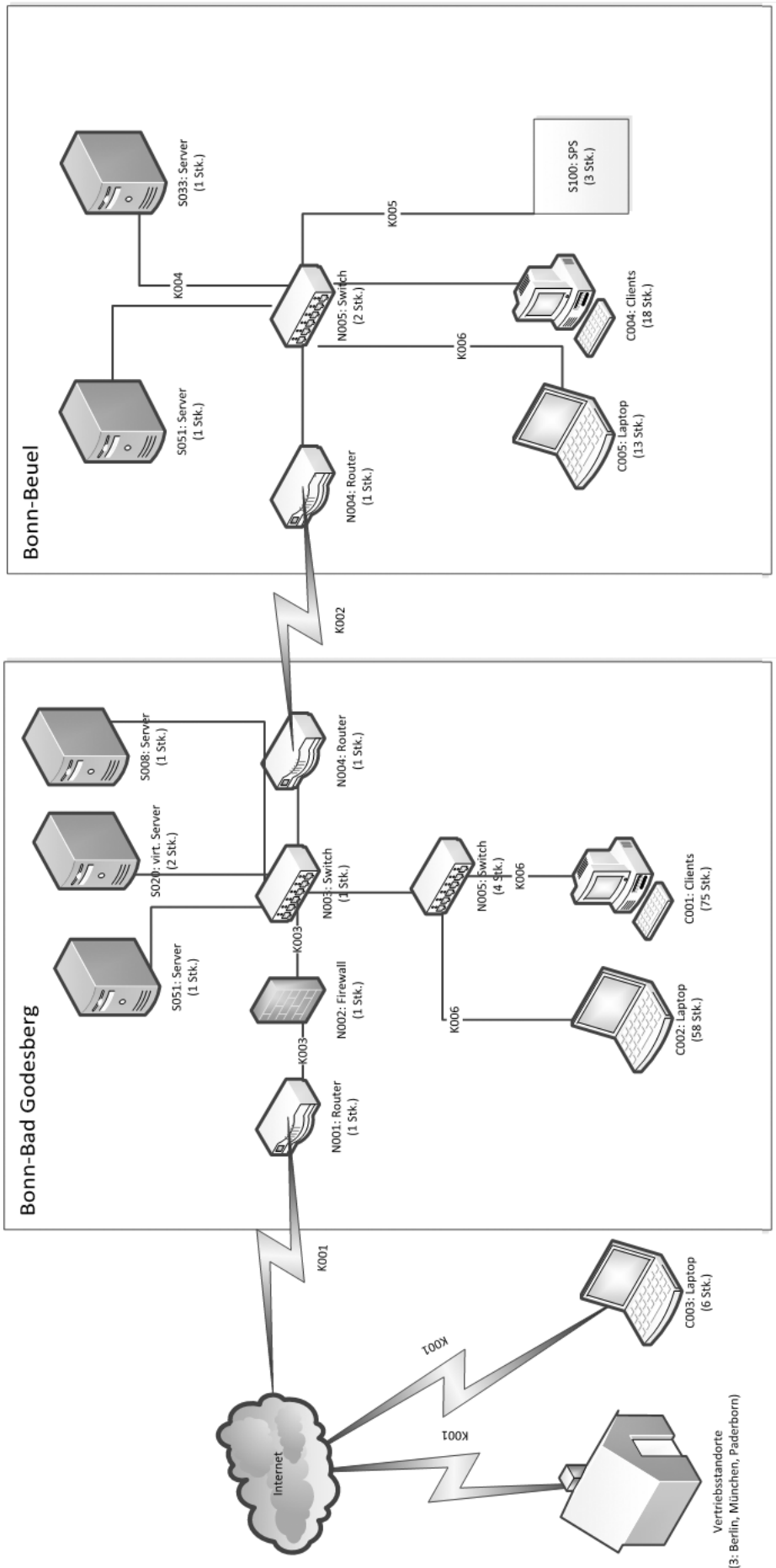


Abbildung 15: Auszug aus dem bereinigten Netzplan der RECPLAST GmbH (Teilausschnitt)

Aktionspunkte zu 8.1.4 Netzplanerhebung
• Existierende grafische Darstellungen des Netzes, beispielsweise Netztopologiepläne, sichten • Netzpläne gegebenenfalls aktualisieren oder neu erstellen • Existierende Zusatzinformationen über die enthaltenen IT-, ICS- und IoT-Systeme sichten und gegebenenfalls aktualisieren und vervollständigen • Existierende Zusatzinformationen über die enthaltenen Kommunikationsverbindungen sichten und gegebenenfalls aktualisieren und vervollständigen

8.1.5 Erhebung der IT-Systeme

Im Hinblick auf die später durchzuführende Schutzbedarfsfeststellung und Modellierung des Informationsverbunds sollte eine Liste der vorhandenen und geplanten IT-Systeme in tabellarischer Form aufgestellt werden. Der Begriff IT-System umfasst dabei nicht nur Computer im engeren Sinn, sondern auch die IoT- und ICS-Geräte, aktive Netzkomponenten, Netzdrucker, TK-Anlagen, Smartphones, virtuelle IT-Systeme usw. Die technische Realisierung eines IT-Systems steht im Vordergrund, beispielsweise Apple MacBook, Client unter Windows, Linux-Server, TK-Anlage usw. An dieser Stelle sollen nur die Systeme als solche erfasst werden (z. B. Linux-Server), nicht die einzelnen Bestandteile, aus denen die IT-Systeme zusammengesetzt sind (also nicht Rechner, Tastatur, Bildschirm usw.).

Hinweis:

Für einen ordnungsmäßigen IT-Betrieb ist eine vollständige und korrekte Erfassung der vorhandenen und geplanten IT-Systeme notwendig, beispielsweise für die Überprüfung, Wartung, Fehlersuche und Instandsetzung von IT-Systemen. Für die Erstellung eines Sicherheitskonzepts reicht es, sich einen Überblick über die gruppierten IT-Systeme zu verschaffen.

Zu erfassen sind sowohl die vernetzten als auch die nicht vernetzten IT-Systeme, insbesondere also auch solche, die nicht im zuvor betrachteten Netzplan aufgeführt sind. IT-Systeme, die im Netzplan zu einer Gruppe zusammengefasst worden sind, können weiterhin als ein Objekt behandelt werden. Auch bei den IT-Systemen, die nicht im Netzplan aufgeführt sind, ist zu prüfen, ob sie sinnvoll zusammengefasst werden können. Möglich ist dies beispielsweise bei einer größeren Anzahl von nicht vernetzten Einzelplatz-PCs, die die im Kapitel 8.1.1 *Komplexitätsreduktion durch Gruppenbildung* genannten Bedingungen für eine Gruppierung erfüllen.

Bei dieser Erfassung sollten folgende Informationen vermerkt werden, die für die nachfolgende Arbeit nützlich sind:

- eine eindeutige Bezeichnung der IT-Systeme bzw. der jeweiligen Gruppe (bei Gruppen sollte auch die Anzahl der zusammengefassten IT-Systeme vermerkt sein),
- Beschreibung (z. B. Funktion, Typ),
- Plattform (z. B. Hardware-Architektur/Betriebssystem),
- Aufstellungsort der IT-Systeme (z. B. Ort, Gebäude, Raum),
- Status der IT-Systeme (in Betrieb, im Test, in Planung) und
- Benutzer bzw. Administratoren der IT-Systeme.

Anschließend werden die Anwendungen jeweils denjenigen IT-Systemen zugeordnet, die für deren Ausführung benötigt werden. Dies können die IT-Systeme sein, auf denen die Anwendungen verarbeitet werden, oder auch diejenigen, die Daten dieser Anwendungen transferieren. Das Ergebnis ist eine Übersicht, in der die Zusammenhänge zwischen den wichtigen Anwendungen und den entsprechenden IT-Systemen dargestellt werden.

Beispiel: RECPLAST GmbH

A.1 Strukturanalyse der RECPLAST GmbH									
Bezeichnung	**Beschreibung des Zielobjektes / der Gruppe der Zielobjekte**	**Plattform / Baustein**	**Ort**	**Gebäude**	**Raum**	**Anzahl**	**Status**	**Benutzer**	**Verantwortlich / Administrator**
N001	**Router Internetanbindung:** Dieser Router regelt die Kommunikation zwischen dem Internet und den internen Prozessen	Router und Switches	Bonn	BG	Serverraum	1	in Betrieb	Administratoren	IT-Betrieb
N002	**Firewall Internet-Eingang:** Diese Firewall dient als Schutz zwischen dem Internet und dem internen Netz	Firewall	Bonn	BG	Serverraum	1	in Betrieb	Administratoren	IT-Betrieb
N003	**Switch – Verteilung** Der Datenfluss in Richtung Internet und internes Netz wird über den Switch gesteuert	Router und Switches	Bonn	BG	Serverraum	1	in Betrieb	Administratoren	IT-Betrieb
N004	**Router Bonn BG – Beuel** Über eine Standleitung sind die beiden Standorte in Bonn verbunden. Diese Router sichern die Verbindung ab.	Router und Switches	Bonn	-	Serverraum	2	in Betrieb	Administratoren	IT-Betrieb
S008	**Print-Server:** Server für die Druckerdienste, die zentral gesteuert werden.	Windows Server 2012	Bonn	BG	Serverraum	1	in Betrieb	Alle Mitarbeiter	IT-Betrieb

A.1 Strukturanalyse der RECPLAST GmbH									
Bezeichnung	**Beschreibung des Zielobjektes / der Gruppe der Zielobjekte**	**Plattform / Baustein**	**Ort**	**Gebäude**	**Raum**	**Anzahl**	**Status**	**Benutzer**	**Verantwortlich / Administrator**
S020	**Virtueller Server (Konfiguration 1):** Auf dem Server können bis zu 20 virtuelle Server konfiguriert werden. Für die Verwaltung der virtualisierten Systeme wird eine Anwendung eingesetzt.	Server unter Unix	Bonn	BG	Serverraum	2	in Betrieb	Administratoren	IT-Betrieb
S033	**Server Produktion:** Die zentralen Daten für die Produktion werden auf diesem Server verarbeitet.	Server unter Unix	Bonn	Beuel	Serverraum	1	in Betrieb	Mitarbeiter Produktion	IT-Betrieb

Abbildung 16: Auszug aus der Strukturanalyse der RECPLAST GmbH (IT-Systeme)

Für die Zuordnung der Anwendungen zu den IT-Systemen setzt die RECPLAST GmbH ein Tool ein, da die Pflege in Form einer Tabelle aufwendig ist. Jede Änderung, sei es ein IT-System oder eine Anwendung, muss immer dokumentiert werden. Diese Zuordnung ist für die später folgende Schutzbedarfsfeststellung erforderlich.

8.1.6 Erhebung der ICS-Systeme

In Institutionen mit Produktion und Fertigung müssen auch die industriellen Steuerungssysteme (ICS), die von der Institution eingesetzt werden, erhoben werden.

Oftmals werden in der Produktion und Fertigung neben IT-Systemen noch eine Reihe weiterer Geräte eingesetzt. Alle ICS-Geräte sollten entsprechend erfasst werden.

Im ICS-Bereich gibt es Arbeitsplatz-PCs, die auch hier zu Gruppen zusammengefasst werden sollten. Oftmals sind diese PCs mit den gleichen Anwendungen wie die der Büroumgebung ausgestattet.

Darüber hinaus sind auf einigen PCs spezielle Anwendungen installiert. Zu vielen PC-Arbeitsplätzen gehört ein Drucker und neben der Standardperipherie (Maus, Tastatur) werden weitere periphere Endgeräte (z. B. Handscanner) eingesetzt, die mit den Arbeitsplatz-PCs direkt verbunden sind. Bei allen peripheren Endgeräten müssen die Kommunikationsverbindungen (z. B. Bluetooth) ebenfalls berücksichtigt werden.

Im Bereich der Produktion und Fertigung werden weitere Endgeräte eingesetzt. Für die industrielle Steuerung gibt es spezielle Endgeräte, z. B. Geräte mit speicherprogrammierbaren Steuerungen (SPSen), WLAN-Module für Industriemaschinen, selbstfahrende Gabelstapler (Flurfahrzeuge).

Bei der Erfassung der ICS-Systeme sollten folgende Informationen vermerkt werden, die für die nachfolgenden Schritte erforderlich sind:

- eine eindeutige Bezeichnung der ICS-Systeme bzw. der jeweiligen Gerätegruppe (die Anzahl der Geräte in den Gruppen sollte ebenfalls vermerkt sein),
- Beschreibung (Typ und Funktion),
- Plattform (z. B. Betriebssystem, Art der (Netz-)Anbindung),
- Aufstellungsort der Geräte (z. B. Gebäude, Halle, Raum)
- Status der ICS-Systeme (in Betrieb, im Test, in Planung) und
- Verantwortliche für den Betrieb der ICS-Systeme.

Beispiel: RECPLAST GmbH

In der folgenden Tabelle sind Beispiele für ICS-Systeme aufgelistet:

A.1 Strukturanalyse der RECPLAST GmbH									
Bezeichnung	**Beschreibung des Zielobjektes / der Gruppe der Zielobjekte**	**Plattform / Baustein**	**Ort**	**Gebäude**	**Raum**	**Anzahl**	**Status**	**Benutzer**	**Verantwortlich / Administrator**
S100	**SPS:** Die Maschinensteuerung für die Produktionsanlagen wird über die SPS programmiert.	SPS	Bonn	Beuel	Produktion	3	in Betrieb	Haustechnik	Haustechnik
S101	**SCADA:** Das Computersystem ermöglicht die Überwachung der Produktionsprozesse	SCADA / HMI	Bonn	Beuel	Produktionshalle	1	in Betrieb	Alle Mitarbeiter	Haustechnik
S103	**Server für Betriebsdatenerfassung:** Der Server wird für die Anwendung BDE benötigt. Dieser Server ist mit den Produtionsanlagen verbunden.	Server unter Unix	Bonn	Beuel	Serverraum	1	in Betrieb	Alle Mitarbeiter	IT-Betrieb

Abbildung 17: Auszug aus der Strukturanalyse der RECPLAST GmbH (ICS-Systeme)

8.1.7 Erhebung sonstiger Geräte

In Institutionen werden je nach Branche unterschiedlichste Geräte eingesetzt, um die Geschäftsprozesse zu unterstützen. Neben IT-Systemen, die unmittelbar als solche zu identifizieren sind, können auch viele andere Arten von Geräten Einfluss auf die Informationssicherheit haben. Zu solchen Geräten gehören beispielsweise Geräte mit Funktionalitäten aus dem Bereich IoT.

Auch Geräte, wie beispielsweise Klimaanlagen, Gefahrenmeldeanlagen oder Kaffeemaschinen, die nicht der direkten Unterstützung der Informationsverarbeitung oder anderer Geschäftsprozesse dienen, können die Informationssicherheit beeinträchtigen, wenn z. B. ein Kabelbrand Folgeschäden nach sich zieht, aber auch, wenn Geräte dieser Art zur besseren Ressourcensteuerung ins IT-Netz integriert werden.

Daher sollte die Institution einen Überblick darüber haben, welche Geräte wo eingesetzt werden und welche Anforderungen an die Informationssicherheit sich hieraus ergeben könnten, wie regelmäßige Überprüfung der Betriebssicherheit, Wartung oder das Einspielen von Patches.

Für die IT-Grundschutz-Modellierung sollten die Geräte mit IoT-Funktionalität erfasst werden, die vernetzt sind, insbesondere auch solche, die nicht im zuvor betrachteten Netzplan aufgeführt sind. Solche Geräte sollten möglichst zu Gruppen zusammengefasst und als ein Objekt behandelt werden.

Bei dieser Erfassung sollten folgende Informationen vermerkt werden, die für die nachfolgende Arbeit nützlich sind:

- eine eindeutige Bezeichnung der Geräte bzw. der jeweiligen Gruppe (bei Gruppen sollte auch die Anzahl der zusammengefassten Geräte vermerkt sein),
- Beschreibung (Typ und Funktion),
- Plattform (z. B. Betriebssystem, Art der Netzanbindung),
- Aufstellungsort der Geräte,
- Status der IT-Systeme (in Betrieb, im Test, in Planung) und
- Verantwortliche für den Betrieb der Geräte.

Internet of Things (IoT)

IoT-Geräte sind häufig dadurch gekennzeichnet, dass sie überschaubare, begrenzte Außenmaße haben, oftmals preislich unterhalb von Grenzen liegen, die einen aufwendigen Beschaffungsvorgang in Institutionen nach sich ziehen, und/oder bei denen die Internetfunktionalität nicht hervorsticht. Daher ist es wahrscheinlich, dass bei jeder Art von Übersicht oder Bestandserhebung IoT-Geräte übersehen werden. Es ist wichtig, sich darüber einen Überblick zu verschaffen,

- welche IoT-Geräte in der Institution derzeit oder demnächst eingesetzt werden und
- wer die Akteure in der Institution sind, die typischerweise IoT-Geräte nutzen, und mit diesen ins Gespräch zu kommen.

Dafür kann es ein sinnvoller Ansatz für den ISB sein, in verschiedene Räumlichkeiten der Institution zu gehen und zu überlegen, welche der dort vorhandenen Komponenten Strom benötigen und ob diese über IT-Netze vernetzt sein könnten. Der ISB sollte insbesondere mit den Kollegen der Haustechnik, aber auch mit den anderen Geräteverantwortlichen sprechen und sich die Funktionalitäten der verschiedenen Geräte erläutern lassen. Die Vernetzung könnte beispielsweise über IT-Verkabelung oder WLAN mit dem LAN erfolgen, über Mobilfunk mit dem Internet, aber auch über freie WLANs in der

Umgebung oder andere Funkschnittstellen wie Bluetooth erfolgen. Zusätzlich sollten regelmäßig Netzscans durchgeführt werden und dabei nach nicht zuzuordnenden Geräten gesucht werden.

Geräte mit IoT-Funktionalitäten können in Institutionen beispielsweise folgende sein:

- Durch Mitarbeiter oder Externe mitgebrachte private Geräte, z. B. Smartwatches, digitale Bilderrahmen, Wetterstationen, Fitnessarmbänder und andere Gadgets.
- Durch die Institution beschaffte und betriebene Geräte wie Brand-, Gas- und andere Warnmelder, Kaffeemaschinen oder Elemente der Gebäudesteuerung. Die Übergänge zu ICS-Systemen sind hier fließend.

Dabei sind IoT-Geräte nicht immer direkt auf den ersten Blick als solche zu erkennen, beispielsweise wenn die IoT-Funktionalität kein kaufentscheidendes Merkmal ist, aber für den Hersteller dadurch eine für ihn gewinnbringende Datensammlung möglich wird, z. B. über die Art und Menge der Verbrauchsmaterialien.

Ein Beispiel für Geräte, in denen sich IoT-Funktionalitäten verstecken könnten, sind Komfortmöbel, die sich automatisch an die jeweiligen Benutzer anpassen und nicht nur lokal die Einstellungen speichern, sondern diese über IT-Netze mit anderen Arbeitsplätzen austauschen, sodass Mitarbeiter an beliebigen Arbeitsplätzen arbeiten können („Smart Workplaces“).

Beispiel: RECPLAST GmbH

In der folgenden Tabelle sind Beispiele für sonstige und IoT-Geräte aufgeführt:

A.1 Strukturanalyse der RECPLAST GmbH									
Bezeichnung	**Beschreibung des Zielobjektes / der Gruppe der Zielobjekte**	**Plattform / Baustein**	**Ort**	**Gebäude**	**Raum**	**Anzahl**	**Status**	**Benutzer**	**Verantwortlich / Administrator**
S200	**Alarmanlage BG:** Die Alarmanlage wird von der Pforte aus gesteuert. Zuständig für die Liegenschaft in Bad Godesberg.	Alarmanlage	Bonn	BG	Pforte	1	in Betrieb	Pförtner, Arbeitssicherheitsfachkraft	Haustechnik
S201	**Alarmanlage Beuel:** Die Alarmanlage wird seit 1996 eingesetzt und erfüllt die Grundlagen einer Alarmanlage. Mit dieser Alarmanlage wird die Liegenschaft in Beuel abgedeckt.	Alarmanlage	Bonn	Beuel	Pforte	1	in Betrieb	Arbeitssicherheitsfachkraft	Haustechnik
S202	**Video-Überwachung:** Rund um das Gelände in der Liegenschaft Bad Godesberg sind die Türen und teilweise die Fenster mit Kameras überwacht. Innen wird jeder Notausgang bewacht.	Server unter Unix	Bonn	Beuel	Serverraum	1	in Betrieb	Pforte	IT-Betrieb
S203	**Kühlschrank IT-Abteilung:** In der IT-Abteilung ist ein Kühlschrank, der mittels einer internen Kamera und einer App eine Inventarliste führt.	Kühlschrank	Bonn	BG	Teeküche EG	1	in Betrieb	IT-Abteilung	Haustechnik

Abbildung 18: Auszug aus der Strukturanalyse der RECPLAST GmbH (sonstige und IoT-Geräte)

Aktionspunkte zu 8.1.5, 8.1.6 und 8.1.7 Erhebung der IT-, ICS-Systeme und sonstiger Geräte

- Prüfen, ob existierende Datenbanken oder Übersichten über die vorhandenen oder geplanten IT-, ICS-Systeme sowie die sonstigen Geräte als Ausgangsbasis für die weitere Vorgehensweise geeignet sind
- Liste der vernetzten und nicht vernetzten IT-Systeme, IoT- und ICS-Geräte erstellen beziehungsweise aktualisieren und vervollständigen
- IT-, ICS-, IoT-Systeme beziehungsweise Systemgruppen mit eindeutigen Nummern oder Kürzeln kennzeichnen
- Die Anwendungen den IT-, ICS-, IoT-Systemen (Servern, Clients, Netzkoppelelementen usw.) zuordnen, die für ihre Ausführung benötigt werden

8.1.8 Erfassung der Räume

Die betrachteten Geschäftsprozesse und Fachaufgaben werden nicht nur auf definierten IT-Systemen betrieben, sondern auch innerhalb der Grenzen der räumlichen Infrastruktur einer Institution. Je nach Größe der Institution und abhängig von vielen anderen Faktoren kann sich eine Institution in einem allein genutzten Gebäude oder auch nur auf einer Etage befinden. Viele Institutionen nutzen Liegenschaften, die weit verstreut sind oder mit anderen Nutzern geteilt werden müssen. Häufig sind Geschäftsprozesse und Fachaufgaben auch in fremden Räumlichkeiten angesiedelt, zum Beispiel im Rahmen von Dienstleistungsverträgen.

In ein Sicherheitskonzept müssen alle Liegenschaften, innerhalb derer die betrachteten Geschäftsprozesse und Fachaufgaben betrieben werden, einbezogen werden. Dazu gehören Betriebsgelände, Gebäude, Etagen, Räume sowie die Wegstrecke zwischen diesen. Alle Kommunikationsverbindungen, die über für Dritte zugängliche Gelände verlaufen, müssen als Außenverbindungen behandelt werden. Dies gilt auch für drahtlose Kommunikationsverbindungen, wenn nicht ausgeschlossen werden kann, dass Dritte darauf zugreifen können. Nicht vergessen werden sollten auch Räumlichkeiten, die außerhalb der offiziellen Liegenschaften liegen, die aber auch sporadisch oder regelmäßig genutzt werden, um dort Geschäftsprozesse und Fachaufgaben zu bearbeiten. Dazu gehören beispielsweise Telearbeitsplätze oder temporär angemietete Arbeitsplätze und Lagerflächen.

Für die weitere Vorgehensweise der Modellierung nach IT-Grundschutz und für die Planung des Soll-Ist-Vergleichs ist es hilfreich, eine Übersicht über die Liegenschaften, vor allem die Räume, zu erstellen, in denen IT-, ICS- oder IoT-Systeme aufgestellt oder die für deren Betrieb genutzt werden. Dazu gehören Räume, die ausschließlich dem IT-Betrieb dienen (wie Serverräume, Datenträgerarchive), solche, in denen unter anderem IT-, ICS- oder IoT-Systeme betrieben werden (wie Büroräume oder Werkhallen), aber auch die Wegstrecken, über die Kommunikationsverbindungen laufen. Wenn IT-Systeme statt in einem speziellen Technikraum in einem Schutzschrank untergebracht sind, ist der Schutzschrank ebenfalls wie ein Raum zu erfassen.

Hinweis:

Bei der Erhebung der IT-, ICS- und IoT-Systeme sind schon die Aufstellungsorte aufgelistet worden.

Zusätzlich muss untersucht werden, ob schutzbedürftige Informationen in weiteren Räumen aufbewahrt werden. Diese Räume müssen dann ebenfalls benannt werden. Hierbei müssen auch Räume hinzugezählt werden, in denen nicht elektronische schutzbedürftige Informationen aufbewahrt werden, also beispielsweise Aktenordner oder Mikrofilme. Die Art der verarbeiteten Informationen muss anhand dieser Dokumentation nachvollziehbar sein.

Beispiel: RECPLAST GmbH

Im folgenden Ausschnitt wird anhand des fiktiven Beispiels der RECPLAST GmbH gezeigt, wie eine tabellarische Übersicht über die Räume aussehen könnte. Räume können wie alle Zielobjekte gruppiert werden. Dies ist möglich, sofern die Räume eine ähnliche Ausstattung und vergleichbare Sicherheitsanforderungen haben.

A.1 Strukturanalyse der RECPLAST GmbH									
Bezeichnung	**Beschreibung des Zielobjektes / der Gruppe der Zielobjekte**	**Plattform / Baustein**	**Ort**	**Gebäude**	**Raum**	**Anzahl**	**Status**	**Benutzer**	**Verantwortlich / Administrator**
R001	**Büroraum** Ein Standard-Büroraum enthält Schreibtische, Schränke, die erforderliche Verkabelung, Präsenzmelder für die Alarmanlage. Die Büroräume sind abschließbar. Die Anzahl der Mitarbeiter je Büroraum ist begrenzt auf ein bis sechs Mitarbeiter.	Büroraum	Bonn	BG	-	27	in Betrieb	Alle Mitarbeiter	Gebäudemanagement
R002	**Besprechungsräume:** Verteilt in der Liegenschaft Bad Godesberg gibt es Besprechungsräume, die mit Tischen, Stühlen, Schränken und Verkabelung bestückt sind. In diesen Räumen dürfen sich Besucher in Begleitung von Mitarbeitern aufhalten.	Besprechungsraum	Bonn	BG	-	5	in Betrieb	Alle Mitarbeiter	Gebäudemanagement

A.1 Strukturanalyse der RECPLAST GmbH									
Bezeichnung	**Beschreibung des Zielobjektes / der Gruppe der Zielobjekte**	**Plattform / Baustein**	**Ort**	**Gebäude**	**Raum**	**Anzahl**	**Status**	**Benutzer**	**Verantwortlich / Administrator**
R003	**Häuslicher Arbeitsplatz:** Einige Mitarbeiter dürfen von ihrem Wohnort aus arbeiten. Der häusliche Arbeitsplatz muss vor Dritten so geschützt sein, dass alle Firmenunterlagen sicher verschlossen werden können. Der ISB kontrolliert mit vorheriger Ankündigung einen häuslichen Arbeitsplatz.	Telearbeit	mobiler Arbeitsplatz	-	-	27	in Betrieb	Telearbeitnehmer	ISB
R004	**Mobiler Arbeitsplatz:** Alle Mitarbeiter, die ein Notebook als IT-System nutzen, können mobil arbeiten. Dies ist innerhalb als auch außerhalb der Räumlichkeiten der RECPLAST GmbH gestattet. Es müssen hierzu verbindliche Richtlinien eingehalten werden. Firmenunterlagen dürfen nur begrenzt mitgenommen werden.	Mobiler Arbeitsplatz	mobiler Arbeitsplatz	-	-	75	in Betrieb	Führungskräfte, Mitarbeiter	IT-Betrieb

Abbildung 19: Auszug aus der Strukturanalyse der RECPLAST GmbH (Räume)

Aktionspunkte zu 8.1.8 Erfassung der Räume
• Liste aller bei der Erfassung der IT-, ICS- und IoT-Systeme notierten Liegenschaften, Gebäude und Räume erstellen • Weitere Räume ergänzen, in denen schutzbedürftige Informationen aufbewahrt oder auf andere Weise verarbeitet werden

8.2 Schutzbedarfsfeststellung

Ziel der Schutzbedarfsfeststellung ist es, für die erfassten Objekte im Informationsverbund zu entscheiden, welchen Schutzbedarf sie bezüglich Vertraulichkeit, Integrität und Verfügbarkeit besitzen. Dieser Schutzbedarf orientiert sich an den möglichen Schäden, die mit einer Beeinträchtigung der betroffenen Anwendungen und damit der jeweiligen Geschäftsprozesse verbunden sind.

Die Schutzbedarfsfeststellung für den Informationsverbund gliedert sich in mehrere Schritte:

- Definition der Schutzbedarfskategorien
- Schutzbedarfsfeststellung für Geschäftsprozesse und Anwendungen
- Schutzbedarfsfeststellung für IT-Systeme, IoT- und ICS-Geräte
- Schutzbedarfsfeststellung für Gebäude, Räume, Werkhallen usw.
- Schutzbedarfsfeststellung für Kommunikationsverbindungen
- Schlussfolgerungen aus den Ergebnissen der Schutzbedarfsfeststellung

Nach der Definition der Schutzbedarfskategorien wird anhand von typischen Schadensszenarien zunächst der Schutzbedarf der Geschäftsprozesse und Anwendungen bestimmt. Anschließend wird daraus der Schutzbedarf der einzelnen IT-Systeme, Räume und Kommunikationsverbindungen abgeleitet.

Die Vorgehensweise hierfür wird in den folgenden Abschnitten detailliert dargestellt.

8.2.1 Definition der Schutzbedarfskategorien

Da der Schutzbedarf meist nicht quantifizierbar ist, beschränkt sich der IT-Grundschutz somit auf eine qualitative Aussage, indem der Schutzbedarf in drei Kategorien unterteilt wird:

Schutzbedarfskategorien	
„normal“	Die Schadensauswirkungen sind begrenzt und überschaubar.
„hoch“	Die Schadensauswirkungen können beträchtlich sein.
„sehr hoch“	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Hinweis:

Es kann für eine Institution auch sinnvoll sein, weitere Kategorien zu definieren. Beispielsweise kann eine Abstufung nach unten, z. B. „unkritisch“, eingeführt werden. (Diese könnte wie folgt definiert sein: „Schäden an Ressourcen der Schutzbedarfskategorie ‚unkritisch‘ haben keine oder nur minimale Beeinträchtigungen der Institution zur Folge.“)

Werden nur ein oder zwei Kategorien genutzt, ist die damit erreichbare Abstufung meist nicht granular genug. Werden dagegen fünf oder mehr Schutzbedarfskategorien verwendet, ist eine klare Unterscheidung zwischen den einzelnen Stufen schwieriger. Zudem ist die Zuordnung von Ressourcen zu einer der möglichen Schutzbedarfskategorien schwer nachvollziehbar und es steigt dadurch auch der Aufwand sowohl bei der Zuordnung als auch bei Revisionen.

Eine andere Möglichkeit ist es, für Vertraulichkeit andere Kategorien als für Integrität oder Verfügbarkeit zu nutzen. Einige Institutionen unterteilen beispielsweise Vertraulichkeit in die Kategorien „offen", „intern", „vertraulich" und „geheim", aber die Kategorien Integrität oder Verfügbarkeit nur in zwei Stufen „normal" und „kritisch".

Wenn mehr als drei Schutzbedarfskategorien definiert werden, so ist zu überlegen, welche der neu definierten Kategorien den Schutzbedarfskategorien „hoch" bzw. „sehr hoch" entsprechen, denn diese Information wird zur Überprüfung der Entscheidung benötigt, welche Objekte in die Risikoanalyse aufgenommen werden.

Die nachfolgenden Schritte erläutern, wie für Geschäftsprozesse und die mit diesen verbundenen Anwendungen jeweils die adäquate Schutzbedarfskategorie ermittelt werden kann.

Die Schäden, die bei dem Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit für einen Geschäftsprozess bzw. eine Anwendung einschließlich ihrer Daten entstehen können, lassen sich typischerweise folgenden Schadensszenarien zuordnen:

- Verstoß gegen Gesetze/Vorschriften/Verträge,
- Beeinträchtigung des informationellen Selbstbestimmungsrechts,
- Beeinträchtigung der persönlichen Unversehrtheit,
- Beeinträchtigung der Aufgabenerfüllung,
- negative Innen- oder Außenwirkung und
- finanzielle Auswirkungen.

Häufig treffen dabei für einen Schaden mehrere Schadensszenarien zu. So kann beispielsweise der Ausfall einer Anwendung die Aufgabenerfüllung beeinträchtigen, was direkte finanzielle Einbußen nach sich zieht und gleichzeitig auch zu einem Imageverlust führt.

Hinweis:

Auch die Art und Anzahl der betrachteten Szenarien können individuell angepasst werden. Je nach Institution gibt es unterschiedliche Schwerpunkte, auf die sich das Sicherheitsmanagement konzentrieren kann. So könnte das Szenario „Beeinträchtigung des informationellen Selbstbestimmungsrechts" entfallen, wenn beispielsweise in der Institution das Datenschutzmanagement dieses Szenario bereits ausreichend betrachtet hat. In vielen Institutionen kann das Szenario „Beeinträchtigung der persönlichen Unversehrtheit" weggelassen werden, es sei denn, es handelt sich um ein Unternehmen, bei dem Fehlfunktionen von IT-Systemen unmittelbar Personenschäden nach sich ziehen können. Dies könnte beispielsweise im Gesundheitswesen oder in Produktionsbereichen der Fall sein.

Es könnten auch zusätzliche Szenarien betrachtet werden, wie beispielsweise

- Einschränkung der Dienstleistungen für Dritte oder

- Auswirkungen auf weitere Infrastrukturen außerhalb des eigenen Informationsverbunds (z. B. Rechenzentren, IT-Betrieb von Kunden oder Dienstleistern).

Um die Schutzbedarfskategorien „normal", „hoch" und „sehr hoch" voneinander abgrenzen zu können, bietet es sich an, die Grenzen für die einzelnen Schadensszenarien zu bestimmen. Zur Orientierung, welchen Schutzbedarf ein potenzieller Schaden und seine Folgen erzeugen, dienen die folgenden Tabellen. Die Tabellen sollten von der jeweiligen Institution auf ihre eigenen Gegebenheiten angepasst werden.

Schutzbedarfskategorie „normal"	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen • Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung erscheint nicht möglich.
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit liegt zwischen 24 und 72 Stunden.
5. Negative Innen- oder Außenwirkung	• Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden bleibt für die Institution tolerabel.

Tabelle 2: Schutzbedarfskategorie „normal"

Schutzbedarfskategorie „hoch"	
1. Verstoß gegen Gesetze/Vorschriften/Verträge	• Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen • Vertragsverletzungen mit hohen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.

Schutzbedarfskategorie „hoch“	
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. • Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.
5. Negative Innen- oder Außenwirkung	• Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	• Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.

Tabelle 3: Schutzbedarfskategorie „hoch“

Schutzbedarfskategorie „sehr hoch“	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Fundamentaler Verstoß gegen Vorschriften und Gesetze • Vertragsverletzungen, deren Haftungsschäden ruinös sind
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. • Gefahr für Leib und Leben
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
5. Negative Innen- oder Außenwirkung	• Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden ist für die Institution existenzbedrohend.

Tabelle 4: Schutzbedarfskategorie „sehr hoch“

Wenn bei individuellen Betrachtungen festgestellt wird, dass über diese sechs Schadensszenarien hinaus weitere infrage kommen, sollten diese entsprechend ergänzt werden. Für alle Schäden, die sich nicht in diese Szenarien abbilden lassen, muss ebenfalls eine Aussage getroffen werden, wo die Grenzen zwischen „normal“, „hoch“ oder „sehr hoch“ zu ziehen sind.

Darüber hinaus sollten die individuellen Gegebenheiten der Institution berücksichtigt werden: Bedeutet in einem Großunternehmen ein Schaden in Höhe von 200.000,- € gemessen am Umsatz noch einen geringen Schaden, so kann für ein Kleinunternehmen schon ein Schaden in Höhe von 10.000,- € existenziell bedrohlich sein. Daher kann es sinnvoll sein, eine prozentuale Größe als Grenzwert zu definieren, der sich am Gesamtumsatz, am Gesamtgewinn oder an einer ähnlichen Bezugsgröße orientiert.

Ähnliche Überlegungen können bezüglich der Verfügbarkeitsanforderungen angestellt werden. So kann beispielsweise ein Ausfall von 24 Stunden Dauer in der Schutzbedarfskategorie „normal“ als

noch tolerabel eingeschätzt werden. Tritt jedoch eine Häufung dieser Ausfälle ein, z. B. mehr als einmal wöchentlich, so kann dies in der Summe nicht tolerierbar sein. Die anhand der Schutzbedarfskategorien festgelegten Verfügbarkeitsanforderungen sollten daher bei Bedarf konkretisiert werden.

Es kann erforderlich sein, für den Bereich ICS die Schutzbedarfskategorien separat festzulegen, aber diese auf die des restlichen Informationsverbunds abzustimmen. In produzierenden Bereichen ist es beispielsweise oftmals erforderlich, für die jeweiligen Kategorien kürzere Ausfallzeiten festzulegen als im Bereich der Büro-IT. Zeitliche Vorgaben können z. B. aus Wartungsverträgen abgeleitet werden. Unter Umständen müssen auch andere Punkte angepasst werden. Auch im Datenschutz muss der Schutzbedarf festgelegt werden, um angemessen technische und organisatorische Schutzmaßnahmen bestimmen und konfigurieren zu können. Das Standard-Datenschutzmodell (SDM) bietet eine ganze Reihe an Kriterien, um das Risiko eines Grundrechtseingriffs, und daraus folgend des Schutzbedarfs, anhand von drei Stufen zu bestimmen. Das SDM bietet zudem Hilfestellungen, sollten die Schutzbedarfe aus Sicht der Informationssicherheit und des Datenschutzes nicht übereinstimmen.

Bei der Festlegung der Grenze zwischen „normal“ und „hoch“ sollte berücksichtigt werden, dass für den normalen Schutzbedarf die Basis- und Standardsicherheitsanforderungen des IT-Grundschutzes ausreichen sollten. Die getroffenen Festlegungen sind in geeigneter Weise im Sicherheitskonzept zu dokumentieren, da hiervon die Auswahl von Sicherheitsmaßnahmen und damit meist Folgekosten abhängen.

Aktionspunkte zu 8.2.1 Definition der Schutzbedarfskategorien
• Typische Schadensszenarien für die Definition von Schutzbedarfskategorien betrachten
• Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ definieren beziehungsweise an die eigene Institution anpassen

8.2.2 Vorgehen bei der Schutzbedarfsfeststellung

Zunächst wird der Schutzbedarf der Geschäftsprozesse und Anwendungen bestimmt. Anschließend wird daraus der Schutzbedarf der einzelnen Objekte (z. B. IT-Systeme, Räume und Kommunikationsverbindungen) abgeleitet.

Die Grundlage zur Bestimmung des Schutzbedarfs verschiedener Objekte ist der Schutzbedarf der Geschäftsprozesse und der zugehörigen Informationen. Der für diese Elemente ermittelte Schutzbedarf vererbt sich auf die für deren Verarbeitung genutzten Objekte, also Anwendungen, IT-Systeme, ICS- und sonstige Geräte, Räume und Kommunikationsverbindungen (**Vererbung**).

Zur Ermittlung des Schutzbedarfs eines Objektes müssen die möglichen Schäden der relevanten Teilobjekte in ihrer Gesamtheit betrachtet werden. Beispielsweise müsste bei einem IT-System beleuchtet werden, welche Auswirkungen Schäden bei den darauf betriebenen Anwendungen und den damit verarbeiteten Informationen haben. Im Wesentlichen bestimmt der Schaden bzw. die Summe der Schäden mit den schwerwiegendsten Auswirkungen den Schutzbedarf eines Objektes (Maximumprinzip).

Bei der Betrachtung der möglichen Schäden und ihrer Folgen muss auch beachtet werden, dass die verschiedenen betrachteten Objekte eines Informationsverbunds natürlich eng miteinander verzahnt sind. So kann z. B. eine IT-Anwendung Arbeitsergebnisse anderer Anwendungen als Input nutzen. Eine, für sich betrachtet, weniger bedeutende Anwendung A kann wesentlich an Wert gewinnen, wenn eine andere wichtige Anwendung B auf ihre Ergebnisse angewiesen ist. In diesem Fall muss der ermittelte Schutzbedarf der Anwendung B auch auf die Anwendung A übertragen werden. Handelt

es sich dabei um Anwendungen verschiedener IT-Systeme, dann müssen Schutzbedarfsanforderungen des einen IT-Systems auch auf das andere übertragen werden (Beachtung von Abhängigkeiten).

Werden mehrere Anwendungen bzw. Informationen auf einem IT-System (oder in einem Raum oder über eine Kommunikationsverbindung) verarbeitet, so ist zu überlegen, ob durch Kumulation mehrerer (z. B. kleinerer) Schäden auf einem IT-System ein insgesamt höherer Gesamtschaden entstehen kann. Dann erhöht sich der Schutzbedarf des Objektes, also hier des IT-Systems, entsprechend (Kumulationseffekt).

Beispiel:

Auf einem Netzserver befinden sich sämtliche für die Kundendatenerfassung benötigten Anwendungen einer Institution. Der Schaden bei Ausfall einer dieser Anwendungen wurde als gering eingeschätzt, da genügend Ausweichmöglichkeiten vorhanden sind. Fällt jedoch der Server (und damit alle Anwendungen, die diesen Server benötigen) aus, so ist der dadurch entstehende Schaden deutlich höher zu bewerten. Die Aufgabenerfüllung kann unter Umständen nicht mehr innerhalb der notwendigen Zeitspanne gewährleistet werden. Daher ist auch der Schutzbedarf dieser „zentralen" Komponente entsprechend höher zu bewerten.

Auch der umgekehrte Effekt kann eintreten. So ist es möglich, dass eine Anwendung einen hohen Schutzbedarf besitzt, ihn aber deshalb nicht auf ein betrachtetes IT-System überträgt, weil auf diesem IT-System nur unwesentliche Teilbereiche der Anwendung laufen. Hier ist der Schutzbedarf zu relativieren (Verteilungseffekt). Der Verteilungseffekt kann natürlich auch bei anderen Zielobjekten, wie beispielsweise Räumen, Gebäuden oder Kommunikationsverbindungen, auftreten.

Beispiel: Der Verteilungseffekt tritt hauptsächlich bezüglich des Grundwertes der Verfügbarkeit auf. So kann bei redundanter Auslegung von IT-Systemen der Schutzbedarf der Einzelkomponenten niedriger sein als der Schutzbedarf der Gesamtanwendung. Auch im Bereich der Vertraulichkeit sind Verteilungseffekte vorstellbar: Falls sichergestellt ist, dass ein Client nur unkritische Daten einer hochvertraulichen Datenbankanwendung abrufen kann, so besitzt der Client im Vergleich zum Datenbankserver unter Umständen einen geringeren Schutzbedarf.

Ein Verteilungseffekt tritt häufig auf, wenn bei der Einrichtung oder dem Aufbau von Zielobjekten durch entsprechende Redundanzen bereits den Anforderungen an einen hohen Schutzbedarf Rechnung getragen wurde. Dies ist im Grunde ein Vorgriff auf Betrachtungen, die im Rahmen der Risikoanalyse erforderlich sind. Deshalb sollten im Rahmen der Schutzbedarfsfeststellung getroffene Entscheidungen sorgfältig dokumentiert werden.

Beispiel:

Bei Anwendungen, die im Hinblick auf Verfügbarkeit einen hohen Schutzbedarf haben, wurden bereits Redundanzen vorgesehen, unter anderem Ausweicharbeitsplätze in Nachbargebäuden. Durch die entstandenen Verteilungseffekte haben diese Arbeitsplätze normalen Schutzbedarf bezüglich Verfügbarkeit, solange ausreichend Ausweicharbeitsplätze zur Verfügung stehen.

Die Schutzbedarfsfeststellung ist ein **iterativer Prozess**. Bereits ganz am Anfang, bei der ersten Diskussion darüber, welche Geschäftsprozesse und Informationen welche Bedeutung für die Institution haben, wird eine erste grobe Schutzbedarfsfeststellung durchgeführt. Auch nach Durchführung von Risikoanalysen sollte die Schutzbedarfsfeststellung erneut dahingehend geprüft werden, ob sie an-

gepasst werden muss, da sich während der Risikoanalyse und der Auswahl von Maßnahmen neue Erkenntnisse für den Schutzbedarf von Assets ergeben können.

8.2.3 Schutzbedarfsfeststellung für Geschäftsprozesse und Anwendungen

Um den Schutzbedarf in den verschiedenen Bereichen eines Informationsverbunds zu bestimmen, muss zunächst der Schutzbedarf der Geschäftsprozesse und der zugehörigen Informationen ermittelt werden. Darauf aufbauend wird daraus der Schutzbedarf der einzelnen Anwendungen, IT-Systeme, ICS- und sonstigen Geräte, Räume und Kommunikationsverbindungen abgeleitet.

Um den Schutzbedarf der Geschäftsprozesse zu ermitteln, sollte zunächst die Bedeutung der einzelnen Geschäftsprozesse für die Institution beleuchtet werden. Davon ausgehend sollte hinterfragt werden, welche Abhängigkeiten zwischen Geschäftsprozessen und Anwendungen bestehen und wie die sich daraus ergebenden Risiken entschärft werden können. Hierzu hat es sich bewährt, mit der Fragestellung „Was wäre, wenn…?" zusammen mit den Anwendern realistische Schadensszenarien zu diskutieren und die zu erwartenden materiellen oder ideellen Schäden zu beschreiben. Oft führt dies auch dazu, dass kritische Abhängigkeiten zwischen Geschäftsprozessen und weiteren Zielobjekten aufgedeckt werden, die vorher nicht im Fokus standen.

Aus dem Schutzbedarf der Geschäftsprozesse ergibt sich der Schutzbedarf der Anwendungen, die für deren Erledigung eingesetzt werden.

Hinweis:

Zur Einschätzung des Schutzbedarfs sollten die geeigneten Ansprechpartner gesucht werden, es ist nicht erforderlich, größere Gruppe von Benutzern zu befragen. Beispielsweise ist es zur Bewertung des Schutzbedarfs bestimmter zentraler Dienste, wie zum Beispiel DNS oder E-Mail, ausreichend, den Schutzbedarf durch die Organisationseinheit festlegen zu lassen, die als Dienstanbieter für die Institution auftritt (meist die IT-Abteilung oder das Provider-Management). Der Schutzbedarf dieser Dienste ist in der Institution zu kommunizieren. Wird ein höherwertiger Schutzbedarf der Dienste durch einzelne Fachabteilungen benötigt, so sind mögliche Lösungen zwischen Fachabteilung, Sicherheitsmanagement und dem Betreiber oder Anbieter des Dienstes zu erörtern. Ein IT-Dienstleister kann im Regelfall seine Services nicht für jede mögliche Schutzbedarfskategorie bereitstellen. Deshalb wird er seine Dienste mit einer von ihm festgelegten Schutzbedarfseignung anbieten. Der Informationseigentümer muss bei Nutzung eines Service für seinen Geschäftsprozess entscheiden, ob die ihm vom IT-Dienstleister angebotene Schutzbedarfseignung ausreicht oder ob zusätzliche Sicherheitsmaßnahmen infolge höheren Schutzbedarfs umgesetzt werden müssen.

In die Schutzbedarfsfeststellung müssen auch die in der Strukturanalyse erfassten Gruppen von Datenträgern und Dokumenten einbezogen werden.

Um die Ermittlung der möglichen Schäden und Auswirkungen zu vereinfachen, werden im Anhang dieses Standards entsprechende Fragestellungen vorgestellt. Diese Anregungen erheben nicht den Anspruch auf Vollständigkeit, sie dienen lediglich zur Orientierung. Um die individuelle Aufgabenstellung und die Situation der Institution zu berücksichtigen, müssen diese Fragen gegebenenfalls entsprechend ergänzt und angepasst werden.

Die Festlegung des Schutzbedarfs der Geschäftsprozesse und Anwendungen ist eine Entscheidung im Rahmen des Risikomanagements und hat oft weitreichende Auswirkungen auf das Sicherheitskonzept für den betrachteten Informationsverbund. Der Schutzbedarf der Geschäftsprozesse und An-

wendungen fließt in die Schutzbedarfsfeststellung der betroffenen technischen und infrastrukturellen Objekte, wie zum Beispiel Server und Räume, ein.

Bei komplexen Geschäftsprozessen, insbesondere wenn diese hohen oder sehr hohen Schutzbedarf haben, kann es sinnvoll sein, diese in Teilprozesse zu zerlegen. Wenn dabei der Bereich mit einem hohen oder sehr hohen Schutzbedarf auf wenige Teilprozesse eingegrenzt werden kann, hat das den Vorteil, dass sich der hohe bzw. sehr hohe Schutzbedarf auf wenige Objekte vererbt.

Um die Ergebnisse der Schutzbedarfsfeststellung und die daraus resultierenden Entscheidungen im Rahmen des Informationssicherheitsmanagements später jederzeit nachvollziehen zu können, müssen die Ergebnisse der Schutzbedarfsfeststellung der Geschäftsprozesse und Anwendungen gut dokumentiert werden. Dabei ist darauf zu achten, dass nicht nur die Festlegung des Schutzbedarfs festgehalten wird, sondern auch die entsprechenden Begründungen. Diese Begründungen erlauben es später, die Festlegungen zu überprüfen und weiter zu verwenden.

Beispiel: RECPLAST GmbH

In der nachfolgenden Tabelle werden für das Unternehmen RECPLAST GmbH die wesentlichen Anwendungen, deren Schutzbedarf und die entsprechenden Begründungen erfasst.

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH									
Bezeichnung	**Beschreibung des Zielobjektes / der Gruppe der Zielobjekte**	**Plattform / Baustein**	**Verantwortlich / Administrator**	**Vertraulichkeit**	**Begründung für die Vertraulichkeit**	**Integrität**	**Begründung für die Integrität**	**Verfügbarkeit**	**Begründung für die Verfügbarkeit**
A003	Textverarbeitung, Tabellenkalkulation	Office-Produkt 2010	IT-Betrieb	normal	Die Anwendung selbst enthält keine Informationen.	normal	Die Anwendung selbst enthält keine Informationen	normal	Die Anwendung wird lokal installiert. Die Lizenzen sind entsprechend aufgehoben, so dass eine Neuinstallation schnell ermöglicht werden kann. Eine Ausfallzeit von mehr als 24 Stunden ist tolerierbar.
A007	Lotus Notes	Lotus Notes	IT-Betrieb	hoch	Über das E-Mailsystem werden viele, teilweise vertrauliche Informationen versendet. Durch die Anwendung werden alle E-Mails verschlüsselt.	normal	Durch eine Signatur kann die Integrität einer E-Mail festgestellt werden.	sehr hoch	Das Mailsystem sollte auch dann zur Verfügung stehen, falls andere Kommunikationsmittel ausfallen (z.B. Faxserver)
C002	Laptop Verwaltung	Client unter Windows 10	IT-Betrieb	normal	Maximumprinzip Auf dem Arbeitsplatzrechner werden keine Informationen gespeichert	normal	Maximumprinzip Auf dem Arbeitsplatzrechner werden keine Informationen gespeichert	normal	Es ist ein Ausfall von höchstens 4 Stunden tolerierbar.

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH									
Bezeichnung	**Beschreibung des Zielobjektes / der Gruppe der Zielobjekte**	**Plattform / Baustein**	**Verantwortlich / Administrator**	**Vertraulichkeit**	**Begründung für die Vertraulichkeit**	**Integrität**	**Begründung für die Integrität**	**Verfügbarkeit**	**Begründung für die Verfügbarkeit**
G003	Vertrieb Berlin	Gebäude	-	hoch	Maximumprinzip In dem Gebäude werden grundsätzlich alle Informationen verarbeitet	hoch	Maximumprinzip In dem Gebäude werden grundsätzlich alle Informationen verarbeitet	hoch	Maximumprinzip In dem Gebäude werden grundsätzlich alle Informationen verarbeitet
K001	Internet – Bonn BG	-	IT-Betrieb	hoch	Maximumprinzip	hoch	Maximumprinzip	hoch	Maximumprinzip
R003	Häuslicher Arbeitsplatz	Telearbeit	IT-Betrieb	hoch	Maximumprinzip	hoch	Maximumprinzip	hoch	Maximumprinzip
N001	Router Internetanbindung	Router und Switches	IT-Betrieb	hoch	Der Router stellt den Anschluss zwischen dem Internet und dem Produktionsnetz dar.	normal	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Ersatzgerät liegt auf Lager und kann schnell durch den IT-Betrieb ausgetauscht werden
S020	Virtueller Server (Konfiguration 1)	Server unter Unix	IT-Betrieb	normal	Die Server sind im eigenen Serverraum mit Zugriff-, Zugangs- und Zutrittsberechtigung untergebracht.	normal	Die Server sind im eigenen Serverraum mit Zugriff-, Zugangs- und Zutrittsberechtigung untergebracht.	normal	Durch die Redundanz der Server kann bei Ausfall eines Servers der Dienst von einem anderen Server übernommen werden.

Abbildung 20: Auszug aus der Schutzbedarfsfeststellung der RECPLAST GmbH

An dieser Stelle kann es sinnvoll sein, über diese Informationen hinaus den Schutzbedarf auch aus einer gesamtheitlichen Sicht der Geschäftsprozesse oder Fachaufgaben zu betrachten. Dazu bietet es sich an, den Zweck einer Anwendung in einem Geschäftsprozess oder in einer Fachaufgabe zu beschreiben und daraus wiederum deren Bedeutung abzuleiten. Diese Bedeutung kann wie folgt klassifiziert werden.

Die Bedeutung der Anwendung ist für den Geschäftsprozess bzw. die Fachaufgabe:

- normal: Der Geschäftsprozess bzw. die Fachaufgabe kann mit tolerierbarem Mehraufwand mit anderen Mitteln (z. B. manuell) durchgeführt werden.
- hoch: Der Geschäftsprozess bzw. die Fachaufgabe kann nur mit deutlichem Mehraufwand mit anderen Mitteln durchgeführt werden.
- sehr hoch: Der Geschäftsprozess bzw. die Fachaufgabe kann ohne die Anwendung überhaupt nicht durchgeführt werden.

Der Vorteil, eine solche ganzheitliche Zuordnung vorzunehmen, liegt insbesondere darin, dass bei der Schutzbedarfsfeststellung die Leitungsebene als Regulativ für den Schutzbedarf der einzelnen Anwendungen agieren kann. So kann es sein, dass ein Verantwortlicher für eine Anwendung deren Schutzbedarf aus seiner Sicht als „normal" einschätzt, die Leitungsebene aus Sicht des Geschäftsprozesses bzw. der Fachaufgabe diese Einschätzung jedoch nach oben korrigiert.

Diese optionalen Angaben sollten ebenfalls tabellarisch oder mithilfe entsprechender Software-produkte dokumentiert werden.

Aktionspunkt zu 8.2.3 Schutzbedarfsfeststellung für Geschäftsprozesse und Anwendungen
• Schutzbedarf der erfassten Geschäftsprozesse und Anwendungen anhand von Schadensszenarien und Fragenkatalogen ermitteln
• Schutzbedarf der Geschäftsprozesse und Anwendungen und die entsprechenden Begründungen tabellarisch dokumentieren

8.2.4 Schutzbedarfsfeststellung für IT-Systeme

Um den Schutzbedarf eines IT-Systems festzustellen, müssen zunächst die Anwendungen betrachtet werden, die in direktem Zusammenhang mit dem IT-System stehen. Eine Übersicht, welche Anwendungen für die unterschiedlichen IT-Systeme relevant sind, wurde im Rahmen der Strukturanalyse (siehe Kapitel 8.1) ermittelt. Der Schutzbedarf der Geschäftsprozesse und Anwendungen (siehe Kapitel 8.2.3) fließt in die Schutzbedarfsfeststellung für die jeweils betroffenen IT-Systeme ein. Hierbei ist darauf zu achten, dass nicht nur die IT-Systeme berücksichtigt werden, auf denen die jeweilige Anwendung installiert ist. Vielmehr ist auch der Datenfluss der Anwendung zu beachten, über den der Schutzbedarf der Anwendung auf die dazwischenliegenden Netzkomponenten vererbt wird.

Zur Ermittlung des Schutzbedarfs eines IT-Systems müssen nun die möglichen Schäden der relevanten Anwendungen in ihrer Gesamtheit betrachtet werden. Die Ergebnisse der Schutzbedarfsfeststellung der IT-Systeme sollten wiederum in einer Tabelle festgehalten werden. Darin sollte verzeichnet sein, welchen Schutzbedarf jedes IT-System bezüglich Vertraulichkeit, Integrität und Verfügbarkeit hat. Der Gesamtschutzbedarf eines IT-Systems leitet sich wiederum aus dem Maximum des Schutzbedarfs bezüglich der drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit ab. Ein IT-System ist also hochschutzbedürftig, wenn es bezüglich eines oder mehrerer Grundwerte den Schutzbedarf „hoch"

hat. Der Schutzbedarf eines IT-Systems sollte für alle drei Grundwerte einzeln dokumentiert werden, da sich hieraus typischerweise verschiedene Arten von Sicherheitsmaßnahmen ergeben.

Bei einem IT-System kann sich beispielsweise der hohe Gesamtschutzbedarf daraus ableiten, dass der Schutzbedarf bezüglich Vertraulichkeit hoch ist, bezüglich Integrität und Verfügbarkeit allerdings normal. Dann kann zwar der Gesamtschutzbedarf mit „hoch" angegeben werden, dies zieht aber nicht nach sich, dass dadurch der Schutzbedarf bezüglich Integrität und Verfügbarkeit angehoben werden muss.

Die Festlegungen des Schutzbedarfs der IT-Systeme müssen begründet werden, damit die Entscheidungen auch für Außenstehende nachvollziehbar sind. Hier kann auf die Schutzbedarfsfeststellung der Anwendungen zurückverwiesen werden.

Beispiel: RECPLAST GmbH

Die Ergebnisse der Schutzbedarfsfeststellung für die IT-Systeme können beispielsweise wie folgt dokumentiert werden (Auszug):

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH								
Bezeichnung	**Beschreibung des Zielobjektes / der Gruppe der Zielobjekte**	**Plattform / Baustein**	**Vertraulichkeit**	**Begründung für die Vertraulichkeit**	**Integrität**	**Begründung für die Integrität**	**Verfügbarkeit**	**Begründung für die Verfügbarkeit**
N001	Router Internetanbindung	Router und Switches	hoch	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Ersatzgerät liegt auf Lager und kann schnell durch den IT-Betrieb ausgetauscht werden
N002	Firewall Internet-Eingang	Firewall	hoch	Die Konfigurationseigenschaften müssen vertraulich bleiben. Diese regeln den Datenverkehr zwischen dem Internet und der RECPLAST	normal	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Ersatzgerät liegt auf Lager und kann schnell durch den IT-Betrieb ausgetauscht werden
N003	Switch – Verteilung	Router und Switches	normal	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Ersatzgerät liegt auf Lager und kann schnell durch den IT-Betrieb ausgetauscht werden
N004	Router Bonn BG – Beuel	Router und Switches	normal	Die Konfigurationseigenschaften müssen vertraulich bleiben. Diese regeln den Datenverkehr zwischen den Standorten der RECPLAST	normal	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Ersatzgerät liegt auf Lager und kann schnell durch den IT-Betrieb ausgetauscht werden

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH								
Bezeichnung	**Beschreibung des Zielobjektes / der Gruppe der Zielobjekte**	**Plattform / Baustein**	**Vertraulichkeit**	**Begründung für die Vertraulichkeit**	**Integrität**	**Begründung für die Integrität**	**Verfügbarkeit**	**Begründung für die Verfügbarkeit**
S008	Print-Server	Windows Server 2012	normal	Es werden keine vertraulichen Dokumente ausgedruckt.	normal	Fehlfunktionen werden durch ein Monitoring schnell erkannt, gemeldet und können sofort behoben werden	normal	Kann schnell auf einem anderen virtuellen Server installiert werden.
S020	Virtueller Server (Konfiguration 1)	Server unter Unix	normal	Die Server sind im eigenen Serverraum mit Zugriff-, Zugangs- und Zutrittsberechtigung untergebracht.	normal	Die Server sind im eigenen Serverraum mit Zugriff-, Zugangs- und Zutrittsberechtigung untergebracht.	normal	Durch die Redundanz der Server kann bei Ausfall eines Servers der Dienst von einem anderen Server übernommen werden.
S033	Server Produktion	Server unter Unix	sehr hoch	Die verarbeiteten Informationen sind für die Produktion notwendig. Insbesondere werden Stücklisten, Arbeitspläne und weitere Informationen zum Produktionsprozess auf diesem Server in einer Datenbank gespeichert.	hoch	Die Informationen auf dem Server müssen für den produzierenden Bereich vollständig und korrekt vorliegen. Insbesondere Stücklisten und Arbeitspläne dürfen nicht unbeachtet verändert werden.	sehr hoch	Der Server muss zu allen Produktionszeiten (täglich 6 – 22 Uhr) zur Verfügung stehen. Einen Ersatz-Server gibt es nicht. Wartungsarbeiten werden grundsätzlich am Wochenende vorgenommen.

Abbildung 21: Auszug aus der Schutzbedarfsfeststellung der RECPLAST GmbH (IT-Systeme)

Schutzbedarfsfeststellung bei virtualisierten Infrastrukturen

Wird Virtualisierung eingesetzt, bleibt die Schutzbedarfsfeststellung im Prinzip gleich. Um den Schutzbedarf eines IT-Systems zu bestimmen, müssen zunächst die Anwendungen betrachtet werden, die im direkten Zusammenhang mit dem IT-System stehen. In virtualisierten Infrastrukturen werden in der Regel mehrere IT-Systeme auf einem Virtualisierungsserver betrieben. Der Schutzbedarf der Anwendungen vererbt sich auf die virtuellen IT-Systeme. Die virtuellen IT-Systeme ihrerseits vererben ihren Schutzbedarf auf den Virtualisierungsserver. Für den Schutzbedarf eines Virtualisierungsservers lassen sich folgende Fälle unterscheiden:

Vertraulichkeit

Ist der Schutzbedarf der virtuellen IT-Systeme beispielsweise „normal", so vererbt sich dieser auf den Virtualisierungsserver. Er bekommt in der Regel auch den Schutzbedarf „normal". Es sollte überlegt werden, ob durch die Kumulation mehrerer (z. B. kleinerer) Schäden auf dem Virtualisierungsserver ein insgesamt höherer Gesamtschaden entstehen kann. Dann erhöht sich der Schutzbedarf des Virtualisierungsservers entsprechend auf „hoch" (**Kumulationseffekt**).

Integrität

Das Schutzziel Integrität wird nicht gesondert betrachtet und ist wie Vertraulichkeit zu behandeln.

Verfügbarkeit

Ist der Schutzbedarf der virtuellen IT-Systeme beispielsweise „normal", dann kommt es durch den Kumulationseffekt in der Regel zu einer Erhöhung der Verfügbarkeit. Gleichzeitig bietet Virtualisierung mit Konzepten wie Cold-, Warm- oder Hot-Standby die Möglichkeit, Redundanzen zu schaffen. Dabei wird parallel zum Produktivsystem ein identisches Ersatzsystem auf einem weiteren physischen Server aufgebaut und entweder ausgeschaltet (Cold-Standby) oder kurzfristig einschaltbar gehalten, aber nicht eingesetzt (Warm-Standby) oder eingeschaltet und synchron gespiegelt mit Daten versorgt (Hot-Standby). Sind entsprechende Maßnahmen umgesetzt, dann sinkt der Schutzbedarf (**Verteilungseffekt**). Es können unter anderem folgende Fälle auftreten:

- Die virtuellen Maschinen weisen in Bezug auf Verfügbarkeit den Schutzbedarf „normal" auf, dann gibt es in der Regel eine Kumulation nach „hoch" und dann durch Verteilung sinkt der Schutzbedarf wieder auf „normal". In diesem Fall reicht der Warm-Standby-Ansatz aus.
- Die virtuellen Maschinen haben den Schutzbedarf „hoch" in Bezug auf Verfügbarkeit. Aufgrund von Kumulation kann sich ein insgesamt sehr hoher Schutzbedarf ergeben, der dann wegen Verteilung auf „hoch" abgesenkt werden kann, wenn entsprechende Maßnahmen (z. B. Hot-Standby) umgesetzt werden.

Schutzbedarfsfeststellung beim Cloud-Computing (IaaS Compute)

Auch beim Cloud Computing ändert sich gegenüber der oben beschriebenen Schutzbedarfsfeststellung wenig. Bei Angeboten der Form „IaaS Compute" werden den Benutzern virtuelle Maschinen zur Verfügung gestellt, z. B. über eine Webschnittstelle. Ähnlich wie bei der Virtualisierung wird der Schutzbedarf des Virtualisierungsservers durch den Schutzbedarf der auf ihm betriebenen virtuellen IT-Systeme beeinflusst. Techniken wie Live Migration, vMotion oder XenMotion ermöglichen, dass die virtuellen Maschinen zwischen den Virtualisierungsservern verschoben werden oder Hostsysteme bei geringer Last in den Stand-by-Modus geschaltet oder sogar heruntergefahren werden können, um Strom zu sparen. Die Vorteile, die sich dadurch ergeben, sind unbestritten. Aber die Live Migration, also die Verschiebung von VMs zwischen Virtualisierungsservern, erschwert die Schutzbedarfsfest-

stellung. Daher wird empfohlen, die Cloud-Computing-Plattform für unterschiedliche Bereiche (Virtualisierungscluster) anzulegen, abhängig vom Schutzbedarf (zum Beispiel „normal“ oder „hoch“).

Anwendungen, die denselben Schutzbedarf aufweisen, sollten dann auf einem hierfür vorgesehenen Virtualisierungscluster betrieben werden. Die einzelnen Bereiche sollten untereinander physisch getrennt sein und es ist sicherzustellen, dass virtuelle Maschinen nicht bereichsübergreifend verschoben werden können.

Auf eine gesonderte Schutzbedarfsfeststellung für virtuelle IT-Systeme und Virtualisierungsserver kann verzichtet werden.

Hinweis:

Besitzen die meisten Anwendungen auf einem IT-System nur einen normalen Schutzbedarf und sind nur eine oder wenige hochschutzbedürftig, so sollte in Erwägung gezogen werden, die hochschutzbedürftigen Anwendungen auf ein isoliertes IT-System auszulagern, da dies wesentlich gezielter abgesichert werden kann und somit häufig kostengünstiger ist. Eine solche Alternative kann dem Management zur Entscheidung vorgelegt werden.

8.2.5 Schutzbedarfsfeststellung für ICS-Systeme

Im Bereich industrieller Steuerungsanlagen muss der Schutzbedarf aller ICS-Systeme festgestellt werden. Die ICS-Systeme wurden bereits in Kapitel 8.1.6 erfasst.

Bei der Feststellung des Schutzbedarfes für die ICS-Systeme muss berücksichtigt werden, dass nicht per se alle Objekte einem sehr hohen Schutzbedarf unterliegen. In enger Abstimmung ist es sinnvoll, mit den Verantwortlichen der ICS-Systeme in einem Gespräch die Schutzbedarfsfeststellung durchzuführen, da diese wissen, welche ICS-Geräte welche Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit haben. Der Schutzbedarf leitet sich hierbei aus dem Anwendungszweck der industriellen Steuerungsanlage ab.

Dabei sollte berücksichtigt werden, dass ICS-Systeme für verschiedene Aufgaben verwendet werden können. So kann in einer Produktionsstraße im Wechsel ein für ein Unternehmen wichtiges umsatzstarkes Produkt produziert werden und ein weniger umsatzstarkes Produkt. Bei der Feststellung des Schutzbedarfs müssen diese Abhängigkeiten beachtet werden (Maximumprinzip).

Für die Definition des Schutzbedarfes kann es sinnvoll sein, die für alle weiteren Schutzbedarfsfeststellungen definierten Klassifikationen zu übernehmen. Darüber hinaus können die Schutzbedarfskategorien entsprechend angepasst formuliert werden.

Beispiel: RECPLAST GmbH

Für ein IT-System aus einer Büroumgebung liegt eine Ausfallzeit von bis zu 30 Stunden im normalen Bereich. Diese Ausfallzeit kann auch für den Betrieb von ICS-Systemen sinnvoll sein, möglicherweise ist es jedoch erforderlich, die Ausfallzeit für die ICS-Geräte im normalen Schutzbedarf auf zwölf bis 24 Stunden zu reduzieren.

Der Schutzbedarf für jedes ICS-System wird bezüglich Vertraulichkeit, Integrität und Verfügbarkeit ermittelt. Der Gesamtschutzbedarf der ICS-Systeme leitet sich nach dem Maximumprinzip bezüglich der drei Grundwerte der Vertraulichkeit, Integrität und Verfügbarkeit ab.

Die Festlegungen des Schutzbedarfs von ICS-Systeme müssen kurz begründet werden, damit die Entscheidungen für Dritte nachvollziehbar sind.

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH								
Bezeichnung	**Beschreibung des Zielobjektes / der Gruppe der Zielobjekte**	**Plattform / Baustein**	**Vertraulichkeit**	**Begründung für die Vertraulichkeit**	**Integrität**	**Begründung für die Integrität**	**Verfügbarkeit**	**Begründung für die Verfügbarkeit**
S100	SPS	SPS	normal	Der Quellcode enthält nur wenige vertrauliche Informationen. Der Zugriff auf den Quellcode ist auf befugte Personen beschränkt.	sehr hoch	Die Konfigurationsdaten müssen jederzeit korrekt sein.	hoch	Die SPSen müssen jederzeit verfügbar sein. Bei Nichtverfügbarkeit kann die Produktion nicht weiterlaufen.
S101	SCADA	SCADA / HMI	normal	Der Quellcode enthält nur wenige vertrauliche Informationen. Der Zugriff auf den Quellcode ist auf befugte Personen beschränkt.	hoch	Die verarbeiteten Informationen müssen korrekt und vollständig vorhanden sein.	hoch	Ohne den Server können keine Informationen in der Produktion verarbeitet werden.
S103	Server für Betriebsdatenerfassung	Server unter Unix	normal	Maximumprinzip	sehr hoch	Die Betriebsdaten müssen zu jeder Zeit korrekt vorhanden sein	hoch	Ein Ausfall der Betriebsdatensteuerung ist bis 7 Stunden tolerierbar, da es einen entsprechenden Puffer in der Produktion gibt.
S104	Server für Betriebsdatenerfassung	Server unter Unix	normal	Maximumprinzip	sehr hoch	Die Betriebsdaten müssen zu jeder Zeit korrekt vorhanden sein	hoch	Ein Ausfall der Betriebsdatensteuerung ist bis 7 Stunden tolerierbar, da es einen entsprechenden Puffer in der Produktion gibt.

Abbildung 22: Auszug aus der Schutzbedarfsfeststellung der RECPLAST GmbH (ICS-Systeme)

8.2.6 Schutzbedarfsfeststellung für sonstige Geräte

Um den Schutzbedarf sonstiger Geräte festzustellen, muss zunächst bestimmt werden, für welche Geschäftsprozesse und Anwendungen diese Geräte eingesetzt werden und wie sich deren Schutzbedarf vererbt. Diese Informationen wurden in Kapitel 8.1.7 ermittelt. Dabei muss der Datenfluss über diese Geräte beachtet werden, über den sich der Schutzbedarf auf die dazwischenliegenden Netzkomponenten vererbt.

Um den Schutzbedarf eines Geräts zu ermitteln, müssen nun die möglichen Schäden der relevanten Geschäftsprozesse in ihrer Gesamtheit betrachtet werden. Die Ergebnisse der Schutzbedarfsfeststellung von Geräten sollten wiederum in einer Tabelle festgehalten werden, wenn diese Einfluss auf die Informationssicherheit haben. Um nicht beliebig viele Geräte in einer Institution erfassen zu müssen, sollten nur Geräte betrachtet werden, die die Informationssicherheit nennenswert beeinträchtigen könnten. Diese sollten möglichst zu Gruppen zusammengefasst und als ein Objekt behandelt werden.

Es sollte vermerkt werden, welchen Schutzbedarf jedes Gerät bezüglich Vertraulichkeit, Integrität und Verfügbarkeit hat. Der Gesamtschutzbedarf eines Geräts leitet sich wiederum aus dem Maximum des Schutzbedarfs bezüglich der drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit ab.

Die Festlegungen des Schutzbedarfs von Geräten müssen kurz begründet werden, damit die Entscheidungen auch für Außenstehende nachvollziehbar sind. Hier kann auf die Schutzbedarfsfeststellung der Geschäftsprozesse und Anwendungen zurückverwiesen werden.

In Institutionen werden je nach Branche unterschiedlichste Geräte eingesetzt, um die Geschäftsprozesse zu unterstützen. Neben IT-Systemen, die unmittelbar als solche zu identifizieren sind, können auch viele andere Arten von Geräten Einfluss auf die Informationssicherheit haben. Zu solchen Geräten gehören beispielsweise Geräte mit Funktionalitäten aus dem Bereich Internet of Things (IoT).

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH								
Bezeichnung	**Beschreibung des Zielobjektes / der Gruppe der Zielobjekte**	**Plattform / Baustein**	**Vertraulichkeit**	**Begründung für die Vertraulichkeit**	**Integrität**	**Begründung für die Integrität**	**Verfügbarkeit**	**Begründung für die Verfügbarkeit**
S200	Alarmanlage BG	Alarmanlage	normal	Es haben keine unbefugten Personen Zugriff auf die Alarmanlage.	sehr hoch	Aufgrund der sofortigen Meldung an die Feuerwehr und den entsprechenden Sensoren ist die Korrektheit der Daten sehr wichtig.	sehr hoch	Die Alarmanlage schützt das Gebäude und muss zu jeder Zeit verfügbar sein.
S201	Alarmanlage Beuel	Alarmanlage	normal	Es haben keine unbefugten Personen Zugriff auf die Alarmanlage.	sehr hoch	Aufgrund der sofortigen Meldung an die Feuerwehr und den entsprechenden Sensoren ist die Korrektheit der Daten sehr wichtig.	sehr hoch	Die Alarmanlage schützt das Gebäude und muss zu jeder Zeit verfügbar sein.
S202	Video-Überwachung	Server unter Unix	normal	Es haben keine unbefugten Personen Zugriff auf die Videodaten.	normal	Durch überlappende Aufnahmebereiche können veränderte Aufnahmen kompensiert werden.	hoch	Ein Ausfall der Videokameras kann durch weitere Maßnahmen kompensiert werden.
S203	Kühlschrank IT-Abteilung	Kühlschrank	normal	Der Kühlschrank erfasst keine vertraulichen Daten.	normal	Die gespeicherten Daten sollten korrekt sein, jedoch wird der Kühlschrank in einem separaten Netz betrieben.	normal	Der Kühlschrank kann bei einem Ausfall nicht geöffnet werden. Aufgrund der darin enthaltenen Lebensmittel ist ein Ausfall bis 12 Stunden tolerierbar.

Abbildung 23: Auszug aus der Schutzbedarfsfeststellung der RECPLAST GmbH (sonstige und IoT-Geräte)

Aktionspunkte zu 8.2.4, 8.2.5 und 8.2.6 Schutzbedarfsfeststellung für IT-, ICS-Systeme und sonstige Geräte

- Schutzbedarf der IT-, ICS-Systeme und sonstigen Geräte anhand des Schutzbedarfs der Geschäftsprozesse und Anwendungen ermitteln
- Abhängigkeiten, das Maximumprinzip und gegebenenfalls den Kumulations- beziehungsweise Verteilungseffekt berücksichtigen
- Pro System(-Gruppe) die Ergebnisse für Vertraulichkeit, Integrität und Verfügbarkeit sowie die Begründungen dokumentieren

8.2.7 Schutzbedarfsfeststellung für Räume

Aus den Ergebnissen der Schutzbedarfsfeststellung der Geschäftsprozesse und Anwendungen sowie der IT-Systeme, ICS- und sonstigen Geräte sollte abgeleitet werden, welcher Schutzbedarf für die jeweiligen Liegenschaften bzw. Räume daraus resultiert. Dieser Schutzbedarf leitet sich aus dem Schutzbedarf der im jeweiligen Raum installierten Objekte, verarbeiteten Informationen oder der Datenträger, die in diesem Raum gelagert und benutzt werden, nach dem Maximumprinzip ab. Dabei sollten eventuelle Abhängigkeiten und ein möglicher Kumulationseffekt berücksichtigt werden, wenn sich in einem Raum eine größere Anzahl von IT-Systemen oder ICS-Geräten, Datenträgern usw. befindet, wie typischerweise bei Serverräumen, Rechenzentren, Werkhallen oder Datenträgerarchiven. Für jede Schutzbedarfseinschätzung sollte eine Begründung dokumentiert werden.

Hilfreich ist auch hier eine tabellarische Erfassung der notwendigen Informationen, aufbauend auf der bereits vorher erstellten Übersicht über die erfassten Räume.

Beispiel: RECPLAST GmbH

Die folgende Tabelle zeigt einen Auszug aus den Ergebnissen der Schutzbedarfsfeststellung für die Räume der RECPLAST GmbH:

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH								
Bezeichnung	**Beschreibung des Zielobjektes / der Gruppe der Zielobjekte**	**Plattform / Baustein**	**Vertraulichkeit**	**Begründung für die Vertraulichkeit**	**Integrität**	**Begründung für die Integrität**	**Verfügbarkeit**	**Begründung für die Verfügbarkeit**
R001	Büroräume	Büroraum	normal	In den Büroräumen stehen ausreichend abschließbare Schränke zur Verfügung. Die Mitarbeiter sind angewiesen, vertrauliche Informationen nach Arbeitsende zu verschließen.	normal	Die Büroräume können verschlossen werden, Fremde haben keinen Zutritt	normal	Es stehen ausreichend Büroräume zur Verfügung.
R002	Besprechungsräume	Besprechungsraum	normal	In den Besprechungsräumen werden keine Unterlagen aufbewahrt.	normal	In den Besprechungsräumen werden keine Unterlagen aufbewahrt.	normal	Besprechungen können auch in anderen Räumlichkeiten durchgefürht werden.
R003	Häuslicher Arbeitsplatz	Telearbeit	normal	Am häuslichen Arbeitsplatz dürfen keine vertraulichen Dokumente bearbeitet werden.	normal	Es dürfen nur Daten am häuslichen Arbeitsplatz verarbeitet werden, deren Integrität den Schutzbedarf normal entsprechen.	normal	Ein Telearbeitsplatz wird nur sporadisch genutzt, der generelle Arbeitsplatz liegt innerhalb der RECPLAST in Büroräumen.
R004	Mobiler Arbeitsplatz	Mobiler Arbeitsplatz	normal	Mobil dürfen keine vertraulichen Dokumente bearbeitet werden.	normal	Es dürfen nur Daten am mobilen Arbeitsplatz verarbeitet werden, deren Integrität den Schutzbedarf normal entsprechen.	normal	Ein mobiler Arbeitsplatz wird nur sporadisch genutzt, der generelle Arbeitsplatz liegt innerhalb der RECPLAST in Büroräumen.

Abbildung 24: Auszug aus der Schutzbedarfsfeststellung der RECPLAST GmbH (Räume)

Aktionspunkte zu 8.2.7 Schutzbedarfsfeststellung für Räume
• Schutzbedarf der Räume aus dem Schutzbedarf der Geschäftsprozesse, Anwendungen und IT-Systeme, ICS- und sonstigen Geräte ableiten • Abhängigkeiten, das Maximumprinzip und gegebenenfalls den Kumulationseffekt berücksichtigen • Ergebnisse und Begründungen nachvollziehbar dokumentieren

8.2.8 Schutzbedarfsfeststellung für Kommunikationsverbindungen

Nachdem die Schutzbedarfsfeststellung für die betrachteten Geschäftsprozesse, Anwendungen, IT-Systeme, ICS- und sonstigen Geräte und Räume abgeschlossen wurde, wird nun der Schutzbedarf bezüglich der Vernetzungsstruktur erarbeitet. Grundlage für die weiteren Überlegungen ist der in Kapitel 8.1.4 *Netzplanerhebung* erarbeitete Netzplan des zu untersuchenden Informationsverbunds.

Um die Entscheidungen vorzubereiten, auf welchen Kommunikationsstrecken kryptografische Sicherheitsmaßnahmen eingesetzt werden sollten, welche Strecken redundant ausgelegt sein sollten und über welche Verbindungen Angriffe durch Innen- und Außentäter zu erwarten sind, müssen die Kommunikationsverbindungen analysiert werden. Hierbei werden folgende Kommunikationsverbindungen als kritisch gewertet:

- Kommunikationsverbindungen, die Außenverbindungen darstellen, d. h. die in oder über unkontrollierte Bereiche führen (z. B. ins Internet oder über öffentliches Gelände). Dazu können auch drahtlose Kommunikationsverbindungen gehören, da es hierbei schwierig ist, zu verhindern, dass auf diese von öffentlichem Gelände aus zugegriffen wird. Bei Außenverbindungen besteht die Gefahr, dass durch externe Angreifer Penetrationsversuche auf das zu schützende System vorgenommen oder Schadprogramme eingespielt werden können. Darüber hinaus könnten unter Umständen Innentäter über eine solche Verbindung vertrauliche Informationen nach außen übertragen. Auch in Bezug auf den Grundwert Verfügbarkeit sind Außenverbindungen oft besonders gefährdet. Es darf nicht vergessen werden, Außenverbindungen für die Fernadministration mit zu erfassen.
- Kommunikationsverbindungen, über die hochschutzbedürftige Informationen übertragen werden, wobei dies sowohl Informationen mit einem hohen Anspruch an Vertraulichkeit wie auch Integrität oder Verfügbarkeit sein können. Diese Verbindungen können das Angriffsziel vorsätzlichen Abhörens oder vorsätzlicher Manipulation sein. Darüber hinaus kann der Ausfall einer solchen Verbindung die Funktionsfähigkeit wesentlicher Teile des Informationsverbunds beeinträchtigen.
- Kommunikationsverbindungen, die im produzierenden Bereich eingesetzt werden, müssen im Netzplan ebenfalls erfasst werden. Dazu gehören (z. B. bei einer Netztrennung) die Kommunikationsverbindungen zwischen den Netzen.

Bei der Erfassung der kritischen Kommunikationsverbindungen kann wie folgt vorgegangen werden. Zunächst werden sämtliche „Außenverbindungen" als kritische Verbindungen identifiziert und erfasst. Anschließend werden sämtliche Verbindungen untersucht, die von einem IT-System oder einer Gruppe von IT-Systemen mit hohem oder sehr hohem Schutzbedarf ausgehen. Dabei werden diejenigen Verbindungen identifiziert, über die hochschutzbedürftige Informationen übertragen werden. Danach werden die Verbindungen untersucht, über die diese hochschutzbedürftigen Daten weiter-

geleitet werden. Abschließend sind die Kommunikationsverbindungen zu identifizieren, über die derlei Informationen nicht übertragen werden dürfen. Zu erfassen sind dabei:

- die Verbindungsstrecke,
- ob es sich um eine Außenverbindung handelt und
- ob hochschutzbedürftige Informationen übertragen werden und ob der Schutzbedarf aus der Vertraulichkeit, Integrität oder Verfügbarkeit resultiert.

Die Entscheidungen, welche Kommunikationsverbindungen als kritisch zu betrachten sind, sollten tabellarisch dokumentiert oder grafisch im Netzplan hervorgehoben werden.

Beispiel: RECPLAST GmbH

Für das Unternehmen RECPLAST GmbH ergeben sich die Kommunikationsverbindungen, die im Netzplan im Kapitel 8.1.4 *Netzplanerhebung* dargestellt wurden. Diese wurden bei der RECPLAST aufgrund von ähnlichen Anforderungen gruppiert und sowohl in der Strukturanalyse als auch in der Schutzbedarfsfeststellung beschrieben und bewertet. Anhand der folgenden Tabellen können die oben dargestellten Kommunikationsverbindungen nachvollzogen werden:

A.1 Strukturanalyse der RECPLAST GmbH									
Bezeichnung	**Beschreibung des Zielobjektes / der Gruppe der Zielobjekte**	**Plattform / Baustein**	**Ort**	**Gebäude**	**Raum**	**Anzahl**	**Status**	**Benutzer**	**Verantwortlich / Administrator**
K001	**Internet – Bonn BG** Internetverbindung für den Anschluss der RECPLAST an das Internet; dieser Anschluss ist gleichwertig mit dem Anschluss der Vertriebsstandorte an die RECPLAST	-	-	-	-	-	in Betrieb	Alle Mitarbeiter	IT-Betrieb
K002	**Standleitung Bonn BG – Bonn Beuel** Standleitung für die Anbindung der beiden Standorte in Bonn	-	-	-	-	-	in Betrieb	Alle Mitarbeiter	IT-Betrieb
K003	**Verbindungen zwischen Netzkomponenten innerhalb der RECPLAST** Verbindungen zwischen Routern, Switchen und Firewall, die in mindestens einem Schutzziel der Datenübertragung einen hohen Schutzbedarf aufweisen.	-	-	-	-	-	in Betrieb	Administratoren	IT-Betrieb
K004	**Verbindungen Netzkomponenten zu Servern innerhalb der RECPLAST** Verbindungen zwischen Netzkomponenten und Servern, die in mindestens einem Schutzziel der Datenübertragung einen hohen Schutzbedarf aufweisen.	-	-	-	-	-	in Betrieb	Administratoren	IT-Betrieb

A.1 Strukturanalyse der RECPLAST GmbH									
Bezeichnung	**Beschreibung des Zielobjektes / der Gruppe der Zielobjekte**	**Plattform / Baustein**	**Ort**	**Gebäude**	**Raum**	**Anzahl**	**Status**	**Benutzer**	**Verantwortlich / Administrator**
K005	**Verbindungen Netzkomponenten zu ICS-, IoT- oder sonstigen Geräten** Verbindungen zwischen den Netzkomponenten und ICS-, IoT- oder sonstigen Geräten, die in mindestens einem Schutzziel der Datenübertragung einen hohen Schutzbedarf aufweisen.	-	-	-	-	-	in Betrieb	Administratoren	IT-Betrieb
K006	**Verbindungen Netzkomponenten zu Arbeitsplätzen innerhalb der RECPLAST** Verbindungen zwischen den Netzkomponenten und den Clients oder Laptops, die in mindestens einem Schutzziel der Datenübertragung einen hohen Schutzbedarf aufweisen.	-	-	-	-	-	in Betrieb	Administratoren	IT-Betrieb

Abbildung 25: Auszug aus der Strukturanalyse der RECPLAST GmbH (Kommunikationsverbindungen)

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH								
Bezeichnung	**Beschreibung des Zielobjektes / der Gruppe der Zielobjekte**	**Plattform / Baustein**	**Vertraulichkeit**	**Begründung für die Vertraulichkeit**	**Integrität**	**Begründung für die Integrität**	**Verfügbarkeit**	**Begründung für die Verfügbarkeit**
K001	Internet – Bonn BG	-	hoch	Maximumprinzip Abgefangene Informationen können z.B. an den Wettbewerb gelangen.	hoch	Maximumprinzip Ein Großteil der Kommunikation erfolgt über das Internet. Falsche Informationen können z.B. den Ruf schädigen.	hoch	Maximumprinzip Es handelt sich hierbei um die Außenverbindung. Ohne Außenverbindung kann keine Kommunikation mehr stattfinden.
K002	Standleitung Bonn BG – Bonn Beuel	-	hoch	Maximumprinzip Die internen Informationen müssen vertraulich übertragen werden.	normal	Maximumprinzip Da die Standleitung durch die internen Administratoren abgesichert wurde, können Informationen nur mit hohem Aufwand verfälscht werden.	hoch	Maximumprinzip Ohne die Anbindung an den Produktionsstandort können dort keine Produktionsaufträge mehr bearbeitet werden.
K003	Verbindungen zwischen Netzkomponenten innerhalb der RECPLAST	-	normal	Informationen, die innerhalb der internen Netze übertragen werden, können nicht von Dritten eingesehen werden.	normal	Informationen, die innerhalb der internen Netze übertragen werden, können nicht von Dritten verändert werden.	hoch	Maximumprinzip Wenn eine interne Verbindung ausfällt, sind die Netzkomponenten nicht mehr erreichbar und der interne Datenfluss ist nicht mehr möglich.

Abbildung 26: Auszug aus der Schutzbedarfsfeststellung der RECPLAST GmbH (Kommunikationsverbindungen)

Aktionspunkte zu 8.2.8 Schutzbedarfsfeststellung für Kommunikationsverbindungen
• Außenverbindungen erfassen und in tabellarischer oder grafischer Form dokumentieren • Verbindungen, über die kritische Informationen übertragen werden, identifizieren • Alle kritischen Kommunikationsverbindungen in tabellarischer oder grafischer Form dokumentieren

8.2.9 Schlussfolgerungen aus den Ergebnissen der Schutzbedarfsfeststellung

Die bei der Schutzbedarfsfeststellung erzielten Ergebnisse bieten einen Anhaltspunkt für die weitere Vorgehensweise der Sicherheitskonzeption. Für den Schutz, der von den in den IT-Grundschutz-Bausteinen beschriebenen Sicherheitsanforderungen ausgeht, wird bezüglich der Schutzbedarfskategorien Folgendes angenommen:

Schutzwirkung von Sicherheitsanforderungen nach IT-Grundschutz	
Schutzbedarfskategorie „normal“	Sicherheitsanforderungen nach IT-Grundschutz sind im Allgemeinen ausreichend und angemessen.
Schutzbedarfskategorie „hoch“	Sicherheitsanforderungen nach IT-Grundschutz liefern eine Standard-Absicherung, sind aber unter Umständen alleine nicht ausreichend. Weitergehende Maßnahmen sollten auf Basis einer Risikoanalyse ermittelt werden.
Schutzbedarfskategorie „sehr hoch“	Sicherheitsanforderungen nach IT-Grundschutz liefern eine Standard-Absicherung, reichen aber alleine im Allgemeinen nicht aus. Die erforderlichen zusätzlichen Sicherheitsmaßnahmen müssen individuell auf der Grundlage einer Risikoanalyse ermittelt werden.

Tabelle 5: Schutzwirkung von Sicherheitsanforderungen nach IT-Grundschutz

Außer bei hohem oder sehr hohem Schutzbedarf muss eine Risikoanalyse auch dann durchgeführt werden, wenn die Objekte des betrachteten Informationsverbunds

- mit den existierenden Bausteinen des IT-Grundschutzes nicht hinreichend abgebildet (modelliert) werden können oder
- in Einsatzszenarien (Umgebung, Anwendung) betrieben werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

Ausführliche Informationen zur Risikoanalyse finden sich in Kapitel 8.5.

Bereiche mit unterschiedlichem Schutzbedarf

Bei der Schutzbedarfsfeststellung zeigt sich häufig, dass es Bereiche innerhalb des betrachteten Informationsverbunds gibt, in denen Informationen verarbeitet werden, die einen hohen oder sehr hohen Schutzbedarf haben. Auch wenn nur wenige, herausgehobene Daten besonders schutzbedürftig sind, führt die starke Vernetzung und Kopplung von IT-Systemen, ICS- und sonstigen Geräten und Anwendungen schnell dazu, dass sich der höhere Schutzbedarf nach dem Maximumprinzip auf andere Bereiche überträgt.

Um Risiken und Kosten einzudämmen, sollten daher Sicherheitszonen zur Trennung von Bereichen mit unterschiedlichem Schutzbedarf eingerichtet werden. Solche Sicherheitszonen können sowohl räumlich als auch technisch oder personell ausgeprägt sein.

Beispiele:

- *Räumliche Sicherheitszonen: Um nicht jeden einzelnen Büroraum permanent abschließen oder überwachen zu müssen, sollten Zonen mit starkem Besucherverkehr von hochschutzbedürftigen Bereichen getrennt werden. So sollten sich Besprechungs-, Schulungs- oder Veranstaltungsräume ebenso wie eine Kantine, die externes Publikum anzieht, in der Nähe des Gebäudeeingangs befinden. Der Zugang zu Gebäudeteilen mit Büros kann dann von einem Pförtner einfach überwacht werden. Besonders sensitive Bereiche wie eine Entwicklungsabteilung sollten mit einer zusätzlichen Zugangskontrolle, z. B. über Chipkarten, abgesichert werden.*
- *Technische Sicherheitszonen: Um vertrauliche Daten auf bestimmte Bereiche innerhalb eines LANs zu begrenzen und um zu verhindern, dass Störungen in bestimmten Komponenten oder Angriffe die Funktionsfähigkeit beeinträchtigen, ist es hilfreich, das LAN in mehrere Teilnetze aufzuteilen (siehe auch Baustein NET.1.1 Netzarchitektur und -design im IT-Grundschutz-Kompendium).*
- *Personelle Sicherheitszonen: Grundsätzlich sollten an jede Person immer nur so viele Rechte vergeben werden, wie es für die Aufgabenwahrnehmung erforderlich ist. Darüber hinaus gibt es auch verschiedene Rollen, die eine Person nicht gleichzeitig wahrnehmen sollte. So sollte ein Revisor nicht gleichzeitig in der Buchhaltung und in der IT-Administration arbeiten, da er sich nicht selbst kontrollieren kann und darf. Um die Vergabe von Zugangs- und Zutrittsrechte zu vereinfachen, sollten Personengruppen, die nicht miteinander vereinbare Funktionen wahrnehmen, in getrennten Gruppen oder Abteilungen arbeiten.*
- *Zonenkonzept bei virtualisierten Infrastrukturen:*
  Wird Virtualisierung eingesetzt, dann muss dies auch im technischen Zonenkonzept berücksichtigt werden. Virtualisierung bedeutet eine Konsolidierung der Server, d. h. die Möglichkeit, mehrere Server virtuell auf einem physischen Host zu betreiben. Hierbei können die eingesetzten Server unterschiedlichem Schutzbedarf unterliegen, aufgrund der verschiedenen Anwendungen und Dienste, die darauf laufen. Daher sollte vor einer Virtualisierung festgelegt werden, welche Dienste oder Anwendungen zusammen in einer virtuellen Umgebung betrieben werden dürfen und welche durch geeignete Maßnahmen separiert werden müssen. Bei der Segmentierung sollte darauf geachtet werden, dass alle Bereiche der IT-Infrastruktur („Server", „Netze", „Storage" und „Management") erfasst sind.
  Bei der Entscheidung, welche Systeme auf einer gemeinsamen physischen Hardware virtualisiert werden dürfen, ist Folgendes zu beachten:
- *Die Server sollten aus organisatorischer Sicht und aus Sicherheitsgründen sinnvoll in Zonen gruppiert werden. Zonen sollten nicht zusammen mit der Sicherheitskomponente, die für die Separierung der Zonen sorgt, virtualisiert werden.*
- *Welche Komponenten zusammen auf einer gemeinsamen physischen Hardware virtualisiert werden können, ist abhängig vom Schutzbedarf und Bedarfsträger.*
  Bedarfsträger können unterschiedliche Mandanten (Hosting-Szenarien), unterschiedliche Organisationseinheiten innerhalb eines Unternehmens oder einer Behörde oder unterschiedliche Verfahren sein. Im ersten Fall besteht die Herausforderung bei der Planung, ein gleiches Verständnis der Bedarfsträger über die verwendeten Schutzbedarfskategorien zu erreichen.

- *Zonenkonzept beim Cloud Computing:*

Um dem unterschiedlichen Schutzbedarf der Anwender Rechnung zu tragen, müssen Cloud-Computing-Plattformen mandantenfähig sein und eine verlässliche und durchgängige Trennung der Anwender über den kompletten Cloud-Computing-Stack (Server, Netze, Storage und Management) gewährleisten. Neben den gängigen Sicherheitsmaßnahmen wie Schadprogramm- und Spamschutz, IDS und IPS sollte auf Netzebene auf eine geeignete Segmentierung geachtet werden, indem abhängig vom Schutzbedarf Sicherheitszonen definiert und eingerichtet werden. Beispiele hierfür sind:

- *Sicherheitszone für das Management der Cloud*
- *Sicherheitszone für die Live Migration*
- *Sicherheitszone für das Storage-Netz*
- *Sicherheitszonen für die virtuellen Maschinen*

Darüber hinaus wird empfohlen, unterschiedliche Zonen für die Server-Hardware anhand des Schutzbedarfs einzurichten und diese untereinander unter Verwendung von Sicherheitsgateways zu trennen.

Bei der Planung neuer Geschäftsprozesse, Fachaufgaben oder Anwendungen sollte frühzeitig geprüft werden, ob es zweckmäßig ist, Sicherheitszonen einzurichten. Häufig kann dadurch in allen nachfolgenden Phasen bis hin zur Revision viel Arbeit gespart werden.

Aktionspunkte zu 8.2.9 Schlussfolgerungen aus den Ergebnissen der Schutzbedarfsfeststellung
• Prüfen, ob Objekte mit erhöhten Sicherheitsanforderungen in Sicherheitszonen konzentriert werden können • Objekte mit erhöhten Sicherheitsanforderungen für eine Risikoanalyse vormerken

8.3 Modellierung eines Informationsverbunds

Nachdem die notwendigen Informationen aus der Strukturanalyse und der Schutzbedarfsfeststellung vorliegen, besteht der nächste Schritt darin, den betrachteten Informationsverbund mithilfe der vorhandenen Bausteine aus dem IT-Grundschutz-Kompendium nachzubilden. Das Ergebnis ist ein IT-Grundschutz-Modell des Informationsverbunds, das aus verschiedenen, gegebenenfalls auch mehrfach verwendeten Bausteinen besteht und durch die Verwendung der Bausteine die sicherheitsrelevanten Aspekte des Informationsverbunds beinhaltet.

8.3.1 Das IT-Grundschutz-Kompendium

Das IT-Grundschutz-Kompendium (siehe [GSK]) kann in der jeweils aktuellen Fassung vom BSI-Webserver heruntergeladen oder beim Bundesanzeiger Verlag erworben werden.

Die IT-Grundschutz-Bausteine

Das IT-Grundschutz-Kompendium enthält für verschiedene Vorgehensweisen, Komponenten und IT-Systeme die Gefährdungslage, Sicherheitsanforderungen und weiterführende Informationen, die jeweils in einem Baustein zusammengefasst sind.

Um Innovationsschübe und Versionswechsel vor allem im IT-Bereich zu berücksichtigen, ist das IT-Grundschutz-Kompendium mithilfe seiner Bausteinstruktur modular aufgebaut und konzentriert sich auf die Darstellung der wesentlichen Sicherheitsanforderungen für die jeweiligen Bausteine. Damit ist es leicht erweiter- und aktualisierbar. Übergeordnet sind die Bausteine in prozess- und systemorientierte Bausteine aufgeteilt und nach zusammengehörigen Themen in ein Schichtenmodell einsortiert.

Die prozessorientierten Bausteine sind in die folgenden Schichten gruppiert:

- ISMS (Managementsysteme für Informationssicherheit)
- ORP (Organisation und Personal)
- CON (Konzepte und Vorgehensweisen)
- OPS (Betrieb)
- DER (Detektion und Reaktion)

Die systemorientierten Bausteine sind in die folgenden Schichten gruppiert:

- INF (Infrastruktur)
- NET (Netze und Kommunikation)
- SYS (IT-Systeme)
- APP (Anwendungen)
- IND (Industrielle IT)

Gefährdungen

In jedem Baustein wird zunächst die zu erwartende spezifische Gefährdungslage beschrieben. Ergänzend hierzu befindet sich im separaten Anhang der jeweiligen Bausteine eine Auflistung der elementaren Gefährdungen, die bei der Erstellung des Bausteins berücksichtigt wurden. Diese Gefährdungsliste ist Teil einer ersten Stufe der vereinfachten Risikoanalyse für typische Umgebungen der Informationsverarbeitung und bildet die Grundlage, auf Basis derer das BSI spezifische Anforderungen zusammengestellt hat, um ein angemessenes Niveau der Informationssicherheit in einer Institution zu gewährleisten. Der Vorteil dabei ist, dass die Anwender bei typischen Anwendungsfällen keine aufwändigen oder weiterführenden Analysen benötigen, um das für einen normalen Schutzbedarf notwendige Sicherheitsniveau zu erreichen. Vielmehr ist es ausreichend, die für die betrachteten Geschäftsprozesse, und ihrer notwendigen Ressourcen relevanten Bausteine zu identifizieren und die darin empfohlenen Anforderungen konsequent und vollständig zu erfüllen.

Auch wenn besondere Komponenten oder Einsatzumgebungen vorliegen, die im IT-Grundschutz nicht hinreichend behandelt werden, bietet das IT-Grundschutz-Kompendium dennoch eine wertvolle Arbeitshilfe. Die dann notwendige Risikoanalyse kann sich auf die elementaren Gefährdungen dieser Komponenten oder Rahmenbedingungen konzentrieren.

Sicherheitsanforderungen

In jedem Baustein werden die Sicherheitsanforderungen, die für den Schutz des betrachteten Gegenstands relevant sind, aufgeführt. Sie beschreiben, *was* zu dessen Schutz zu tun ist. Die Anforderungen sind in drei Kategorien unterteilt:

- **Basis-Anforderungen** müssen vorrangig erfüllt werden, da bei diesen Empfehlungen mit (relativ) geringem Aufwand der größtmögliche Nutzen erzielt werden kann. Es handelt sich um uneinge-

schränkte Anforderungen. Die Basis-Anforderungen sind ebenfalls die Grundlage für die Vorgehensweise „Basis-Absicherung".

- **Standard-Anforderungen** bauen auf den Basis-Anforderungen auf und adressieren den normalen Schutzbedarf. Sie sollten grundsätzlich erfüllt werden, aber nicht vorrangig. Die Ziele der Standard-Anforderungen müssen erreicht werden, um eine Standard-Absicherung zu erzielen. Es können sich aber durch die jeweiligen Rahmenbedingungen der Institution auch Gründe ergeben, warum eine Standard-Anforderung nicht wie beschrieben umgesetzt wird, sondern die Sicherheitsziele auf andere Weise erreicht werden. Wenn eine Standard-Anforderung durch andere Sicherheitsmaßnahmen erfüllt wird, müssen die dadurch entstehenden Auswirkungen sorgfältig abgewogen und geeignet dokumentiert werden.
- **Anforderungen bei erhöhtem Schutzbedarf** sind eine Auswahl von Vorschlägen für eine weiterführende Absicherung, die bei erhöhten Sicherheitsanforderungen oder unter bestimmten Rahmenbedingungen als Grundlage für die Erarbeitung geeigneter Anforderungen und Maßnahmen berücksichtigt werden können.

Die Bausteine wenden sich an Sicherheitsbeauftragte und Sicherheitsverantwortliche in Institutionen.

Umsetzungshinweise

Zusätzlich zu den Bausteinen des IT-Grundschutz-Kompendiums kann es Umsetzungshinweise geben. Diese beschreiben, wie die Anforderungen der Bausteine umgesetzt werden können, und enthalten dafür passende Sicherheitsmaßnahmen mit einer detaillierten Beschreibung. Die Sicherheitsmaßnahmen können als Grundlage für Sicherheitskonzeptionen verwendet werden, sollten aber unter Umständen noch an die Rahmenbedingungen der jeweiligen Institution angepasst werden.

Die Umsetzungshinweise adressieren jeweils die Personengruppen, die für die Umsetzung der Anforderungen aus den Bausteinen zuständig sind, beispielsweise den IT-Betrieb oder die Haustechnik. Diese Umsetzungshinweise werden für ausgewählte, vor allem für stark nachgefragte Themen bereitgestellt.

8.3.2 Modellierung eines Informationsverbunds: Auswahl von Bausteinen

Das erstellte IT-Grundschutz-Modell ist unabhängig davon, ob der Informationsverbund aus bereits im Einsatz befindlichen Komponenten besteht oder ob es sich um einen Informationsverbund handelt, der sich ganz oder teilweise im Planungsstadium befindet. Jedoch kann das Modell unterschiedlich verwendet werden:

- Das IT-Grundschutz-Modell eines bereits realisierten Informationsverbunds identifiziert über die verwendeten Bausteine die relevanten Sicherheitsanforderungen. Es kann in Form eines **Prüfplans** benutzt werden, um einen Soll-Ist-Vergleich durchzuführen.
- Das IT-Grundschutz-Modell eines geplanten Informationsverbunds stellt hingegen ein **Entwicklungskonzept** dar. Es beschreibt über die ausgewählten Bausteine, welche Sicherheitsanforderungen bei der Realisierung des Informationsverbunds erfüllt werden müssen.

Die Einordnung der Modellierung und die möglichen Ergebnisse verdeutlicht die folgende Abbildung:

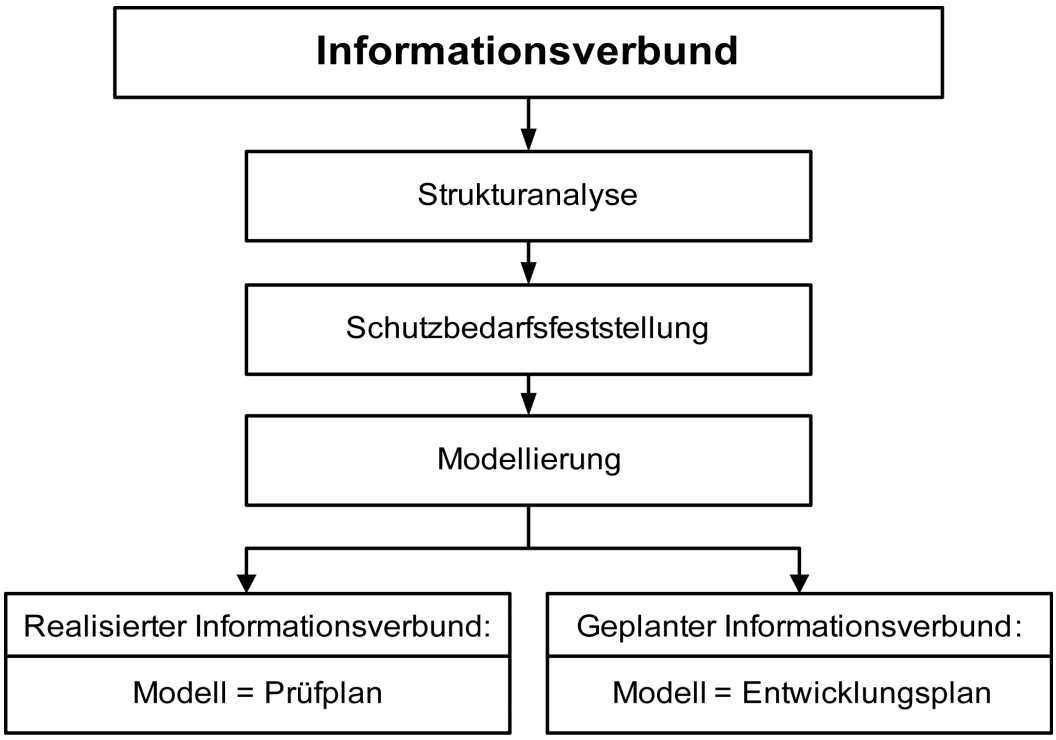


Abbildung 27: Ergebnis der Modellierung nach IT-Grundschutz

Typischerweise wird ein im Einsatz befindlicher Informationsverbund sowohl realisierte als auch in Planung befindliche Anteile umfassen. Das resultierende IT-Grundschutz-Modell beinhaltet dann sowohl einen Prüfplan wie auch Anteile eines Entwicklungskonzepts. Alle im Prüfplan bzw. im Entwicklungskonzept vorgesehenen Sicherheitsanforderungen bilden dann gemeinsam die Basis für die Erstellung des Sicherheitskonzepts. Dazu gehören neben den bereits erfüllten Sicherheitsanforderungen die bei Durchführung des Soll-Ist-Vergleichs als unzureichend oder gar nicht erfüllt identifizierten Anforderungen sowie diejenigen, die sich für die in Planung befindlichen Anteile des Informationsverbunds ergeben.

Um einen im Allgemeinen komplexen Informationsverbund nach IT-Grundschutz zu modellieren, müssen die passenden Bausteine des IT-Grundschutz-Kompendiums ausgewählt und umgesetzt werden. Um die Auswahl zu erleichtern, sind die Bausteine im IT-Grundschutz-Kompendium zunächst in prozess- und systemorientierte Bausteine aufgeteilt und diese jeweils in einzelne Schichten untergliedert.

Die Sicherheitsaspekte eines Informationsverbunds werden wie folgt den einzelnen Schichten zugeordnet:

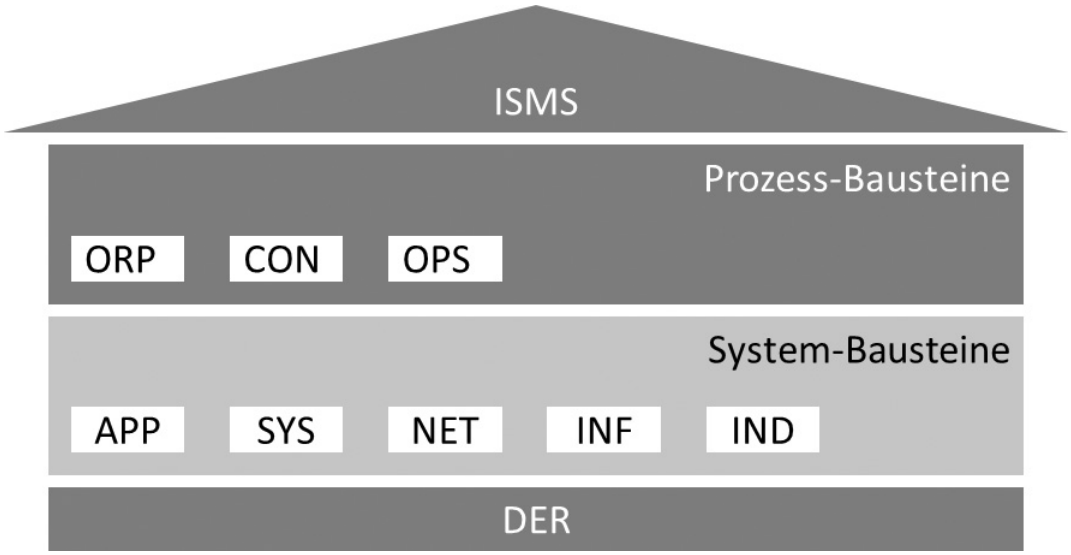


Abbildung 28: Das Schichtenmodell des IT-Grundschutzes

Prozessorientierte Bausteine:

- Die Schicht ISMS enthält als Grundlage für alle weiteren Aktivitäten im Sicherheitsprozess den Baustein *Sicherheitsmanagement.*
- In der Schicht ORP finden sich Bausteine, die organisatorische und personelle Sicherheitsaspekte abdecken, wie die Bausteine *Organisation* und *Personal*.
- Die Schicht CON enthält Bausteine, die sich mit Konzepten und Vorgehensweisen befassen. Typische Bausteine der Schicht CON sind unter anderem *Kryptokonzept* und *Datenschutz*.
- Die Schicht OPS umfasst alle Sicherheitsaspekte betrieblicher Art. Insbesondere sind dies die Sicherheitsaspekte des operativen IT-Betriebs, sowohl bei einem Betrieb im Haus als auch bei einem IT-Betrieb, der in Teilen oder komplett durch Dritte betrieben wird. Ebenso enthält er die Sicherheitsaspekte, die bei einem IT-Betrieb für Dritte zu beachten sind. Beispiele für die Schicht OPS sind die Bausteine *Schutz vor Schadprogrammen* und *Outsourcing* für Kunden.
- In der Schicht DER finden sich alle Bausteine, die für die Überprüfung der umgesetzten Sicherheitsmaßnahmen und insbesondere für die Detektion von Sicherheitsvorfällen sowie die geeigneten Reaktionen darauf relevant sind. Typische Bausteine der Schicht DER sind *Behandlung von Sicherheitsvorfällen* und *Forensik*.

System-Bausteine:

- Die Schicht APP beschäftigt sich mit der Absicherung von Anwendungen und Diensten, unter anderem in den Bereich Kommunikation, Verzeichnisdienste, netzbasierte Dienste sowie Business- und Client-Anwendungen. Typische Bausteine der Schicht APP sind *Groupware*, *Office-Produkte*, *Webserver* und *Browser.*
- Die Schicht SYS betrifft die einzelnen IT-Systeme des Informationsverbunds, die gegebenenfalls in Gruppen zusammengefasst wurden. Hier werden die Sicherheitsaspekte von Servern, Desktop-Systemen, Mobile Devices und sonstigen IT-Systemen wie Druckern und TK-Anlagen behandelt. Zur Schicht SYS gehören beispielsweise Bausteine zu konkreten Betriebssystemen, *Smartphones* und *Tablets* und *Drucker, Kopierer* und *Multifunktionsgeräte*.

- Die Schicht NET betrachtet die Vernetzungsaspekte, die sich nicht auf bestimmte IT-Systeme, sondern auf die Netzverbindungen und die Kommunikation beziehen. Dazu gehören z. B. die Bausteine *Netzmanagement*, *Firewall* und *WLAN-Betrieb*.
- Die Schicht INF befasst sich mit den baulich-technischen Gegebenheiten, hier werden Aspekte der infrastrukturellen Sicherheit zusammengeführt. Dies betrifft unter anderem die Bausteine *Gebäude und Rechenzentrum*.
- Die Schicht IND befasst sich mit Sicherheitsaspekten industrieller IT. In diese Schicht fallen beispielsweise die Bausteine *Maschine*, *Sensoren* und *Speicherprogrammierbare Steuerung (SPS)*.

Die Einteilung in diese Schichten hat folgende Vorteile:

- Die Komplexität der Informationssicherheit wird reduziert, indem eine sinnvolle Aufteilung der Einzelaspekte vorgenommen wird.
- Da übergeordnete Aspekte und gemeinsame infrastrukturelle Fragestellungen getrennt von den IT-Systemen betrachtet werden, kommt es zu einer Vermeidung von Redundanzen, weil diese Aspekte nur einmal bearbeitet werden müssen und nicht wiederholt für jedes IT-System.
- Die einzelnen Schichten sind so gewählt, dass auch die Zuständigkeiten für die betrachteten Aspekte gebündelt sind. So betreffen beispielsweise die Schichten ISMS und ORP Grundsatzfragen des sicheren Umgangs mit Informationen, die Schicht INF den Bereich Haustechnik, die Schicht SYS die Zuständigen für die IT-Systeme, die Schicht NET die Ebene der Netzadministratoren und die Schicht APP schließlich die Anwendungsverantwortlichen und -betreiber.
- Aufgrund der Aufteilung der Sicherheitsaspekte in Schichten können Einzelaspekte in resultierenden Sicherheitskonzepten leichter aktualisiert und erweitert werden, ohne dass andere Schichten umfangreich tangiert werden.

Die Modellierung nach dem IT-Grundschutz besteht nun darin, für die Bausteine einer jeden Schicht zu entscheiden, ob und wie sie zur Abbildung des Informationsverbunds herangezogen werden können. Je nach betrachtetem Baustein können die Zielobjekte dieser Abbildung von unterschiedlicher Art sein: einzelne Geschäftsprozesse oder Komponenten, Gruppen von Komponenten, Gebäude, Liegenschaften, Organisationseinheiten usw.

8.3.3 Reihenfolge der Baustein-Umsetzung

Um grundlegende Risiken abzudecken und eine ganzheitliche Informationssicherheit aufzubauen, müssen die essenziellen Sicherheitsanforderungen frühzeitig erfüllt und entsprechende Sicherheitsmaßnahmen umgesetzt werden. Daher wird im IT-Grundschutz eine Reihenfolge für die umzusetzenden Bausteine vorgeschlagen.

Im IT-Grundschutz-Kompendium ist im Kapitel *Schichtenmodell und Modellierung* beschrieben, wann ein einzelner Baustein sinnvollerweise eingesetzt werden soll und auf welche Zielobjekte er anzuwenden ist. Außerdem sind die Bausteine danach gekennzeichnet, ob sie vor- oder nachrangig umgesetzt werden sollten.

- R1: Diese Bausteine sollten vorrangig umgesetzt werden, da sie die Grundlage für einen effektiven Sicherheitsprozess bilden.
- R2: Diese Bausteine sollten als Nächstes umgesetzt werden, da sie in wesentlichen Teilen des Informationsverbunds für nachhaltige Sicherheit erforderlich sind.

- R3: Diese Bausteine werden zur Erreichung des angestrebten Sicherheitsniveaus ebenfalls benötigt und müssen umgesetzt werden, es wird aber empfohlen, diese erst nach den anderen Bausteinen zu betrachten

Mit R1 sind die Bausteine gekennzeichnet, die notwendig sind, um ein grundlegendes Sicherheitsgerüst zu erreichen. Es handelt sich um die Bausteine der Bereiche

- ISMS Managementsysteme für Informationssicherheit,
- ORP Organisation und Personal,
- OPS.1.1 Kern-IT-Betrieb.

Die im zweiten und dritten Schritt umzusetzenden Bausteine (R2 und R3) finden sich in allen anderen Schichten des IT-Grundschutz-Kompendiums.

Diese Kennzeichnung zeigt nur die sinnvolle zeitliche Reihenfolge für die Umsetzung der Anforderungen des jeweiligen Bausteins auf und stellt keine Gewichtung der Bausteine untereinander dar. Grundsätzlich müssen alle für den jeweiligen Informationsverbund relevanten Bausteine des IT-Grundschutz-Kompendiums umgesetzt werden.

Die Kennzeichnung der Bausteine stellt außerdem nur eine Empfehlung dar, in welcher Reihenfolge die verschiedenen Bausteine sinnvoll umgesetzt werden könnten. Jede Institution kann hier eine davon abweichende, für sich sinnvolle Reihenfolge festlegen.

8.3.4 Zuordnung von Bausteinen

Die IT-Grundschutz-Modellierung, also die Zuordnung von Bausteinen zu Zielobjekten, sollte in Form einer Tabelle mit folgenden Spalten dokumentiert werden:

- Nummer und Titel des Bausteins
- Relevanz: Diese Spalte dient der Entscheidung, ob ein Baustein für den zu modellierenden Informationsverbund relevant ist oder nicht. Sie liefert einen schnellen Überblick darüber, ob kein Baustein vergessen wurde.
- Zielobjekt: Wenn ein Baustein für den Informationsverbund relevant ist, erfolgt über diese Spalte die Zuordnung zum Zielobjekt bzw. einer Zielobjektgruppe.
- Begründung: In dieser Spalte können Randinformationen und Begründungen für die Modellierung dokumentiert werden. Sind Bausteine für den betrachteten Informationsverbund nicht relevant, sollte dies hier explizit begründet werden.
- Ansprechpartner: Der konkrete Ansprechpartner wird nicht im Rahmen der Modellierung, sondern erst bei der Planung des eigentlichen Soll-Ist-Vergleichs im IT-Grundschutz-Check ermittelt. Basierend auf den Rollen und Verantwortlichen, die in den Bausteinen genannten werden, kann hier jedoch schon eine entsprechende Vorarbeit geleistet werden.

Beispiel: RECPLAST GmbH

Die folgende Tabelle ist ein Auszug aus der Modellierung für das Unternehmen RECPLAST GmbH:

A.3 Modellierung der RECPLAST GmbH				
Nummer und Titel des Bausteins	**Relevanz**	**Zielobjekt**	**Begründung**	**Ansprechpartner**
APP.5.2 Microsoft Exchange / Outlook	nein		Wird nicht eingesetzt.	
APP 3.6 DNS-Server	ja	S019		
Benutzerdef.BS.1 PC für die Industriesteuerung	ja	C005		
CON.7: Informationssicherheit auf Auslandsreisen	nein		Auslandsreisen sind für Informationsverbund nicht relevant.	
INF.1 Allgemeines Gebäude	ja	G001		
INF.7 Datenträgerarchiv	nein		Es gibt kein Datenträgerarchiv.	
INF.4 IT-Verkabelung	ja	Informationsverbund		
ISMS.1 (Sicherheitsmanagement)	ja	Informationsverbund		
NET.1.1 Netz-Architektur und -design	ja	Informationsverbund		
NET.3.1 Router und Switches	ja	S033		
OPS.1.1.2 Ordnungsgemäße IT-Administration	nein		Die IT-Administration findet außerhalb des Informationsverbundes statt.	
OPS.2.4 Fernwartung	ja	Informationsverbund		
SYS.1.3 Server unter Unix	ja	S020		
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte	ja	S048		

Abbildung 29: Auszug aus der Modellierung der RECPLAST GmbH

Eine detaillierte Beschreibung der Vorgehensweise zur Modellierung eines Informationsverbunds findet sich im IT-Grundschutz-Kompendium im Kapitel *Schichtenmodell und Modellierung*.

8.3.5 Modellierung bei Virtualisierung und Cloud-Systemen

Grundsätzlich erfolgt die Modellierung virtueller IT-Systeme nach den gleichen Regeln wie bei eigenständigen physischen IT-Systemen, d. h. es sind die Hinweise in Kapitel 2 des IT-Grundschutz-Kompendiums zu beachten. Die Zuordnung der IT-Grundschutz-Bausteine richtet sich bei IT-Komponenten in erster Linie nach der Funktion des IT-Systems (Server, Client, usw.), nach dem verwendeten Betriebssystem (Linux, Windows usw.) und nach den darauf betriebenen Applikationen (Datenbank, Webserver usw.).

Bei Virtualisierungssoftware gibt es Produkte, die ein unterliegendes Betriebssystem benötigen (hostbasierte Virtualisierungslösungen), und andere, die direkt auf der physischen Hardware laufen (Bare Metal Virtualisierung), ohne unterliegendes Betriebssystem. Falls unterhalb der Virtualisierungsschicht ein vollwertiges und eigenständiges Betriebssystem eingesetzt wird, muss der dazu passende Baustein ebenfalls zugeordnet werden (z. B. aus SYS.1.2 *Windows-Server*), unabhängig von den virtuellen IT-Systemen.

Wurde der Hypervisor direkt auf der physischen Hardware installiert (Bare Metal Virtualisierung) handelt es sich hierbei um ein Zielobjekt, das im IT-Grundschutz-Kompendium nicht enthalten ist, da es sich hierbei um ein sehr spezielles Zielobjekt handelt. Daher muss eine Risikoanalyse für das entsprechende Zielobjekt durchgeführt und die Ergebnisse sollten anschließend mit den Anforderungen des Bausteins SYS.1.5 *Virtualisierung* konsolidiert werden.

Beispielszenario:

Als Beispiel wird ein physischer Server S1 betrachtet, auf dem mithilfe einer Virtualisierungssoftware die drei virtuellen Server VM1, VM2 und VM3 betrieben werden. Als Basis-Betriebssystem kommt auf dem physischen Server S1 eine Linux-Version zum Einsatz. Die Virtualisierungsschicht ist in diesem Beispiel eine Software-Komponente, die unter Linux läuft, also eine hostbasierte Servervirtualisierung (Typ 2). Die beiden virtuellen Server VM1 und VM2 werden mit Windows 2012 betrieben, auf VM3 ist hingegen Linux installiert. Applikationen können sowohl auf den drei virtuellen Servern als auch (unter Umgehung der Virtualisierungsschicht) direkt auf dem Basis-Betriebssystem des physischen Servers S1 ablaufen. Die folgende Abbildung zeigt ein Schema dieser Beispielkonfiguration:

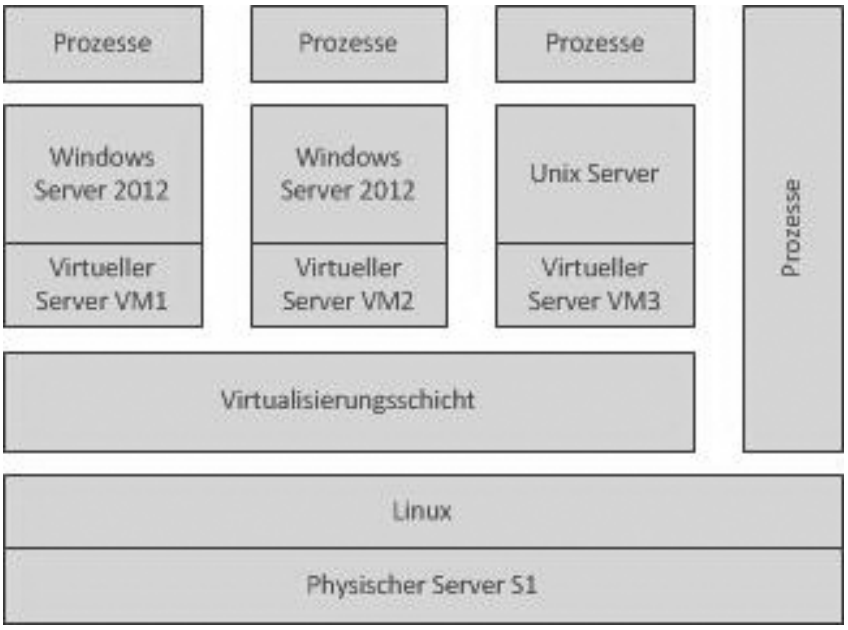


Abbildung 30: Schema einer Beispielkonfiguration

Baustein	Zielobjekt
SYS.1.1 *Allgemeiner Server*	S1
SYS.1.1 *Allgemeiner Server*	VM3
SYS.1.1 *Allgemeiner Server*	Gruppe aus VM1 und VM2
SYS.1.3 *Server unter Unix*	S1
SYS.1.3 *Server unter Unix*	VM3
SYS.1.2.2 *Windows Server 2012*	Gruppe aus VM1 und VM2

Tabelle 6: Zuordnung Bausteine aus Virtualisierungsschicht zu Zielobjekten

Modellierung beim Cloud-Computing

Um eine angemessene Gesamtsicherheit für den IT-Betrieb von Cloud-Diensten zu erreichen, müssen alle Cloud-Dienste (mit ihren zugeordneten virtuellen IT-Systemen, Netzen und weiteren Cloud-Komponenten) systematisch in der Sicherheitskonzeption berücksichtigt werden. Alle über Cloud-Dienste bereitgestellten IT-Systeme, Netze und Anwendungen, die sich einerseits in der Betriebsverantwortung und andererseits im Geltungsbereich des ISMS des Cloud-Diensteanbieters befinden, müssen in der Modellierung gemäß der IT-Grundschutz-Vorgehensweise berücksichtigt werden. Hierbei kann der Geltungsbereich des Informationsverbunds gleichzeitig als Grenze der Verantwortlichkeit verstanden werden: An der Grenze des Informationsverbunds endet die Verantwortung des Cloud-Diensteanbieters und beginnt die Verantwortung des Cloud-Anwenders. Der Umfang des Informationsverbunds unterscheidet sich dabei je nach dem Servicemodell.

Modellierung von IaaS-Angeboten

Bei IaaS (Infrastructure as a Service) ist der Cloud-Diensteanbieter für den Verwaltungsserver für die Cloud und den Virtualisierungsserver verantwortlich. Deshalb kommen bei IaaS aus den Schichten APP *(Anwendungen)* und SYS *(IT-Systeme)* nur die Verwaltungs- und die Virtualisierungssoftware als Zielobjekte vor. Für diese müssen somit die zugehörigen Bausteine ausgewählt werden. Nach der IT-Grundschutz-Vorgehensweise sind dies die Bausteine für *IT-Systeme als Server* (Schicht SYS.1). Für den Cloud-Verwaltungsserver müssen die Bausteine SYS 1.5 *Virtualisierung* und OPS.3.2 *Cloud-Anbieter* umgesetzt werden.

Für IaaS stellt der Cloud-Diensteanbieter nicht mehr als eine virtuelle „Hülle" über ein virtuelles Netz bereit. Die Absicherung des Netzes nach IT-Grundschutz verantwortet bei IaaS der Cloud-Diensteanbieter, wohingegen die Cloud-Anwender die IT-Systeme des Cloud-Angebotes verantworten. Für das Netz sind die passenden Bausteine aus der Schicht *Netze und Kommunikation* zu modellieren (z. B. NET.1.1 *Netzarchitektur und -design*). In der Regel wird dem virtuellen Server ein Speicherkontingent aus einem Speichernetz zugeordnet, hierfür ist der Baustein SYS.1.8 *Speicherlösungen/Cloud Storage* ebenfalls vom Cloud-Diensteanbieter umzusetzen.

Ein virtueller Server aus der Cloud, der per IaaS angeboten wird, wird durch den Cloud-Anwender konfiguriert. Die Umsetzungsverantwortung für seine Sicherheitsmaßnahmen liegt somit ebenfalls beim Cloud-Anwender. Im Hinblick auf die Abgrenzung des Informationsverbunds des Cloud-Diensteanbieters befindet sich also dieser virtuelle Server außerhalb des Informationsverbunds des Cloud-Diensteanbieters.

Die Schnittstelle zur Bereitstellung von IaaS-Cloud-Diensten (Self-Service-Portal) ist durch geeignete Mechanismen zur Netztrennung (z. B. über Netze, virtuelle Firewalls, Routing) vom Cloud-Diensteanbieter abzusichern und gegebenenfalls der Baustein APP.3.1 *Webanwendungen* umzusetzen.

Eine Modellierung der IaaS-Server als IT-Systeme im Sicherheitskonzept des Cloud-Diensteanbieters ist möglich, allerdings nicht notwendig, da die Cloud-Anwender diese IT-Systeme verwalten.

Modellierung von PaaS-Angeboten

Bei PaaS (Platform as a Service) ist der Cloud-Diensteanbieter zusätzlich zu IaaS für die sichere Bereitstellung eines virtuellen Servers und einer angebotenen Plattform verantwortlich (z. B. einer Datenbank oder eines Webservers). Dementsprechend muss der Cloud-Diensteanbieter im Servicemodell PaaS zunächst, wie bei IaaS, den Cloud-Verwaltungsserver und dessen Verwaltungssoftware modellieren. Dort erfolgt zentral die Zuordnung des Bausteins OPS.3.2 *Cloud-Anbieter*.

Darüber hinaus muss der Cloud-Diensteanbieter ein IT-System mit dem entsprechenden Betriebssystem modellieren. Zu diesem IT-System ist je nach Cloud-Dienst auf Anwendungsschicht eine Datenbank oder ein Webserver zu modellieren.

Das PaaS-IT-System mit den verbundenen Cloud-Anwendungen muss für jeden Cloud-Mandanten modelliert werden, wobei Mandanten mit gleichen Plattformen, gleichen Anwendungen und gleichem Schutzbedarf gemäß den Vorgaben in Kapitel 8.1.1 *Komplexitätsreduktion durch Gruppenbildung* in einer Gruppe zusammengefasst werden können.

In der Praxis werden Cloud-Dienste des Servicemodells PaaS über virtuelle Profile bereitgestellt, die für mehrere Cloud-Anwender bzw. Mandanten eingesetzt werden können. Es bietet sich daher in der IT-Grundschutz-Modellierung an, diese Kombinationen in Form von Musterservern zu modellieren und pro Mandant zu verknüpfen bzw. zu vervielfachen.

Modellierung von SaaS-Angeboten

Bei SaaS (Software as a Service) müssen zunächst die für die unterliegende Cloud-Infrastruktur relevanten Zielobjekte wie bei IaaS und PaaS identifiziert und entsprechenden Bausteinen zugeordnet werden.

Im Vergleich zu PaaS werden bei SaaS weitere Anwendungen auf den Cloud-IT-Systemen modelliert (z. B. ein Webservice, eine Webanwendung oder ein SAP-System). Bei SaaS ist der Cloud-Diensteanbieter praktisch für den gesamten Cloud-Computing-Stack (Server, Netze, Storage, Management und Anwendungen) verantwortlich. Die SaaS-Anwendungen liegen auch in seinem Verantwortungsbereich und müssen somit in seinem Informationsverbund modelliert werden. Dabei können sowohl mehrfache Ausprägungen derselben SaaS-Anwendung als auch Gruppen von SaaS-Anwendungen gemäß den Vorgaben in Kapitel 8.1.1 zusammengefasst werden, wenn die dort angegebenen Voraussetzungen erfüllt sind.

8.3.6 Anpassung der Baustein-Anforderungen

Über die Modellierung wurden die Bausteine des IT-Grundschutz-Kompendiums ausgewählt, die für die einzelnen Zielobjekte des betrachteten Informationsverbunds umzusetzen sind. In den Bausteinen werden die Sicherheitsanforderungen aufgeführt, die typischerweise für diese Komponenten geeignet und angemessen sind.

Für die Erstellung eines Sicherheitskonzepts oder für ein Audit müssen jetzt die einzelnen Anforderungen bearbeitet und darauf aufbauend geeignete Sicherheitsmaßnahmen formuliert werden.

Die Anforderungen sind knapp und präzise. Sie geben die Teilziele vor, die zusammen zur Umsetzung der Ziele eines Bausteins beitragen. Die Sicherheitsanforderungen müssen daher noch in Handlungsvorgaben für die verschiedenen Akteure im Sicherheitsprozess umgewandelt werden. Dafür müssen auf Basis der Anforderungen Sicherheitsmaßnahmen ausgearbeitet werden, die

- an die jeweiligen Rahmenbedingungen und den Sprachgebrauch einer Institution angepasst sein müssen,
- ausreichend konkret sind, um im vorliegenden Informationsverbund angewendet zu werden, also z. B. ausreichend technische Details enthalten.

Generell sollten die Anforderungen der IT-Grundschutz-Bausteine immer sinngemäß umgesetzt werden. Alle Änderungen gegenüber dem IT-Grundschutz-Kompendium sollten dokumentiert werden, damit die Gründe auch später noch nachvollziehbar sind.

Zu vielen Bausteinen des IT-Grundschutz-Kompendiums gibt es Umsetzungshinweise, in denen zu den Sicherheitsanforderungen detailliertere Maßnahmen beschrieben sind. Diese Maßnahmen sind einerseits so allgemein formuliert, dass sie in möglichst vielen Umgebungen anwendbar sind, und andererseits so ausführlich, dass die Maßnahmenbeschreibungen als Umsetzungshilfe dienen können.

Auch die in den Umsetzungshinweisen vorgeschlagenen Maßnahmen sollten noch an die jeweiligen Rahmenbedingungen einer Institution angepasst werden. Es kann beispielsweise sinnvoll sein,

- Maßnahmen weiter zu konkretisieren, also z. B. um technische Details zu ergänzen,
- Maßnahmen dem Sprachgebrauch der Institution anzupassen, also z. B. andere Rollenbezeichnungen zu verwenden, und
- aus Maßnahmen die im betrachteten Bereich nicht relevanten Empfehlungen zu streichen.

Um den Anwendern die zielgruppengerechte Anpassung der IT-Grundschutz-Texte zu erleichtern, werden sämtliche Texte, Bausteine, Umsetzungshinweise, Tabellen und Hilfsmittel auch in elektronischer Form zur Verfügung gestellt. Damit können diese Texte bei der Erstellung eines Sicherheitskonzepts und bei der Realisierung von Sicherheitsmaßnahmen weiterverwendet werden.

Bei der Sichtung der Sicherheitsanforderungen kann sich ergeben, dass einzelne Anforderungen unter den konkreten Rahmenbedingungen nicht umgesetzt werden können. Dies kann beispielsweise der Fall sein, wenn die Anforderungen in der betrachteten Umgebung nicht relevant sind (z. B. weil Dienste nicht aktiviert wurden). In seltenen Fällen kann dies auch im Bereich der uneingeschränkt notwendigen Basis-Anforderungen vorkommen, wenn deren Umsetzung essenzielle Schwierigkeiten in anderen Bereichen mit sich bringen würde. Dies könnte beispielsweise der Fall sein, wenn sich Anforderungen des Brand- und des Einbruchschutzes nicht miteinander vereinbaren lassen würden. Dann müssten andere Lösungen gefunden und dies nachvollziehbar dokumentiert werden.

Werden Sicherheitsanforderungen zusätzlich aufgenommen oder geändert, muss dies im Sicherheitskonzept dokumentiert werden. Dies erleichtert auch die Durchführung des IT-Grundschutz-Checks.

Bei der Auswahl und Anpassung der Sicherheitsmaßnahmen auf Basis der Anforderungen ist zu beachten, dass diese immer angemessen sein müssen. Angemessen bedeutet:

- Wirksamkeit (Effektivität): Sie müssen vor den möglichen Gefährdungen wirksam schützen, also den identifizierten Schutzbedarf abdecken.

- Eignung: Sie müssen in der Praxis tatsächlich umsetzbar sein, dürfen also z. B. nicht die Organisationsabläufe zu stark behindern oder andere Sicherheitsmaßnahmen aushebeln.
- Praktikabilität: Sie sollen leicht verständlich, einfach anzuwenden und wenig fehleranfällig sein.
- Akzeptanz: Sie müssen für alle Benutzer anwendbar (barrierefrei) sein und dürfen niemanden diskriminieren oder beeinträchtigen.
- Wirtschaftlichkeit: Mit den eingesetzten Mitteln sollte ein möglichst gutes Ergebnis erreicht werden. Die Sicherheitsmaßnahmen sollten also einerseits das Risiko bestmöglich minimieren und andererseits in geeignetem Verhältnis zu den zu schützenden Werten stehen.

8.3.7 Einbindung externer Dienstleister

Viele Institutionen setzen externe oder interne Dienstleister ein, um Geschäftsprozesse ganz oder teilweise durch diese durchführen zu lassen. Grundsätzlich kann die Einbindung externer Dienstleister auf viele Arten erfolgen, z. B. in Form von Personal, das temporär eingesetzt wird, oder in Form von Auslagerungen von IT-Systemen.

Bereits im Vorfeld der Einbindung externer Dienstleister müssen die Aufgaben im Bereich der Informationssicherheit abgegrenzt und die Schnittstellen genau festgelegt werden. Aufgaben können an externe Dienstleister ausgelagert werden, die Verantwortung für die Informationssicherheit verbleibt jedoch immer bei der auslagernden Institution.

Es muss geklärt sein, welche sicherheitsrelevanten Aufgaben durch den externen Dienstleister und welche durch das eigene Sicherheitsmanagement abgedeckt werden. Folgende Fragen sollten vor der Einbindung externer Dienstleister grundlegend geregelt werden:

- Welche Geschäftsprozesse, welche IT-Systeme oder welche Dienstleistungen sollen an einen externen Dienstleister ausgelagert werden?
- Welchen Schutzbedarf haben die Zielobjekte, die durch einen externen Dienstleister oder im Outsourcing verarbeitet werden?
- Auf welche Zielobjekte und welche Informationen hat der externe Dienstleister Zugriff? Hier muss einerseits berücksichtigt werden, welche Zielobjekte und Informationen im Fokus der Dienstleistungserbringung stehen, aber andererseits auch, auf welche Zielobjekte und Informationen die Dienstleister zugreifen könnten, wie z. B. Reinigungskräfte auf Informationen in Büroräumen.

Sofern sich eine Institution für die Einbindung externer Dienstleister entscheidet, müssen neben vertraglichen Rahmenbedingungen ebenfalls die Voraussetzungen für die Umsetzung der Anforderungen des IT-Grundschutzes erfüllt werden. Generell muss die Modellierung der Bausteine getrennt für die eigene Institution und für jeden externen Dienstleister durchgeführt werden. Die Vorgehensweise der Modellierung erfolgt wie in Kapitel 8.3.4 „Zuordnung von Bausteinen“ beschrieben.

Auch bei der Einbindung externer Dienstleister muss es zu jedem Zeitpunkt für die auslagernde Institution möglich sein, die Risiken im Bereich der Informationssicherheit zu identifizieren und zu kontrollieren. Informationen und Geschäftsprozesse müssen immer auf einem vergleichbaren Niveau gemäß den Sicherheitszielen der Institution geschützt werden, auch wenn externe Dienstleister (oder wiederum deren Dienstleister) diese ganz oder in Teilen verarbeiten. Des Weiteren ist eine hohe Ereignistransparenz erforderlich, d. h., es muss Mechanismen geben, die gewährleisten, dass Gefährdungen und Risiken, die Auswirkungen auf die Dienstleistungen haben könnten, erkannt und entsprechend kommuniziert werden.

Hierfür ist es erforderlich, Sicherheitsanforderungen sowie die regelmäßige Überwachung ihrer Einhaltung in den Verträgen aufzunehmen.

Bei der Einbindung externer Dienstleister ist es möglich, dass der Dienstleister bereits für die eingebundene Dienstleistung ein Zertifikat vorweisen kann. Hierbei muss immer berücksichtigt werden, ob der Geltungsbereich des ausgestellten Zertifikates die Dienstleistung auch tatsächlich umfasst.

Aktionspunkte zu 8.3 Modellierung eines Informationsverbunds

- Kapitel *Schichtenmodell und Modellierung* aus dem IT-Grundschutz-Kompendium systematisch durcharbeiten
- Für jeden Baustein des IT-Grundschutz-Kompendiums ermitteln, auf welche Zielobjekte er im betrachteten Informationsverbund anzuwenden ist
- Zuordnung von Bausteinen zu Zielobjekten („IT-Grundschutz-Modell") sowie die entsprechenden Ansprechpartner dokumentieren
- Zielobjekte, die nicht geeignet modelliert werden können, für eine Risikoanalyse vormerken
- Festlegung einer Reihenfolge für die Umsetzung der Bausteine
- Sicherheitsanforderungen aus den identifizierten Bausteinen sorgfältig lesen und darauf aufbauend passende Sicherheitsmaßnahmen festlegen

8.4 IT-Grundschutz-Check

Für die nachfolgenden Betrachtungen wird vorausgesetzt, dass für einen ausgewählten Informationsverbund folgende Teile des Sicherheitskonzepts nach IT-Grundschutz erstellt wurden:

Anhand der Strukturanalyse des Informationsverbunds wurde eine Übersicht über die vorhandenen Geschäftsprozesse, die IT und deren Vernetzung, die unterstützten Anwendungen und die Räumlichkeiten erstellt. Darauf aufbauend wurde anschließend die Schutzbedarfsfeststellung durchgeführt, deren Ergebnis eine Übersicht über den Schutzbedarf der Geschäftsprozesse, Anwendungen, IT-Systeme, der genutzten Räume und der Kommunikationsverbindungen ist. Mithilfe dieser Informationen wurde die Modellierung des Informationsverbunds nach IT-Grundschutz durchgeführt. Das Ergebnis war eine Abbildung des betrachteten Informationsverbunds auf Bausteine des IT-Grundschutzes.

Die Modellierung nach IT-Grundschutz wird nun als Prüfplan benutzt, um anhand eines Soll-Ist-Vergleichs herauszufinden, welche Anforderungen ausreichend oder nur unzureichend erfüllt wurden.

Dieses Kapitel beschreibt, wie bei der Durchführung des IT-Grundschutz-Checks vorgegangen werden sollte. Der IT-Grundschutz-Check besteht aus drei unterschiedlichen Schritten. Im ersten Schritt werden die organisatorischen Vorbereitungen getroffen, insbesondere die relevanten Ansprechpartner für den Soll-Ist-Vergleich ausgewählt. Im zweiten Schritt wird der eigentliche Soll-Ist-Vergleich mittels Interviews und stichprobenartiger Kontrolle durchgeführt. Im letzten Schritt werden die erzielten Ergebnisse des Soll-Ist-Vergleichs einschließlich der erhobenen Begründungen dokumentiert.

Nachfolgend werden die Schritte des IT-Grundschutz-Checks detailliert beschrieben.

8.4.1 Organisatorische Vorarbeiten für den IT-Grundschutz-Check

Für die reibungslose Durchführung des Soll-Ist-Vergleichs sind einige Vorarbeiten erforderlich. Zunächst sollten alle hausinternen Papiere, z. B. Organisationsverfügungen, Arbeitshinweise, Sicherheitsanweisungen, Handbücher und „informelle" Vorgehensweisen, die die sicherheitsrelevanten Abläufe regeln, gesichtet werden. Auch die Dokumentation der bereits umgesetzten Sicherheitsmaßnahmen gehört dazu. Diese Dokumente können bei der Ermittlung des Umsetzungsgrades hilfreich sein, insbesondere bei Fragen nach bestehenden organisatorischen Regelungen. Weiterhin ist zu klären, wer gegenwärtig für deren Inhalt zuständig ist, um später die richtigen Ansprechpartner bestimmen zu können.

Als Nächstes sollte festgestellt werden, ob und in welchem Umfang externe Stellen bei der Ermittlung des Umsetzungsstatus beteiligt werden müssen. Dies kann beispielsweise bei externen Rechenzentren, vorgesetzten Behörden, Firmen, die Teile von Geschäftsprozessen oder des IT-Betriebes als Outsourcing-Dienstleistung übernehmen, oder Baubehörden, die für infrastrukturelle Maßnahmen zuständig sind, erforderlich sein.

Ein wichtiger Schritt vor der Durchführung des eigentlichen Soll-Ist-Vergleichs ist die Ermittlung geeigneter Interviewpartner. Hierzu sollte zunächst für jeden einzelnen Baustein, der für die Modellierung des vorliegenden Informationsverbunds herangezogen wurde, ein Hauptansprechpartner festgelegt werden. Bei den Anforderungen in den Bausteinen werden die Rollen genannt, die für die Umsetzung der Anforderungen erforderlich sind. Hieraus können die geeigneten Ansprechpartner für die jeweilige Thematik in der Institution identifiziert werden. Nachfolgend finden sich einige Beispiele für Ansprechpartner der verschiedenen Bereiche:

- Bei den Bausteinen der Schicht ORP, CON und OPS ergibt sich ein geeigneter Ansprechpartner in der Regel direkt aus der im Baustein behandelten Thematik. Beispielsweise sollte für den Baustein ORP.2 *Personal* ein Mitarbeiter der zuständigen Personalabteilung als Ansprechpartner ausgewählt werden. Bei den konzeptionellen Bausteinen, z. B. Baustein CON.1 *Kryptokonzept*, steht im Idealfall der Mitarbeiter zur Verfügung, der für die Fortschreibung des entsprechenden Dokuments zuständig ist. Anderenfalls sollte derjenige Mitarbeiter befragt werden, zu dessen Aufgabengebiet die Fortschreibung von Regelungen in dem betrachteten Bereich gehört.
- Im Bereich der Schicht INF *(Infrastruktur)* sollte die Auswahl geeigneter Ansprechpartner in Abstimmung mit der Abteilung Innerer Dienst/Haustechnik vorgenommen werden. Je nach Größe der betrachteten Institution können beispielsweise unterschiedliche Ansprechpartner für die Infrastrukturbereiche Gebäude und Technikräume zuständig sein. In kleinen Institutionen kann in vielen Fällen der Hausmeister Auskunft geben. Zu beachten ist im Bereich der Infrastruktur, dass hier unter Umständen externe Stellen zu beteiligen sind. Dies betrifft insbesondere größere Institutionen.
- In den systemorientierten Bausteinen der Schichten SYS, NET und IND werden in den zu prüfenden Sicherheitsmaßnahmen verstärkt technische Aspekte behandelt. In der Regel kommt daher der Administrator derjenigen Komponente bzw. Gruppe von Komponenten, der der jeweilige Baustein bei der Modellierung zugeordnet wurde, als Hauptansprechpartner infrage.
- Für die Bausteine der Schicht APP *(Anwendungen)* sollten die Betreuer bzw. die Verantwortlichen der einzelnen Anwendungen als Hauptansprechpartner ausgewählt werden.

Für die anstehenden Interviews mit den Systemverantwortlichen, Administratoren und sonstigen Ansprechpartnern sollte ein Terminplan erstellt werden. Ein besonderes Augenmerk gilt hier der Termin-

koordination mit Personen aus anderen Organisationseinheiten oder anderen Institutionen. Zudem erscheint es sinnvoll, bereits im Vorhinein Ausweichtermine abzustimmen.

Je nach Größe der Projektgruppe sollten für die Durchführung der Interviews Teams mit verteilten Aufgaben gebildet werden. Es hat sich bewährt, in jeder Gruppe zwei Personen für die Durchführung des Interviews einzuplanen. Dabei stellt eine Person die notwendigen Fragen und die andere Person notiert die Ergebnisse und Anmerkungen, die durch den Interviewpartner gegeben werden.

Beispiel: RECPLAST GmbH

A.4 IT-Grundschutz-Check der RECPLAST GmbH				
Baustein:	**Sicherheitsmanagement**			
Anforderung	**Anforderungstitel**	**Verantwortung**	**Status**	**Umsetzung**
ISMS.1.A1	Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene	Institutionsleitung	umgesetzt	Die Geschäftsführung hat die Erstellung der Leitlinie initiiert. Die Leitlinie wurde von der Geschäftsführung unterzeichnet. Die Geschäftsführung hat die gesamte Verantwortung für das Thema Informationssicherheit übernommen und delegiert an den ISB die Umsetzung der geforderten Maßnahmen. Einmal monatlich erhält die Geschäftsführung einen Management-Report, kontrolliert den Umsetzungsstatus der Maßnahmen und initiiert ggf. weitere Maßnahmen und bewilligt das entsprechende Budget.
ISMS.1.A5	Vertragsgestaltung bei Bestellung eines externen Informationssicherheitsbeauftragten	Institutionsleitung	entbehrlich	Der Informationssicherheitsbeauftragte ist ein interner Mitarbeiter der RECPLAST GmbH.
ISMS.1.A7	Festlegung von Sicherheitsmaßnahmen	ISB	teilweise	Alle Mitarbeiter, die Maßnahmen im Sinne der Informationssicherheit umsetzen, sind verpflichtet, diese zu dokumentieren und dem ISB per E-Mail zuzusenden. Eine Auswertung und ausreichende Dokumentation der eingehenden umgesetzten Maßnahmen gibt es nicht. Umsetzungszeitpunkt für ausführliche Dokumentation: 30.04.

A.4 IT-Grundschutz-Check der RECPLAST GmbH				
Baustein:	**Sicherheitsmanagement**			
Anforderung	**Anforderungstitel**	**Verantwortung**	**Status**	**Umsetzung**
ISMS.1.A11	Aufrechterhaltung der Informationssicherheit	ISB	umgesetzt	Alle Dokumente und Prozesse werden einmal jährlich einem internen Audit unterzogen. Der ISB hat dafür die entsprechende fachliche Weisungsbefugnis für die Mitarbeiter, in deren Verantwortungsbereich einzelne Dokumente und Prozesse fallen.

Abbildung 31: Auszug aus dem IT-Grundschutz-Check der RECPLAST GmbH (Baustein ISMS.1)

Aktionspunkte zu 8.4.1 Organisatorische Vorarbeiten des IT-Grundschutz-Checks

- Hausinterne Dokumente mit Verfügungen und Regelungen sichten und Zuständigkeiten für diese Unterlagen klären
- Feststellen, in welchem Umfang externe Stellen beteiligt werden müssen
- Hauptansprechpartner für jeden in der Modellierung angewandten Baustein festlegen
- Terminplan für Interviews abstimmen
- Team für Interviews zusammenstellen

8.4.2 Durchführung des Soll-Ist-Vergleichs

Sind alle erforderlichen Vorarbeiten erledigt, kann die eigentliche Erhebung an den zuvor festgesetzten Terminen beginnen. Hierzu werden die Sicherheitsanforderungen des jeweiligen Bausteins, für den die Interviewpartner zuständig sind, der Reihe nach durchgearbeitet.

Als Antworten bezüglich des Umsetzungsstatus der einzelnen Anforderungen kommen folgende Aussagen in Betracht:

„entbehrlich" Die Erfüllung der Anforderung ist in der vorgeschlagenen Art nicht notwendig, weil die Anforderung im betrachteten Informationsverbund nicht relevant ist (z. B. weil Dienste nicht aktiviert wurden) oder durch Alternativmaßnahmen behandelt wurde. Wird der Umsetzungsstatus einer Anforderung auf „entbehrlich" gesetzt, müssen über die Kreuzreferenztabelle des jeweiligen Bausteins die zugehörigen elementaren Gefährdungen identifiziert werden. Wurden Alternativmaßnahmen ergriffen, muss begründet werden, dass das Risiko, das von allen betreffenden elementaren Gefährdungen ausgeht, angemessen minimiert wurde. Generell ist zu beachten, dass bei Basis-Anforderungen das entstehende Risiko nicht übernommen werden kann.
Anforderungen dürfen nicht auf „entbehrlich" gesetzt werden, wenn das Risiko für eine im Baustein identifizierte elementare Gefährdung über die Kreuzreferenztabelle pauschal akzeptiert oder ausgeschlossen wird.

„ja" Zu der Anforderung wurden geeignete Maßnahmen vollständig, wirksam und angemessen umgesetzt.

„teilweise" Die Anforderung wurde nur teilweise umgesetzt.

„nein" Die Anforderung wurde noch nicht erfüllt, also geeignete Maßnahmen sind größtenteils noch nicht umgesetzt.

Es ist sinnvoll, bei den Interviews nicht nur die Bausteintexte, sondern auch die Umsetzungshinweise oder andere ergänzende Materialien griffbereit zu haben. Den Befragten sollte der Zweck des IT-Grundschutz-Checks kurz vorgestellt werden. Es bietet sich an, mit den Anforderungsüberschriften fortzufahren und die Anforderungen kurz zu erläutern. Dem Gesprächspartner sollte die Möglichkeit gegeben werden, auf die bereits umgesetzten Anforderungen und Maßnahmen einzugehen und danach noch offene Punkte zu besprechen.

Die Befragungstiefe richtet sich zunächst nach dem Niveau von Basis- und Standard-Anforderungen; über diese hinausweisende Aspekte hochschutzbedürftiger Anwendungen sollten erst nach Abschluss des IT-Grundschutz-Checks betrachtet werden. Falls der Bedarf besteht, die in den Interviews gemachten Aussagen zu verifizieren, bietet es sich an, stichprobenartig die entsprechenden Regelun-

gen und Konzepte zu sichten, im Bereich Infrastruktur gemeinsam mit dem Ansprechpartner die zu untersuchenden Objekte vor Ort zu besichtigen sowie Client- bzw. Servereinstellungen an ausgewählten IT-Systemen zu überprüfen.

Zum Abschluss jedes Bausteins sollte den Befragten das Ergebnis (Umsetzungsstatus der Anforderungen: entbehrlich/ja/teilweise/nein) mitgeteilt und diese Entscheidung erläutert werden.

Aktionspunkte zu 8.4.2 Durchführung des Soll-Ist-Vergleichs
• Je nach Fachgebiet vorab Checklisten erstellen
• Zielsetzung des IT-Grundschutz-Checks den Interviewpartnern erläutern
• Umsetzungsstatus der einzelnen Anforderungen erfragen
• Antworten anhand von Stichproben am Objekt verifizieren
• Den Befragten die Ergebnisse mitteilen

8.4.3 Dokumentation der Ergebnisse

Die Ergebnisse des IT-Grundschutz-Checks sollten so dokumentiert werden, dass sie für alle Beteiligten nachvollziehbar sind und als Grundlage für die Umsetzungsplanung der defizitären Anforderungen und Maßnahmen genutzt werden können. Der Dokumentationsaufwand sollte nicht unterschätzt werden. Daher sollten geeignete Hilfsmittel genutzt werden, die bei der Erstellung und Aktualisierung aller im Sicherheitsprozess erforderlichen Dokumente unterstützen.

Dies können zum einen geeignete IT-Grundschutz-Tools sein, also Anwendungen, die die gesamte Vorgehensweise nach IT-Grundschutz unterstützen, beginnend bei der Stammdatenerfassung, über die Schutzbedarfsfeststellung, die Risikoanalyse sowie den Soll-Ist-Vergleich (IT-Grundschutz-Check) bis hin zur Erfüllung der Anforderungen. Hierdurch ergeben sich komfortable Möglichkeiten zur Auswertung und Revision der Ergebnisse, z. B. die Suche nach bestimmten Einträgen, die Generierung von Reports, Kostenauswertungen sowie Statistikfunktionen.

Des Weiteren stehen als Hilfsmittel zum IT-Grundschutz Formulare zur Verfügung. Zu jedem Baustein des IT-Grundschutz-Kompendiums gibt es eine Datei, in der tabellarisch für jede Anforderung des Bausteins die Ergebnisse des Soll-Ist-Vergleichs erfasst werden können.

Zur Dokumentation des IT-Grundschutz-Checks sollten erfasst werden:

- Die Nummer und die Bezeichnung des Objektes oder Gruppe von Objekten, der der Baustein bei der Modellierung zugeordnet wurde,
- der Standort der zugeordneten Objekte bzw. Gruppe von Objekten,
- das Erfassungsdatum und der Name des Erfassers und
- die befragten Ansprechpartner.

Die eigentlichen Ergebnisse des Soll-Ist-Vergleichs sollten tabellarisch erfasst werden. Dabei sollten zu jeder Anforderung des jeweiligen Bausteins folgende Informationen festgehalten werden:

- Umsetzungsgrad (entbehrlich/ja/teilweise/nein)
  Der im Interview ermittelte Umsetzungsstatus der jeweiligen Anforderung ist zu erfassen. Im Hinblick auf eine mögliche Zertifizierung sollte zudem festgehalten werden, durch welche Maßnahmen die Anforderungen konkret erfüllt werden.

- Umsetzung bis . . .
  Ein solches Feld ist sinnvoll, auch wenn es während eines IT-Grundschutz-Checks im Allgemeinen nicht ausgefüllt wird. Es dient als Platzhalter, um in der Realisierungsplanung an dieser Stelle zu dokumentieren, bis zu welchem Termin die Anforderung vollständig umgesetzt sein soll.
- Verantwortliche
  Falls es bei der Durchführung des Soll-Ist-Vergleichs eindeutig ist, welche Mitarbeiter für die vollständige Umsetzung einer defizitären Anforderung oder Maßnahme verantwortlich sind, sollte das namentlich in diesem Feld dokumentiert werden. Falls die Verantwortung nicht eindeutig erkennbar ist, sollte das Feld frei gelassen werden. Im Zuge der späteren Realisierungsplanung ist dann ein Verantwortlicher zu bestimmen, dessen Name hier eingetragen werden kann.
- Bemerkungen/Begründungen
  Ein solches Feld ist wichtig, um getroffene Entscheidungen später nachvollziehen zu können, beispielsweise für die Zertifizierung. Bei Anforderungen, deren Umsetzung entbehrlich erscheint, ist hier die Begründung zu nennen. Bei Anforderungen, die noch nicht oder nur teilweise umgesetzt sind, sollte in diesem Feld dokumentiert werden, welche Maßnahmen noch umgesetzt werden müssen. In dieses Feld sollten auch alle anderen Bemerkungen eingetragen werden, die bei der Beseitigung von Defiziten hilfreich oder im Zusammenhang mit der Anforderung zu berücksichtigen sind.
- Defizite/Kostenschätzung
  Für Anforderungen, die nicht oder nur teilweise erfüllt wurden, ist das damit verbundene Risiko in geeigneter Form zu ermitteln und zu dokumentieren. Dies ist beispielsweise für Audits und Zertifizierungen wichtig. Bei solchen Maßnahmen sollte außerdem geschätzt werden, welchen finanziellen und personellen Aufwand die Beseitigung der Defizite erfordert.

Aktionspunkte zu 8.4.3 Dokumentation der Ergebnisse
• Stamminformationen über jedes Zielobjekt erfassen
• Informationen zum IT-Grundschutz-Check und zum Umsetzungsstatus dokumentieren
• Felder beziehungsweise Platzhalter für die Realisierungsplanung vorsehen

8.5 Risikoanalyse

Eine Risikoanalyse im Kontext der Informationssicherheit hat die Aufgabe, relevante Gefährdungen für den Informationsverbund zu identifizieren und die daraus möglicherweise resultierenden Risiken abzuschätzen. Das Ziel ist es, die Risiken durch angemessene Gegenmaßnahmen auf ein akzeptables Maß zu reduzieren, die Restrisiken transparent zu machen und dadurch das Gesamtrisiko systematisch zu steuern.

Zweistufiger Ansatz der IT-Grundschutz-Vorgehensweise

In der Vorgehensweise nach IT-Grundschutz wird bei der Erstellung der IT-Grundschutz-Bausteine implizit eine Risikobewertung für Bereiche mit normalem Schutzbedarf durchgeführt. Hierbei werden nur solche Gefährdungen betrachtet, die nach sorgfältiger Analyse eine so hohe Eintrittswahrscheinlichkeit oder so einschneidende Auswirkungen haben, dass Sicherheitsmaßnahmen ergriffen werden müssen. Typische Gefährdungen, gegen die sich jeder schützen muss, sind z. B. Schäden durch Feuer, Einbrecher, Schadsoftware oder Hardware-Defekte. Dieser Ansatz hat den Vorteil, dass Anwender des IT-Grundschutzes für einen Großteil des InformationsverbundesInformationsverbunds keine individu-

elle Bedrohungs- und Schwachstellenanalyse durchführen müssen, weil diese Bewertung vorab bereits vorgenommen wurde.

In bestimmten Fällen muss jedoch eine explizite Risikoanalyse durchgeführt werden, beispielsweise wenn der betrachtete Informationsverbund Zielobjekte enthält, die

- einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben oder
- mit den existierenden Bausteinen des IT-Grundschutzes nicht hinreichend abgebildet (modelliert) werden können oder
- in Einsatzszenarien (Umgebung, Anwendung) betrieben werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

In diesen Fällen stellen sich folgende Fragen:

- Welchen Gefährdungen für die Informationsverarbeitung ist durch die Umsetzung der relevanten IT-Grundschutz-Bausteine noch nicht ausreichend oder sogar noch gar nicht Rechnung getragen worden?
- Müssen eventuell ergänzende Sicherheitsmaßnahmen, die über das IT-Grundschutz-Modell hinausgehen, eingeplant und umgesetzt werden?

Zur Beantwortung dieser Fragen empfiehlt das BSI die Anwendung einer Risikoanalyse auf der Basis von IT-Grundschutz, wie sie im BSI-Standard 200-3 beschrieben ist.

In dem Standard wird dargestellt, wie für bestimmte Zielobjekte festgestellt werden kann, ob und in welcher Hinsicht über den IT-Grundschutz hinaus Handlungsbedarf besteht, um Risiken für die Informationsverarbeitung zu reduzieren. Hierzu werden Risiken, die von elementaren Gefährdungen ausgehen, eingeschätzt und anhand einer Matrix bewertet. Die Einschätzung erfolgt über die zu erwartende Häufigkeit des Eintretens und die Höhe des Schadens, der bei Eintritt des Schadensereignisses entsteht. Aus diesen beiden Anteilen ergibt sich das Risiko. Die Methodik lässt sich wie folgt in den IT-Grundschutz-Prozess integrieren:

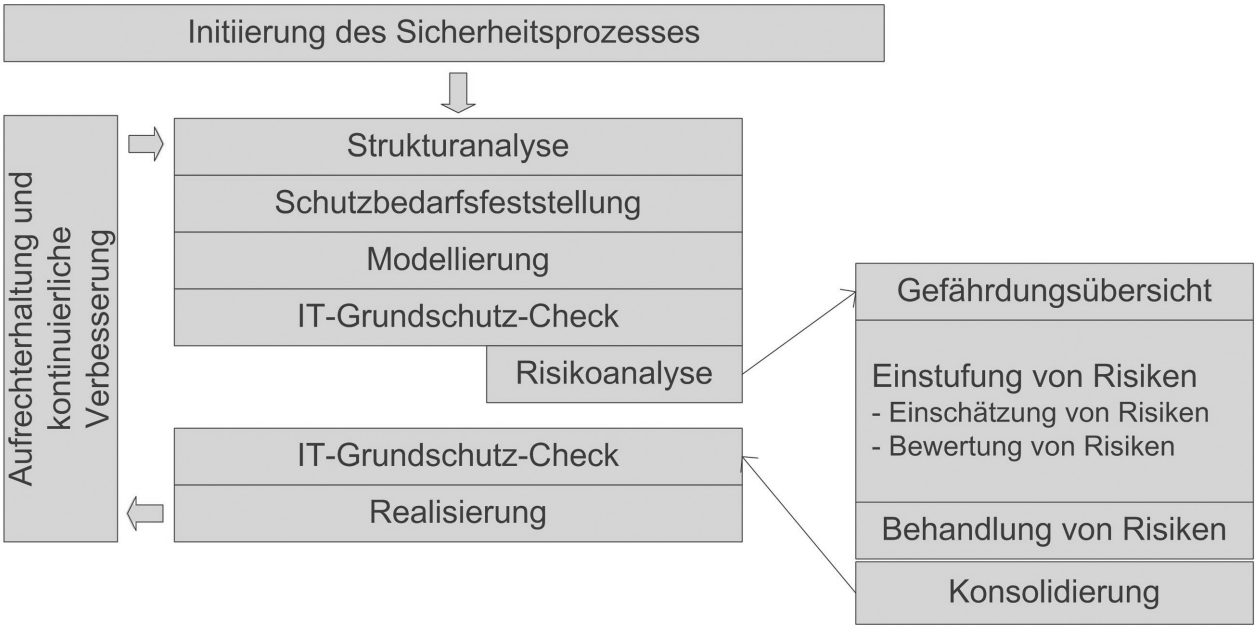


Abbildung 32: Integration der Risikoanalyse in den IT-Grundschutz-Prozess

Der Standard bietet sich an, wenn Institutionen bereits erfolgreich mit der IT-Grundschutz-Methodik arbeiten und möglichst direkt eine Risikoanalyse an die IT-Grundschutz-Analyse anschließen möchten. Hierzu empfiehlt der BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz* folgende zusätzliche Arbeitsschritte, die hier kurz im Überblick aufgeführt sind:

- Etablierung eines Risikomanagementprozesses
  Die Risikoanalyse ist ein wichtiger Bestandteil des Managementsystems für Informationssicherheit (ISMS). Daher sollten die Grundvoraussetzungen dafür von der Institutionsleitung vorgegeben werden. Die grundsätzliche Vorgehensweise der Institution zur Durchführung von Risikoanalysen sollte in einer Richtlinie (siehe BSI-Standard 200-3, Kapitel 2) dokumentiert und durch die Leitungsebene verabschiedet werden.
- Erstellung der Gefährdungsübersicht
  In diesem Arbeitsschritt wird für jedes zu analysierende Zielobjekt eine Liste der jeweils relevanten Gefährdungen zusammengestellt. Bei der Ermittlung von Gefährdungen geht das BSI zweistufig vor. Zunächst werden die relevanten elementaren Gefährdungen identifiziert und darauf aufbauend werden weitere mögliche Gefährdungen (zusätzliche Gefährdungen) ermittelt, die über die elementaren Gefährdungen hinausgehen und sich aus dem spezifischen Einsatzszenario ergeben. Dies erfolgt im Rahmen eines gemeinsamen Brainstormings.
- Risikoeinstufung
  Die Risikoanalyse ist zweistufig angelegt. Für jedes Zielobjekt und jede Gefährdung wird eine Bewertung unter der Annahme vorgenommen, dass bereits Sicherheitsmaßnahmen umgesetzt oder geplant worden sind. In der Regel wird es sich hierbei um Sicherheitsmaßnahmen handeln, die aus den Basis- und Standard-Anforderungen des IT-Grundschutz-Kompendiums abgeleitet worden sind. An die erste Bewertung schließt sich eine zweite an, bei der mögliche Sicherheitsmaßnahmen zur Risikobehandlung betrachtet werden. Durch einen Vorher-Nachher-Vergleich lässt sich die Wirksamkeit der Sicherheitsmaßnahmen prüfen, die zur Risikobehandlung eingesetzt worden sind.
- Behandlung von Risiken
  Abhängig vom Risikoappetit einer Institution sind jeweils unterschiedliche Risikoakzeptanzkriterien möglich. Risikoappetit bezeichnet die durch kulturelle, interne, externe oder wirtschaftliche Einflüsse entstandene Neigung einer Institution, wie sie Risiken bewertet und mit ihnen umgeht. Es gibt folgende Optionen zur Behandlung von Risiken:
- Risiken können vermieden werden (z. B. durch Umstrukturierung von Geschäftsprozessen oder des Informationsverbunds).
- Risiken können durch entsprechende Sicherheitsmaßnahmen reduziert werden.
- Risiken können transferiert werden (z. B. durch Outsourcing oder Versicherungen).

Daran anschließend muss eine Institution Risikoakzeptanzkriterien festlegen und die Behandlung des Risikos darauf abbilden. Bei der Entscheidung, wie mit den identifizierten Risiken umzugehen ist, muss auf jeden Fall die Leitungsebene beteiligt werden, da sich daraus unter Umständen erhebliche Schäden ergeben oder zusätzliche Kosten entstehen können.

Die Schritte Gefährdungsbewertung und Risikobehandlung werden so lange durchlaufen, bis die Risikoakzeptanzkriterien der Institution erfüllt sind und das verbleibende Risiko („Restrisiko“) im Einklang mit den Zielen und Vorgaben der Institution steht. Das verbleibende Risiko muss anschließend

der Leitungsebene zur Zustimmung vorgelegt werden („**Risiko-Akzeptanz**"). Damit wird nachvollziehbar dokumentiert, dass die Institution sich des Restrisikos bewusst ist.

- Konsolidierung des Sicherheitskonzepts
  Bevor der originäre IT-Grundschutz-Prozess fortgesetzt werden kann, muss das erweiterte Sicherheitskonzept konsolidiert werden. Dabei werden die Eignung, das Zusammenwirken, die Benutzerfreundlichkeit und die Angemessenheit der Sicherheitsmaßnahmen insgesamt überprüft.
- Außerdem wird im BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz* erläutert, wie die Methodik anzuwenden ist, wenn der Informationsverbund Zielobjekte umfasst, für die im IT-Grundschutz-Kompendium bislang kein geeigneter Baustein enthalten ist.

Eine ausführliche Darstellung der Methodik findet sich im BSI-Standard 200-3.

Wichtig:

Die Risikoanalyse auf der Basis von IT-Grundschutz ist eine Vorgehensweise, um bei Bedarf Sicherheitsvorkehrungen zu ermitteln, die über die im IT-Grundschutz-Kompendium genannten Sicherheitsanforderungen hinausgehen. Obwohl diese Methodik gegenüber vielen anderen ähnlichen Verfahren vereinfacht wurde, ist sie oft mit erheblichem Aufwand verbunden. Um schnellstmöglich die wichtigsten Sicherheitsprobleme zu beseitigen, ist es manchmal zweckmäßig, zuerst die IT-Grundschutz-Anforderungen vollständig zu erfüllen und erst danach eine Risikoanalyse durchzuführen (abweichend von obigem Schema). Dadurch müssen zwar insgesamt einige Schritte öfter durchlaufen werden, die IT-Grundschutz-Anforderungen werden jedoch früher erfüllt.

Diese alternative Reihenfolge bietet sich besonders dann an, wenn

- der betrachtete Informationsverbund bereits realisiert und in Betrieb ist und
- die vorliegenden Zielobjekte mit den existierenden Bausteinen des IT-Grundschutz-Kompendiums hinreichend modelliert werden können.

Für geplante Informationsverbünde oder für solche mit untypischen Techniken bzw. Einsatzszenarien wird dagegen die oben abgebildete originäre Reihenfolge empfohlen. Die folgende Tabelle fasst die jeweiligen Vor- und Nachteile der beiden alternativen Reihenfolgen zusammen:

Risikoanalyse direkt nach dem IT-Grundschutz-Check	**Risikoanalyse erst nach vollständiger Umsetzung der Sicherheitsmaßnahmen**
Mögliche Vorteile: • Es wird Mehraufwand vermieden, da keine Maßnahmen umgesetzt werden, die im Rahmen der Risikoanalyse eventuell durch stärkere Maßnahmen ersetzt werden. • Eventuell erforderliche Hochsicherheitsmaßnahmen werden früher identifiziert und umgesetzt.	Mögliche Vorteile: • Sicherheitsmaßnahmen werden früher umgesetzt, da die Risikoanalyse häufig aufwendig ist. • Elementare Sicherheitslücken werden vorrangig behandelt, bevor fortgeschrittene Gefährdungen analysiert werden.
Mögliche Nachteile: • Sicherheitsmaßnahmen werden später umgesetzt, da die Risikoanalyse häufig aufwendig ist. • Eventuell werden elementare Sicherheitslücken vernachlässigt, während fortgeschrittene Gefährdungen analysiert werden.	Mögliche Nachteile: • Es kann Mehraufwand entstehen, da eventuell einige Sicherheitsmaßnahmen umgesetzt werden, die später im Rahmen der Risikoanalyse durch stärkere Maßnahmen ersetzt werden. • Eventuell erforderliche Hochsicherheitsmaßnahmen werden erst später identifiziert und umgesetzt.

Tabelle 7: Vor- und Nachteile der alternativen Reihenfolgen bei der Risikoanalyse

Wichtig ist außerdem, dass eine Risikoanalyse auf der *Basis von IT-Grundschutz* häufig leichter durchzuführen ist, wenn sie nacheinander auf kleine Teilaspekte des Informationsverbunds angewandt wird. Als ersten Schritt kann die Analyse beispielsweise auf die baulich-physische Infrastruktur beschränkt werden, d. h. auf den Schutz vor Brand, Wasser und unbefugtem Zutritt sowie auf die ordnungsgemäße Strom- und Klimaversorgung.

In vielen Behörden und Unternehmen existieren bereits Verfahren zur Risikoanalyse beziehungsweise zur Risikobehandlung. Um eine einheitliche Methodik zu erreichen, kann es in solchen Fällen zweckmäßig sein, die vorhandenen Verfahren auf die Informationssicherheit auszudehnen und gegebenenfalls nur Teilaspekte des BSI-Standards 200-3 anzuwenden. International haben sich eine Reihe von unterschiedlichen Ansätzen zur Durchführung von Risikoanalysen im Bereich der Informationssicherheit etabliert. Diese Verfahren unterscheiden sich beispielsweise in Bezug auf den Detaillierungsgrad, die Formalisierung und die thematischen Schwerpunkte. Abhängig von den Rahmenbedingungen einer Institution und der Art des Informationsverbunds kann es zweckmäßig sein, alternativ zum BSI-Standard 200-3 ein anderes etabliertes Verfahren oder eine angepasste Methodik für die Analyse von Informationsrisiken zu verwenden.

Aktionspunkte zu 8.5 Risikoanalyse

- Grundsätzliche Vorgehensweise der Institution zur Durchführung von Risikoanalysen in einer Richtlinie dokumentieren und der Leitungsebene zur Verabschiedung vorlegen
- Ermitteln, für welche Zielobjekte oder Gruppen von Zielobjekten eine Risikoanalyse durchgeführt werden soll
- BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz* systematisch durcharbeiten
- Ergebnisse der Risikoanalysen in das Sicherheitskonzept integrieren

9 Umsetzung der Sicherheitskonzeption

In diesem Kapitel werden verschiedene Aspekte vorgestellt, die bei der Planung und Realisierung von Sicherheitsmaßnahmen beachtet werden müssen. Dabei wird beschrieben, wie die Umsetzung von Sicherheitsmaßnahmen geplant, durchgeführt, begleitet und überwacht werden kann. Zu vielen Bausteinen des IT-Grundschutzes existieren Umsetzungshinweise mit beispielhaften Empfehlungen für Sicherheitsmaßnahmen, mittels derer die Anforderungen der Bausteine umgesetzt werden können. Diese basieren auf Best Practices und langjähriger Erfahrung von Experten aus dem Bereich der Informationssicherheit. Die Maßnahmen aus den Umsetzungshinweisen sind jedoch nicht als verbindlich zu betrachten, sondern können und sollten durch eigene Maßnahmen ergänzt oder ersetzt werden. Solche eigenen Maßnahmen sollten wiederum dem IT-Grundschutz-Team des BSI mitgeteilt werden, vor allem, wenn sie neue Aspekte enthalten, damit die Umsetzungshinweise entsprechend ergänzt werden können.

Bei der Erstellung der Sicherheitskonzeption sind für den untersuchten Informationsverbund die Strukturanalyse, die Schutzbedarfsfeststellung und die Modellierung erfolgt. Ebenso liegen zu diesem Zeitpunkt die Ergebnisse des IT-Grundschutz-Checks, also des daran anknüpfenden Soll-Ist-Vergleichs, vor. Sollte für ausgewählte Bereiche eine Risikoanalyse durchgeführt worden sein, so sollten die dabei erarbeiteten Maßnahmenvorschläge ebenfalls vorliegen und nachfolgend berücksichtigt werden.

Für die Realisierung der Maßnahmen stehen in der Regel nur beschränkte Ressourcen an Geld und Personal zur Verfügung. Ziel der nachfolgend beschriebenen Schritte ist daher, eine möglichst effiziente Umsetzung der vorgesehenen Sicherheitsmaßnahmen zu erreichen. Ein Beispiel zur Erläuterung der Vorgehensweise findet sich am Ende dieses Kapitels.

9.1 Sichtung der Untersuchungsergebnisse

In einer Gesamtsicht sollte ausgewertet werden, welche Anforderungen aus den IT-Grundschutz-Bausteinen nicht oder nur teilweise umgesetzt wurden. Dazu bietet es sich an, diese aus den Ergebnissen des IT-Grundschutz-Checks zu extrahieren und in einer Tabelle zusammenzufassen.

Durch Risikoanalysen könnten eventuell weitere zu erfüllende Anforderungen sowie zu realisierende Maßnahmen identifiziert worden sein. Diese sollten ebenfalls tabellarisch erfasst werden. Diese zusätzlichen Anforderungen und Maßnahmen sollten den vorher betrachteten Zielobjekten der Modellierung und den entsprechenden IT-Grundschutz-Bausteinen thematisch zugeordnet werden.

Die zu erfüllenden Anforderungen aus den IT-Grundschutz-Bausteinen müssen passend zu den organisatorischen und technischen Gegebenheiten der Institution zu Sicherheitsmaßnahmen konkretisiert werden. Die Umsetzungshinweise des IT-Grundschutzes geben dazu für viele Bausteine und Anforderungen praxisnahe Empfehlungen. Außerdem sollten alle Anforderungen und alle daraus abgeleiteten Sicherheitsmaßnahmen noch einmal daraufhin überprüft werden, ob sie auch geeignet sind: Sie müssen vor den möglichen Gefährdungen wirksam schützen, aber auch in der Praxis tatsächlich umsetzbar sein, dürfen also z. B. nicht die Organisationsabläufe behindern oder andere Sicherheitsmaßnahmen aushebeln. Des Weiteren müssen sie wirtschaftlich sein, siehe unten. In solchen Fällen kann es notwendig werden, bestimmte IT-Grundschutz-Anforderungen so anzupassen, dass dieselben Sicherheitsziele erreicht werden. Basis-Anforderungen sind so elementar, dass diese im Normalfall nicht ersetzt werden können.

Um auch später noch nachvollziehen zu können, wie die konkrete Maßnahmenliste erstellt und verfeinert wurde, sollte dies geeignet dokumentiert werden.

Weiterführende Hinweise zur Konsolidierung der Sicherheitsmaßnahmen finden sich außerdem im BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz*.

Beispiele:

- *Bei einer Risikoanalyse wurde festgestellt, dass zusätzlich zu den IT-Grundschutz-Anforderungen auch eine chipkartengestützte Authentisierung und lokale Verschlüsselung der Festplatten an Clients der Personaldatenverarbeitung notwendig sind. Diese zusätzlichen Anforderungen sollten im Sicherheitskonzept ergänzt werden.*
- *Im Sicherheitskonzept für ein Krankenhaus wurde festgelegt, dass für alle IT-Systeme eine Authentifizierung erforderlich ist und ein Time-out nach zehn Minuten erfolgt. Beim IT-Grundschutz-Check stellt sich heraus, dass die Vorgabe zu pauschal und in dieser Form nicht praxistauglich ist. Daher wird diese jetzt im Sicherheitskonzept differenziert:*
  - *IT-Systeme im Verwaltungsbereich erfordern eine erneute Authentisierung nach 15 Minuten Inaktivität.*
  - *Bei IT-Systemen in Bereichen, wo Patienten- und Besucherverkehr herrscht, erfolgt ein Time-out nach fünf Minuten.*
  - *Bei IT-Systemen in Behandlungsräumen wird die automatische Abmeldung deaktiviert. Die Mitarbeiter erhalten die Anweisung, sich nach dem Verlassen der Räume abzumelden.*

9.2 Kosten- und Aufwandsschätzung

Da das Budget zur Umsetzung von Sicherheitsmaßnahmen praktisch immer begrenzt ist, sollte für jede zu realisierende Maßnahme festgehalten werden, welche Investitionskosten und welcher Personalaufwand dafür benötigt werden. Hierbei sollte zwischen einmaligen und wiederkehrenden Investitionskosten bzw. Personalaufwand unterschieden werden. An dieser Stelle zeigt sich häufig, dass Einsparungen bei technischen oder infrastrukturellen Sicherheitsmaßnahmen dazu führen, dass sie einen hohen fortlaufenden Personaleinsatz verursachen. Umgekehrt führen Einsparungen beim Personal schnell zu kontinuierlich immer größeren werden Sicherheitsdefiziten.

In diesem Zusammenhang ist zu ermitteln, ob alle im ersten Zug aus den Anforderungen abgeleiteten Maßnahmen wirtschaftlich umsetzbar sind. Falls es Maßnahmen gibt, die nicht wirtschaftlich sind, sollten Überlegungen angestellt werden, durch welche Ersatzmaßnahmen die Anforderungen dennoch erfüllt werden könnten. Auch bei Informationssicherheit führen häufig viele Wege zum Ziel. Oftmals gibt es verschiedene Optionen, Anforderungen mit geeigneten Maßnahmen zu erfüllen. Falls keine angemessene Maßnahme gefunden werden kann, muss das entstehende Restrisiko sowie die Entscheidung dokumentiert werden. Basis-Anforderungen müssen im Normalfall immer erfüllt werden, die Akzeptanz eines Restrisikos ist aufgrund ihrer elementaren Natur nicht vorgesehen.

Stehen die geschätzten Ressourcen für Kosten- und Personaleinsatz zur Verfügung, muss üblicherweise noch eine Entscheidung herbeigeführt werden, wie viele Ressourcen für die Umsetzung der Sicherheitsmaßnahmen tatsächlich eingesetzt werden sollen. Hierfür bietet es sich an, der Leitungsebene die Ergebnisse der Sicherheitsuntersuchung darzustellen. Geordnet nach Schutzbedarf soll-

ten die festgestellten Schwachstellen (nicht oder unzureichend erfüllte Sicherheitsanforderungen) zur Sensibilisierung vorgestellt werden. Auch auf die spezifischen Gefährdungen, die in den jeweiligen Bausteinen genannt werden, kann hierbei zurückgegriffen werden. Darüber hinaus bietet es sich an, die für die Realisierung der noch notwendigen Maßnahmen anfallenden Kosten und den zu erwartenden Aufwand aufzubereiten. Im Anschluss sollte eine Entscheidung über das Budget erfolgen.

Kann kein ausreichendes Budget für die Realisierung aller fehlenden Maßnahmen bereitgestellt werden, so sollte aufgezeigt werden, welches Restrisiko dadurch entsteht, dass einige Anforderungen gar nicht oder nur verzögert erfüllt werden. Zu diesem Zweck können die sogenannten *Kreuzreferenztabellen* aus den Hilfsmitteln zum IT-Grundschutz hinzugezogen werden. Die *Kreuzreferenztabellen* geben für jeden Baustein eine Übersicht darüber, welche Anforderungen gegen welche elementaren Gefährdungen wirken. Analog lässt sich anhand dieser Tabellen ebenfalls ermitteln, gegen welche elementaren Gefährdungen kein ausreichender Schutz besteht, wenn Anforderungen aus den Bausteinen nicht erfüllt werden. Das entstehende Restrisiko sollte für zufällig eintretende oder absichtlich herbeigeführte Gefährdungen transparent beschrieben und der Leitungsebene zur Entscheidung vorgelegt werden. Die weiteren Schritte können erst nach der Entscheidung der Leitungsebene, dass das Restrisiko tragbar ist, erfolgen, da die Leitungsebene letztlich auch die Verantwortung für die Konsequenzen tragen muss.

9.3 Festlegung der Umsetzungsreihenfolge der Maßnahmen

Kapitel 8.3.3 beschreibt eine Reihenfolge, in der die Bausteine umgesetzt werden sollten, von grundlegenden und übergreifenden Bausteinen bis hin zu solchen, die speziellere Themen abdecken und daher in der zeitlichen Reihenfolge eher nachrangig betrachtet werden können. Diese Reihenfolge der Baustein-Umsetzung ist vor allem bei der Basis-Absicherung wichtig. Sie kann aber auch allgemein bei der Festlegung der Umsetzungsreihenfolge für die einzelnen Maßnahmen eines Sicherheitskonzepts herangezogen werden.

Grundsätzlich sind als Erstes die aus den Basis-Anforderungen abgeleiteten Maßnahmen umzusetzen, dann die der Standard-Anforderungen. Die zusätzlichen Maßnahmen für den erhöhten Schutzbedarf sollten erst anschließend angepasst und realisiert werden.

Wenn das vorhandene Budget oder die personellen Ressourcen nicht ausreichen, um sämtliche noch notwendigen Maßnahmen sofort umsetzen zu können, muss hier eine Priorisierung festgelegt werden.

Die weitere Umsetzungsreihenfolge orientiert sich daran, was für die jeweilige Institution am sinnvollsten ist. Tipps dazu sind:

- Die Umsetzungsreihenfolge lässt sich daran festmachen, wann im Lebenszyklus eines Zielobjektes die jeweiligen Maßnahmen umzusetzen sind. Bei neuen Zielobjekten sind beispielsweise Maßnahmen aus den Bereichen Planung und Konzeption vor solchen umzusetzen, bei denen es um den sicheren Betrieb geht, während bei schon länger im Informationsverbund vorhandenen Zielobjekten zunächst die Absicherung des Betriebs im Vordergrund stehen sollte.
- Bei einigen Maßnahmen ergibt sich durch Abhängigkeiten und logische Zusammenhänge eine zwingende zeitliche Reihenfolge. So kann eine restriktive Rechtevergabe (Basis-Anforderung) auf einem neuen Server nur erfolgen, wenn dieser zunächst sicher installiert wurde (Standard-Anforderung). Diese Reihenfolge kann mit der Klassifikation in Basis- und Standard-Anforderungen auf

den ersten Blick kollidieren. Dennoch haben Basis-Anforderungen inhaltlich stets Priorität, sofern sie bereits erfüllbar sind, im Beispiel etwa bei einem bestehenden Server.

- Manche Maßnahmen erzielen eine große Breitenwirkung, manche jedoch nur eine eingeschränkte lokale Wirkung. Oft ist es sinnvoll, zuerst auf die Breitenwirkung zu achten. Auch daher sollten bevorzugt die Basis-Anforderungen umgesetzt werden, da mit diesen die schnellste Absicherung in der Breite erreicht werden kann. Es lohnt sich aber auch durchaus, die Maßnahmen aus den verschiedenen Bereichen danach zu gewichten, wie schnell sie sich umsetzen lassen und welchen Sicherheitsgewinn sie liefern. Sogenannte „Quick Wins" lassen sich häufig im organisatorischen Bereich finden oder durch zentrale Konfigurationseinstellungen erreichen.
- Es gibt Bausteine, die auf das angestrebte Sicherheitsniveau einen größeren Einfluss haben als andere. Maßnahmen eines solchen Bausteins sollten bevorzugt behandelt werden, insbesondere wenn hierdurch Schwachstellen in hochschutzbedürftigen Bereichen beseitigt werden. So sollten immer zunächst die Server abgesichert werden (unter anderem durch Umsetzung des Bausteins SYS.1.1 *Allgemeiner Server*) und dann erst die angeschlossenen Clients.
- Bausteine mit auffallend vielen nicht umgesetzten Anforderungen repräsentieren Bereiche mit vielen Schwachstellen. Sie sollten ebenfalls bevorzugt behandelt werden.

Die Entscheidung, welche Sicherheitsmaßnahmen ergriffen oder zunächst verschoben werden und wo Restrisiken akzeptiert werden können, sollte auch aus juristischen Gründen sorgfältig dokumentiert werden. In Zweifelsfällen sollten hierfür weitere Meinungen eingeholt und diese ebenfalls dokumentiert werden, um in späteren Streitfällen die Einhaltung der erforderlichen Sorgfaltspflicht belegen zu können.

Hinweis

Bereits einleitend wurde darauf hingewiesen, dass die Erfüllung von Anforderungen an fehlenden Ressourcen scheitern kann. Die oben angeführten Aspekte ermöglichen eine erste Priorisierung. Bei dieser Vorgehensweise werden jedoch die verbleibenden Restrisiken nicht hinreichend betrachtet. Wenn Anforderungen aus IT-Grundschutz-Bausteinen nicht erfüllt sind, ist es empfehlenswert, im Rahmen einer vereinfachten Risikoanalyse die entstandenen Defizite zu betrachten. In diesem Fall kann die in der Risikoanalyse durchzuführende Ermittlung von Gefährdungen entfallen. Dies ist bereits bei der Erstellung der Grundschutz-Bausteine geschehen. Es verbleibt somit die Bewertung des Risikos aufgrund der fehlenden Umsetzung von Anforderungen.

9.4 Festlegung der Aufgaben und der Verantwortung

Nachdem die Reihenfolge für die Umsetzung der Maßnahmen bestimmt wurde, muss anschließend festgelegt werden, wer bis wann welche Maßnahmen realisieren muss. Ohne eine solche verbindliche Festlegung verzögert sich die Realisierung erfahrungsgemäß erheblich bzw. unterbleibt ganz. Dabei ist darauf zu achten, dass der als verantwortlich Benannte ausreichende Fähigkeiten und Kompetenzen zur Umsetzung der Maßnahmen besitzt und dass ihm die erforderlichen Ressourcen zur Verfügung gestellt werden.

Ebenso ist festzulegen, wer für die Überwachung der Realisierung verantwortlich ist bzw. an wen der Abschluss der Realisierung der einzelnen Maßnahmen zu melden ist. Typischerweise wird die Meldung an den ISB erfolgen. Der ISB muss kontinuierlich über den Fortschritt der Realisierung und über die

Ergebnisse der Umsetzung informiert werden. Der ISB wiederum muss regelmäßig die Leitungsebene über den Fortschritt und die damit verbundene Absenkung vorhandener Risiken informieren.

Der Realisierungsplan sollte mindestens folgende Informationen umfassen:

- Bezeichnung des Zielobjektes als Einsatzumfeld,
- Nummer bzw. Titel des betrachteten Bausteins,
- Titel bzw. Beschreibung der zu erfüllenden Anforderung,
- Beschreibung der umzusetzenden Maßnahme bzw. Verweis auf die Beschreibung im Sicherheitskonzept,
- Terminplanung für die Umsetzung, Budgetplanung, beispielsweise für Beschaffung und Betriebskosten von Komponenten,
- Verantwortliche für die Umsetzung der Maßnahmen.

9.5 Realisierungsbegleitende Maßnahmen

Überaus wichtig ist es, notwendige realisierungsbegleitende Maßnahmen rechtzeitig zu identifizieren bzw. zu konzipieren und für die Realisierung entsprechend einzuplanen. Zu diesen Maßnahmen gehören insbesondere Sensibilisierungsmaßnahmen, die darauf abzielen, die Belange der Informationssicherheit zu verdeutlichen und die von neuen Sicherheitsmaßnahmen betroffenen Mitarbeiter über die Notwendigkeit und die Konsequenzen der Maßnahmen zu unterrichten.

Darüber hinaus müssen die betroffenen Mitarbeiter geschult werden, die neuen Sicherheitsmaßnahmen korrekt um- und einzusetzen. Wird diese Schulung unterlassen, können die Maßnahmen oft nicht umgesetzt werden und verlieren ihre Wirkung, wenn sich die Mitarbeiter unzureichend informiert fühlen, was oft zu einer ablehnenden Haltung gegenüber der Informationssicherheit führt.

Beispiel: RECPLAST GmbH

Die obigen Schritte werden nachfolgend anhand des fiktiven Beispiels RECPLAST GmbH auszugsweise beschrieben. In der nachfolgenden Tabelle werden einige zu realisierende Maßnahmen einschließlich der Budgetplanungen dargestellt.

A.6 Realisierungsplan der RECPLAST GmbH						
Zielobjekt	**Baustein**	**Anforderungstext**	**umzusetzende Maßnahmen**	**Terminplanung**	**Budget**	**Verantwortlich für die Umsetzung**
S008 – Print--Server	SYS.1.1 Allgemeiner Server	SYS.1.1.A3 Restriktive Rechtvergabe	In der Rechtevergabe müssen die letzten Gruppenberechtigungen aufgelöst werden.	Q3 des Jahres	- €	Herr Schmidt (IT-Betrieb)
S008 – Print--Server	SYS.1.1 Allgemeiner Server	SYS.1.1.A4 Rollentrennung	Es sind noch nicht für jeden Administrator separate Benutzer-Kennungen eingerichtet.	31.07. des Jahres	- €	Herr Schmidt (IT-Betrieb)
S008 – Print--Server	SYS.1.1 Allgemeiner Server	SYS.1.1.A8 Regelmäßige Datensicherung	Die Datensicherungen werden derzeit auf Bändern innerhalb des Serverraumes aufbewahrt. Geplant ist hierzu ein externes Backup-System. Ein Angebot für die Initialisierung liegt bereits vor (15.000 €). Die Betriebskosten müssen noch verhandelt werden.	Q1 Folgejahr	Anschaffung: 15.000 € Betriebskosten: noch offen	Frau Meyer (Einkauf)

Abbildung 33: Realisierungsplan der RECPLAST GmbH (Auszug)

Anhand dieser Informationen kann die Umsetzung der Maßnahmen überwacht und gesteuert werden.

Aktionspunkte zu 9 Umsetzung der Sicherheitskonzeption

- Fehlende oder nur teilweise umgesetzte IT-Grundschutz-Anforderungen sowie ergänzende Sicherheitsmaßnahmen in einer Tabelle zusammenfassen
- Sicherheitsmaßnahmen konsolidieren, d. h. überflüssige Maßnahmen streichen, allgemeine Maßnahmen an die Gegebenheiten anpassen und alle Maßnahmen auf Eignung prüfen
- Einmalige und wiederkehrende Kosten und den Aufwand für die umzusetzenden Maßnahmen ermitteln
- Ersatzmaßnahmen für nicht finanzierbare oder nicht leistbare Maßnahmen auflisten
- Entscheidung herbeiführen, welche Ressourcen für die Umsetzung der Maßnahmen eingesetzt werden sollen
- Gegebenenfalls Restrisiko aufzeigen und Entscheidung der Leitungsebene dazur einholen
- Umsetzungsreihenfolge für die Maßnahmen festlegen, begründen und dokumentieren
- Termine für die Umsetzung festlegen und Verantwortung zuweisen
- Verlauf der Umsetzung und Einhaltung der Termine überwachen
- Betroffene Mitarbeiter schulen und sensibilisieren

10 Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit

Um den Informationssicherheitsprozess aufrechtzuerhalten und kontinuierlich verbessern zu können, müssen nicht nur angemessene Sicherheitsmaßnahmen implementiert und Dokumente fortlaufend aktualisiert werden, sondern auch der IS-Prozess selbst muss regelmäßig auf seine Wirksamkeit und Effizienz hin überprüft werden. Dabei sollte regelmäßig eine Erfolgskontrolle und Bewertung des IS-Prozesses durch die Leitungsebene stattfinden (Managementbewertung). Bei Bedarf (z. B. bei der Häufung von Sicherheitsvorfällen oder gravierenden Änderungen der Rahmenbedingungen) muss auch zwischen den Routineterminen getagt werden. Alle Ergebnisse und Beschlüsse müssen nachvollziehbar dokumentiert werden. Die Dokumente müssen aussagekräftig und für die jeweilige Zielgruppe verständlich sein, siehe auch Kapitel 5.2 *Informationsfluss im Informationssicherheitsprozess*. Es ist die Aufgabe des ISB, diese Informationen zu sammeln, zu verarbeiten und entsprechend kurz und übersichtlich für die Leitungsebene aufzubereiten.

10.1 Überprüfung des Informationssicherheitsprozesses auf allen Ebenen

Die Überprüfung des Informationssicherheitsprozesses ist unabdingbar, damit einerseits Fehler und Schwachstellen erkannt und abgestellt werden können und andererseits der IS-Prozess in Bezug auf seine Effizienz optimiert werden kann. Ziel dabei ist unter anderem die Verbesserung der Praxistauglichkeit von Strategie, Maßnahmen und organisatorischen Abläufen. Die wesentlichen Aspekte, die dabei betrachtet werden müssen, werden im Folgenden dargestellt.

Zur Effizienzprüfung und Verbesserung des Informationssicherheitsprozesses sollten Verfahren und Mechanismen eingerichtet werden, die einerseits die Realisierung der beschlossenen Maßnahmen und andererseits ihre Wirksamkeit und Effizienz überprüfen.

Die Informationssicherheitsstrategie sollte daher auch Leitaussagen zur Messung der Zielerreichung machen, dabei sollte mindestens definiert werden:

- Welche Ziele in welcher Form und sinnvoller Anzahl überwacht oder gemessen werden (WAS),
- Wer für die Überwachung oder Messung der zuvor festgelegten Punkte verantwortlich ist (WER),
- Wann und wie häufig die Ergebnisse auszuwerten sind (WANN).

Grundsätzlich sollte sich die Überprüfung des Informationssicherheitsprozesses auf eine sinnvolle Anzahl von Zielen beschränken. Beispiele für Methoden können sein:

- Definition, Dokumentation und Auswertung von Kennzahlen (z. B. Aktualität des Virenschutzes und Anzahl detektierter Schadsoftware usw.)
- Detektion, Dokumentation und Auswertung von Sicherheitsvorfällen
- Durchführung von Übungen und Tests zur Simulation von Sicherheitsvorfällen und Dokumentation der Ergebnisse (z. B. Back-up-Wiederherstellung)
- interne und externe Audits, Datenschutzkontrollen
- Zertifizierung nach festgelegten Sicherheitskriterien (z. B. ISO 27001 auf Basis von IT-Grundschutz)

Die erfolgreiche Umsetzung von Sicherheitsmaßnahmen sollte regelmäßig überprüft werden. Grundsätzlich ist dabei wichtig, dass Prüfungen und Audits nicht von denjenigen durchgeführt werden, die die jeweiligen Sicherheitsvorgaben entwickelt haben, und dass die Leitung der Institution über den aus den Audits abgeleiteten Stand der Informationssicherheit informiert wird.

Um Betriebsblindheit zu vermeiden, kann es sinnvoll sein, externe Experten mit der Durchführung solcher Prüfungsaktivitäten zu beauftragen.

Da der Aufwand bei Audits von der Komplexität und Größe des Informationsverbunds abhängt, sind die Anforderungen auch für kleine Institutionen sehr gut umzusetzen. Mithilfe von automatisiertem Monitoring und Reporting kann eine kontinuierliche Analyse der Informationssicherheit bei geringer Ressourcenbelastung ermöglicht werden. Mit einer Durchsicht vorhandener Dokumentationen, um die Aktualität zu prüfen, und einem Workshop, bei dem Probleme und Erfahrungen mit dem Sicherheitskonzept besprochen werden, kann in kleinen Institutionen bereits ein ausreichender Überblick über den Status der Informationssicherheit gewonnen werden.

10.1.1 Überprüfung anhand von Kennzahlen

Kennzahlen werden in der Informationssicherheit eingesetzt, um den IS-Prozess bzw. Teilaspekte davon messbar zu machen. Sie dienen dazu, den Prozess zu optimieren und Güte, Effizienz und Effektivität der vorhandenen Sicherheitsmaßnahmen zu überprüfen.

Messungen und Kennzahlen dienen häufig der Kommunikation mit dem Management und können dem Informationssicherheitsmanagement wertvolle Argumentationshilfen liefern. Daher ist es wichtig, Messwerkzeuge so auszuwählen und durchgeführte Messungen so aufzubereiten, dass sie in das strategische Umfeld der eigenen Institution passen.

Kennzahlen zu ermitteln, bedeutet immer auch Aufwand. Dieser sollte in einer vernünftigen Relation zu den erhofften bzw. erzielten Ergebnissen stehen. Kennzahlen haben eine begrenzte Aussagekraft, da damit einzelne, meist wenige Bereiche der Informationssicherheit punktuell beleuchtet werden, nämlich meist diejenigen, in denen sich leicht Messwerte erzielen lassen. Dies betrifft im Allgemeinen die technische Sicherheit, bei der über Sensoren automatisiert Messwerte zurückgemeldet werden können, und andere, leicht quantifizierbare Aussagen, wie z. B.

- Anzahl der erkannten Schadsoftware-Muster,
- Anzahl der installierten Sicherheitspatches,
- Dauer der Systemausfälle,
- Anzahl der durchgeführten Sicherheitsschulungen.

Kennzahlen lassen sich immer unterschiedlich interpretieren, wichtig ist daher, dass im Vorfeld klar ist, welches Ziel mit Messungen verfolgt wird und wie und mit welchem Aufwand dies erreicht werden soll. Gegen dieses Ziel kann dann gemessen werden.

10.1.2 Bewertung des ISMS mithilfe eines Reifegradmodells

Die Wirksamkeit des Managementsystems für Informationssicherheit einer Institution sollte regelmäßig bewertet werden. Dies kann mithilfe eines Reifegradmodells erfolgen. Ein Reifegradmodell ermöglicht, den Fortschritt des ISMS nachvollziehbar über die Jahre hinweg zu dokumentieren, ohne sich dabei in Einzelmaßnahmen zu verlieren. Es stellt eine weitere potenzielle Kennzahl zur Steuerung der Informationssicherheit in einer Institution dar. Eine beispielhafte Reifegradbewertung eines ISMS kann wie folgt aussehen:

Reifegrad	Erläuterung
0	Es existiert kein ISMS und es ist auch nichts geplant.
1	ISMS ist geplant, aber nicht etabliert.
2	ISMS ist zum Teil etabliert.
3	ISMS ist voll etabliert und dokumentiert.
4	Zusätzlich zum Reifegrad 3 wird das ISMS regelmäßig auf Effektivität überprüft.
5	Zusätzlich zum Reifegrad 4 wird das ISMS regelmäßig verbessert.

Die Bewertung des Reifegrads eines ISMS kann sich durchaus mehrdimensional anhand von Themenfeldern darstellen, beispielsweise angelehnt an das Schichtenmodell des IT-Grundschutzes:

- ISMS (Managementsysteme für Informationssicherheit)
- ORP (Organisation und Personal)
- CON (Konzepte und Vorgehensweisen)
- OPS (Betrieb)
- DER (Detektion und Reaktion)
- INF (Infrastruktur)
- NET (Netze und Kommunikation)
- SYS (IT-Systeme)
- APP (Anwendungen)
- IND (Industrielle IT)

Informationssicherheit ist eine Querschnittsfunktion, welche mit nahezu allen Bereichen einer Institution verzahnt ist. Aus diesem Grund ist es notwendig, die Informationssicherheit in bestehende Prozesse einer Institution zu integrieren. Beispiele hierfür sind:

- Projektmanagement: Bereits in der Planungsphase eines Projektes muss der Schutzbedarf der zukünftig als Ergebnis zu verarbeitenden Informationen bewertet werden; darauf aufbauend sollte zudem die Planung geeigneter Sicherheitsmaßnahmen erfolgen.
- Incident-Management: Bei Störungen des IT-Betriebs mit Auswirkungen auf die Informationssicherheit muss das Vorgehen mit dem Sicherheitsmanagement abgestimmt sein. Das Security-Incident-Management und Störungsmanagement der IT und des Facility-Managements müssen verzahnt sein.

Existieren solche Managementprozesse nicht, ist es möglich, ein ISMS aufzubauen und zu betreiben, es wird jedoch nicht effizient funktionieren. Wenn das ISMS nicht mit dem Projektmanagement verzahnt ist, kann der Schutzbedarf neuer oder geänderter Geschäftsprozesse nur durch zyklische Abfragen (jährlich, quartalsweise) ermittelt werden. Dadurch ist es deutlich schwieriger, eine vollständige und aktuelle Schutzbedarfsfeststellung aller Zielobjekte zu erhalten. Wenn kein Störungsmanagement vorhanden ist, werden Sicherheitsvorfälle nicht erkannt bzw. nicht an die korrekte Stelle gemeldet. Der Reifegrad der Informationssicherheit hängt somit auch vom Reifegrad der anderen Managementprozesse der Institution ab und ist keine selbstständige Größe.

Der Reifegrad der Informationssicherheit kann von Institution zu Institution sehr unterschiedlich sein. Allein aus der Tatsache, dass ein Sicherheitsmanagement vorhanden ist, kann nicht darauf geschlossen werden, dass die Institution Sicherheitsvorfälle gut bewältigen kann. Durch eine einheitliche und differenzierte Bewertung des Umsetzungsniveaus des ISMS einer Institution können verschiedene wichtige Ziele erreicht werden:

- Überprüfung, ob die einzelnen Aspekte des Sicherheitsmanagements vollständig bearbeitet und umgesetzt wurden,
- Erkennung von Verbesserungs- und Weiterentwicklungspotenzialen,
- Vergleichbarkeit des Umsetzungsniveaus beim Sicherheitsmanagement zwischen verschiedenen Institutionen,
- Nachweisbarkeit des erreichten Umsetzungsniveaus gegenüber Dritten.

Zusätzlich kann die Leitungsebene die Bewertungsergebnisse auch als Kennzahlen nutzen, um das Sicherheitsmanagementsystem zu steuern und weiterzuentwickeln (siehe Kapitel 5.2.1).

Wird das Umsetzungsniveau regelmäßig beurteilt, kann die kontinuierliche Weiterentwicklung des Informationssicherheitsmanagements der Institution nachvollziehbar und effizient dokumentiert werden.

10.1.3 Überprüfung der Umsetzung der Sicherheitsmaßnahmen

Im Realisierungsplan ist für alle Maßnahmen des Sicherheitskonzepts enthalten, wer diese bis wann umzusetzen hat (Aufgabenliste und zeitliche Planung). Anhand dessen ist eine Auswertung möglich, inwieweit diese Planungen eingehalten wurden. Die Überprüfung des Informationssicherheitsprozesses dient zur Kontrolle der Aktivitäten im Rahmen des Sicherheitskonzepts und zur Identifizierung von Planungsfehlern.

Nach der Einführung von neuen Sicherheitsmaßnahmen sollte durch den ISB geprüft werden, ob die notwendige Akzeptanz seitens der Mitarbeiter vorhanden ist. Die Ursachen fehlender Akzeptanz sind herauszuarbeiten und abzustellen.

Sicherheitsrevision

Die Informationssicherheitsrevision (IS-Revision) ist ein Bestandteil eines jeden erfolgreichen Informationssicherheitsmanagements. Nur durch die regelmäßige Überprüfung der etablierten Sicherheitsmaßnahmen und des Informationssicherheitsprozesses können Aussagen über deren wirksame Umsetzung, Aktualität, Vollständigkeit und Angemessenheit und damit über den aktuellen Zustand der Informationssicherheit getroffen werden. Die IS-Revision ist somit ein Werkzeug zum Feststellen, Erreichen und Aufrechterhalten eines angemessenen Sicherheitsniveaus in einer Institution. Das BSI hat hierzu mit dem *Leitfaden für die IS-Revision auf Basis von IT-Grundschutz* ein Verfahren entwickelt, um den Status der Informationssicherheit in einer Institution festzustellen und Schwachstellen identifizieren zu können (siehe [BSIR]).

Die im IT-Grundschutz Kompendium enthaltenen Sicherheitsanforderungen können auch für die Revision der Informationssicherheit genutzt werden. Hierzu wird die gleiche Vorgehensweise wie beim IT-Grundschutz-Check empfohlen. Hilfreich und arbeitsökonomisch ist es, für jeden Baustein des IT-Grundschutz Kompendiums anhand der Anforderungen eine speziell auf die eigene Institution angepasste Checkliste zu erstellen. Dies erleichtert die Revision und verbessert die Reproduzierbarkeit der Ergebnisse.

Cyber-Sicherheits-Check

Mithilfe eines Cyber-Sicherheits-Checks können Institutionen das aktuelle Niveau der Cybersicherheit in ihrer Institution bestimmen. Der Cyber-Sicherheits-Check richtet sich an Institutionen, die sich bislang weniger intensiv mit dem Thema der Cyber-Sicherheit beschäftigt haben. Zur Durchführung eines Cyber-Sicherheits-Checks werden explizit keine obligatorischen Voraussetzungen an Dokumentenlage oder Umsetzungsstatus gestellt (siehe [CSC]).

Der Cyber-Sicherheits-Check und die zugrunde liegenden Maßnahmenziele für die Beurteilung der Cyber-Sicherheit wurden so konzipiert, dass das Risiko, einem Cyber-Angriff zum Opfer zu fallen, durch regelmäßige Durchführung eines Cyber-Sicherheits-Checks minimiert werden kann. Dabei wurde die Vorgehensweise auf Cyber-Sicherheitsbelange ausgerichtet.

Das BSI und die ISACA stellen einen praxisnahen Handlungsleitfaden zur Verfügung, der konkrete Vorgaben und Hinweise für die Durchführung eines Cyber-Sicherheits-Checks und die Berichtserstellung enthält. Ein besonders interessanter Mehrwert ist die Zuordnung der zu beurteilenden Maßnahmenziele zu den bekannten Standards der Informationssicherheit (IT-Grundschutz, ISO 27001, COBIT, PCI DSS).

10.1.4 Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz

Eine Zertifizierung ist eine Methode, um die Erreichung der Sicherheitsziele und die Umsetzung der Sicherheitsmaßnahmen durch qualifizierte unabhängige Stellen zu überprüfen. Durch eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz erhält eine Institution nachvollziehbare, wiederholbare und vergleichbare Auditergebnisse.

10.2 Eignung der Informationssicherheitsstrategie

Um den Informationssicherheitsprozess erfolgreich steuern und lenken zu können, muss die Leitungsebene einen Überblick darüber haben, inwieweit die Sicherheitsziele mithilfe der eingesetzten Sicherheitsstrategie tatsächlich erreicht werden konnten.

Aktualität von Sicherheitszielen, Rahmenbedingungen und Sicherheitskonzeption

Bezüglich einer längeren Perspektive ist es auch notwendig, die gesetzten Sicherheitsziele und Rahmenbedingungen zu überprüfen. Gerade in schnelllebigen Branchen ist eine entsprechende Anpassung der Sicherheitsleitlinie und der Sicherheitsstrategie von elementarer Bedeutung.

Auch betriebliche Änderungen (z. B. Einsatz neuer IT-Systeme, Umzug), organisatorische Änderungen (z. B. Outsourcing) und Änderungen gesetzlicher Anforderungen müssen schon bei ihrer Planungsphase mit in die Sicherheitskonzeption einbezogen werden. Die Sicherheitskonzeption und die dazugehörige Dokumentation muss nach jeder relevanten Änderung aktualisiert werden. Dies muss auch im Änderungsprozess der Institution berücksichtigt werden. Dafür muss der Informationssicherheitsprozess in das Änderungsmanagement der Institution integriert werden.

Wirtschaftlichkeitsbetrachtung

Die Wirtschaftlichkeit der Sicherheitsstrategie und die spezifischen Sicherheitsmaßnahmen sollten konstant unter Beobachtung stehen. Es ist zu prüfen, ob die tatsächlich angefallenen Kosten den ursprünglich geplanten Kosten entsprechen oder ob alternativ andere, ressourcenschonendere Sicherheitsmaßnahmen eingesetzt werden können. Ebenso ist es wichtig, regelmäßig den Nutzen der vorhandenen Sicherheitsmaßnahmen herauszuarbeiten.

Rückmeldungen von Internen und Externen

Rückmeldungen über Fehler und Schwachstellen in den Prozessen kommen im Allgemeinen nicht nur von der Informationssicherheitsorganisation oder der Revision, sondern auch von Mitarbeitern, Geschäftspartnern, Kunden oder Partnern. Die Institution muss daher eine wirksame Vorgehensweise festlegen, um mit Beschwerden und anderen Rückmeldungen von Internen und Externen umzugehen. Beschwerden von Kunden oder Mitarbeitern können dabei auch ein Indikator für Unzufriedenheit sein. Es sollte möglichst bereits entstehender Unzufriedenheit entgegengewirkt werden, da bei zufriedenen Mitarbeitern die Gefahr von fahrlässigen oder vorsätzlichen Handlungen, die den Betrieb stören könnten, geringer ist.

Es muss daher ein klar definiertes Verfahren und eindeutig festgelegte Kompetenzen für den Umgang mit Beschwerden und für die Rückmeldung von Problemen an die zuständige Instanz geben. So sollte auf Beschwerden schnellstmöglich geantwortet werden, damit die Hinweisgeber sich auch ernst genommen fühlen. Die gemeldeten Probleme müssen bewertet und der Handlungsbedarf eingeschätzt werden. Die Institution muss daraufhin angemessene Korrekturmaßnahmen zur Beseitigung der Ursachen von Fehlern ergreifen, um deren erneutes Auftreten zu verhindern.

Fortentwicklung des ISMS

Auch das ISMS muss kontinuierlich weiterentwickelt werden und an neue Erkenntnisse, die sich beispielsweise aus der Überprüfung des Informationssicherheitsprozesses ergeben haben können, angepasst werden.

Erweiterung der gewählten Vorgehensweise

Bei Einstieg in den Sicherheitsprozess hat die Leitung der Institution sich für eine Vorgehensweise entschieden, um auf Basis von IT-Grundschutz oder auch anderen Methoden ein bestimmtes Sicherheitsniveau für einen definierten Geltungsbereich zu erreichen. Wenn diese Vorgehensweise umgesetzt und die Phase der Aufrechterhaltung und kontinuierlichen Verbesserung der Informationssicherheit erreicht wurde, muss überlegt werden, ob

- die gewählte Vorgehensweise ergänzt werden soll (beispielsweise von Basis- auf Standard-Absicherung) und/oder
- der Geltungsbereich erweitert werden soll (beispielsweise von Kern-Absicherung eines eingegrenzten Bereiches auf einen größeren Informationsverbund).

Ziel sollte es sein, langfristig alle Bereiche der Institution auf ein ganzheitliches Sicherheitsniveau zu heben, das mindestens Standard-Absicherung umfasst.

10.3 Übernahme der Ergebnisse in den Informationssicherheitsprozess

Die Ergebnisse der Bewertung sind für die Verbesserung des IS-Prozesses notwendig. Es kann sich dabei herausstellen, dass eine Änderung der Sicherheitsziele, der Sicherheitsstrategie oder des Sicherheitskonzepts zu erfolgen hat und die Informationssicherheitsorganisation den Erfordernissen angepasst werden sollte. Unter Umständen ist es sinnvoll, Geschäftsprozesse, Abläufe oder die IT-Umgebung zu verändern, z. B. wenn Sicherheitsziele unter den bisherigen Rahmenbedingungen nicht oder nur umständlich (also mit hohem finanziellen oder personellen Aufwand) erreicht werden konnten. Wenn größere Veränderungen vorgenommen und umfangreiche Verbesserungen umgesetzt werden, schließt sich der Managementkreislauf wieder und es wird erneut mit der Planungsphase begonnen.

Die Überprüfungen zu den einzelnen Themen müssen von geeigneten Personen durchgeführt werden, die die notwendige Kompetenz und Unabhängigkeit gewährleisten können. Vollständigkeits- und Plausibilitätskontrollen sollten nicht durch die Ersteller der Konzepte vollzogen werden. Durchgeführte Verbesserungen, Korrekturen und Anpassungen sollten dokumentiert werden.

Die grundsätzliche Vorgehensweise der Institution zur Überprüfung und Verbesserung des Informationssicherheitsprozesses sollte in einer entsprechenden Richtlinie dokumentiert und von der Leitungsebene verabschiedet werden. In der **Richtlinie zur Überprüfung und Verbesserung des Informationssicherheitsprozesses** sollte insbesondere geregelt werden, wie interne Audits im Bereich der Informationssicherheit durchzuführen sind und wie die Ergebnisse in den Änderungsprozess einfließen. Prüfergebnisse und -berichte sind im Allgemeinen als vertraulich zu betrachten und müssen daher besonders gut geschützt werden.

Aktionspunkte zu 10 Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit
• Grundsätzliche Vorgehensweise der Institution zur Überprüfung und Verbesserung des Informationssicherheitsprozesses in einer entsprechenden Richtlinie dokumentieren und der Leitungsebene zur Verabschiedung vorlegen
• Messung der Zielerreichung in die Sicherheitsstrategie integrieren
• Einhaltung des Realisierungsplans prüfen
• Realisierung der beschlossenen Maßnahmen überprüfen
• Wirksamkeit und Effizienz der beschlossenen Maßnahmen überprüfen
• Prüfen, ob die Sicherheitsmaßnahmen akzeptiert werden, und gegebenenfalls nachbessern
• Rollenkonflikt zwischen Ersteller und Prüfer beachten
• Vertraulichkeit der Untersuchungsergebnisse sicherstellen
• Eignung und Aktualität von Sicherheitszielen, -strategien und -konzeption prüfen
• Angemessenheit der bereitgestellten Ressourcen und die Wirtschaftlichkeit der Sicherheitsstrategie und der -maßnahmen überprüfen
• Ergebnisse der Überprüfungen in Form von Verbesserungen in den Informationssicherheitsprozess einfließen lassen

11 Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz

Um die erfolgreiche Umsetzung von IT-Grundschutz nach außen transparent machen zu können, kann sich das Unternehmen oder die Behörde nach ISO/IEC 27001 zertifizieren lassen. Das BSI hat ein Zertifizierungsschema für Informationssicherheit entwickelt, das die Anforderungen an Managementsysteme für die Informationssicherheit aus ISO/IEC 27001 berücksichtigt und als Prüfkataloge das IT-Grundschutz-Kompendium sowie die BSI-Standards 200-x zugrunde legt. Dies wird deshalb als ISO 27001-Zertifizierung auf Basis von IT-Grundschutz bezeichnet. Eine solche Zertifizierung ist für die Standard-Absicherung vorgesehen sowie für die Kern-Absicherung grundsätzlich möglich. Bei einer reinen Basis-Absicherung reichen die umgesetzten Sicherheitsmaßnahmen für eine Zertifizierung nicht aus, können aber als Einstieg für eine der anderen beiden Vorgehensweisen dienen.

Das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz bietet Unternehmen und Behörden die Möglichkeit, ihre Bemühungen um Informationssicherheit transparent zu machen. Dies kann sowohl gegenüber Kunden als auch gegenüber Geschäftspartnern als Qualitätsmerkmal dienen und somit zu einem Wettbewerbsvorteil führen.

Dabei sind die Interessen an einer ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz vielfältig:

- Dienstleister möchten mithilfe dieses Zertifikats einen vertrauenswürdigen Nachweis führen, dass sie die Maßnahmen gemäß IT-Grundschutz realisiert haben.
- Kooperierende Unternehmen möchten sich darüber informieren, welchen Grad von Informationssicherheit ihre Geschäftspartner zusichern können.
- Von Institutionen, die neu an ein Netz angeschlossen werden, wird der Nachweis darüber verlangt, dass sie eine ausreichende Informationssicherheit besitzen, damit durch den Anschluss ans Netz keine untragbaren Risiken entstehen.
- Institutionen möchten dem Kunden bzw. Bürger gegenüber ihre Bemühungen um eine ausreichende Informationssicherheit deutlich machen.

Da der IT-Grundschutz mit der in diesem Dokument beschriebenen Vorgehensweise zum Sicherheitsmanagement und den im IT-Grundschutz-Kompendium enthaltenen Sicherheitsanforderungen inzwischen einen Quasi-Standard für Informationssicherheit darstellt, bietet es sich an, dies als allgemein anerkanntes Kriterienwerk für Informationssicherheit zu verwenden.

Grundlage für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist die Durchführung eines Audits durch einen externen, beim BSI zertifizierten Auditor. Das Ergebnis des Audits ist ein Auditbericht, der der Zertifizierungsstelle vorgelegt wird, die über die Vergabe des ISO 27001-Zertifikats auf der Basis von IT-Grundschutz entscheidet. Kriterienwerke des Verfahrens sind neben der Norm ISO 27001 die in diesem Dokument beschriebene IT-Grundschutz-Vorgehensweise und das IT-Grundschutz Kompendium des BSI.

Über ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz wird zunächst nachgewiesen, dass IT-Grundschutz im betrachteten Informationsverbund erfolgreich umgesetzt worden ist. Darüber hinaus zeigt ein solches Zertifikat auch, dass in der jeweiligen Institution

- Informationssicherheit ein anerkannter Wert ist,
- ein funktionierendes IS-Management vorhanden ist und außerdem
- zu einem bestimmten Zeitpunkt ein definiertes Sicherheitsniveau erreicht wurde.

Weitere Informationen zur Zertifizierung nach ISO 27001 und zur Zertifizierung als ISO 27001-Auditor auf der Basis von IT-Grundschutz finden sich auf der Website des BSI (siehe [ZERT]).

Aktionspunkte zu 11 Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz

- Informationen zum Schema für die ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz lesen
- Prüfen, ob die Bemühungen um Informationssicherheit anhand eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz transparent gemacht werden sollen
- Gegebenenfalls prüfen, ob das Informationssicherheitsmanagement und der Sicherheitszustand die entsprechenden Voraussetzungen erfüllen
- Gegebenenfalls den Zertifizierungsprozess initiieren

12 Anhang

12.1 Erläuterungen zu den Schadensszenarien

Im Folgenden sind für die in Kapitel 8.2.1 definierten Schadensszenarien beispielhafte Fragestellungen aufgeführt. Diese Fragen sollen als Hilfsmittel für die Schutzbedarfsfeststellung dienen, vor allem im Bereich der Anwendungen. Anhand der individuellen Anforderungen sollten die Fragen angepasst und ergänzt werden.

Schadensszenario „Verstoß gegen Gesetze/Vorschriften/Verträge"

Sowohl aus dem Verlust der Vertraulichkeit als auch der Integrität und ebenso der Verfügbarkeit können derlei Verstöße resultieren. Die Schwere des Schadens ist dabei oftmals abhängig davon, welche rechtlichen Konsequenzen daraus für die Institution entstehen können.

Beispiele für relevante Gesetze sind (in Deutschland):

Grundgesetz, Bürgerliches Gesetzbuch, Strafgesetzbuch, Bundesdatenschutzgesetz und Datenschutzgesetze der Länder, EU-Datenschutz-Grundverordnung (DSGVO [DSGVO]), Sozialgesetzbuch, Handelsgesetzbuch, Personalvertretungsgesetz, Betriebsverfassungsgesetz, Urheberrechtsgesetz, Patentgesetz, Informations- und Kommunikationsdienstegesetz (IuKDG), Gesetz zur Kontrolle und Transparenz im Unternehmen (KonTraG).

Beispiele für relevante Vorschriften sind:

Verwaltungsvorschriften, Verordnungen und Dienstvorschriften.

Beispiele für Verträge:

Dienstleistungsverträge im Bereich Datenverarbeitung, Verträge zur Wahrung von Betriebsgeheimnissen.

Fragen:

Verlust der Vertraulichkeit

- Erfordern gesetzliche Auflagen die Vertraulichkeit der Informationen?
- Ist im Falle einer Veröffentlichung von Informationen mit Strafverfolgung oder Regressforderungen zu rechnen?
- Sind Verträge einzuhalten, die die Wahrung der Vertraulichkeit bestimmter Informationen beinhalten?

Verlust der Integrität

- Erfordern gesetzliche Auflagen die Integrität der Informationen?
- In welchem Maße wird durch einen Verlust der Integrität gegen Gesetze bzw. Vorschriften verstoßen?

Verlust der Verfügbarkeit

- Sind bei Ausfall der Anwendung Verstöße gegen Vorschriften oder sogar Gesetze die Folge?
- Schreiben Gesetze die dauernde Verfügbarkeit bestimmter Informationen vor?
- Gibt es Termine, die bei Einsatz der Anwendung zwingend einzuhalten sind?
- Gibt es vertragliche Bindungen für bestimmte einzuhaltende Termine?

Schadensszenario „Beeinträchtigung des informationellen Selbstbestimmungsrechts“

Bei der Implementation und dem Betrieb von IT-Systemen und Anwendungen besteht die Gefahr einer Verletzung des informationellen Selbstbestimmungsrechts bis hin zu einem Missbrauch personenbezogener Daten.

Beispiele für die Beeinträchtigung des informationellen Selbstbestimmungsrechts sind:

- Unzulässige Erhebung personenbezogener Daten ohne Rechtsgrundlage oder Einwilligung,
- unbefugte Kenntnisnahme bei der Datenverarbeitung bzw. der Übermittlung von personenbezogenen Daten,
- unbefugte Weitergabe personenbezogener Daten,
- Nutzung von personenbezogenen Daten zu einem anderen als dem bei der Erhebung zulässigen Zweck und
- Verfälschung von personenbezogenen Daten in IT-Systemen oder bei der Übertragung.

Die folgenden Fragen können zur Abschätzung möglicher Folgen und Schäden herangezogen werden:

Fragen:

Verlust der Vertraulichkeit

- Welche Schäden können für den Betroffenen entstehen, wenn seine personenbezogenen Daten nicht vertraulich behandelt werden?
- Werden personenbezogene Daten für unzulässige Zwecke verarbeitet?
- Ist es im Zuge einer zulässigen Verarbeitung personenbezogener Daten möglich, aus diesen Daten z. B. auf den Gesundheitszustand oder die wirtschaftliche Situation einer Person zu schließen?
- Welche Schäden können durch den Missbrauch der gespeicherten personenbezogenen Daten entstehen?

Verlust der Integrität

- Welche Schäden entstünden für den Betroffenen, wenn seine personenbezogenen Daten unabsichtlich verfälscht oder absichtlich manipuliert würden?
- Wann würde der Verlust der Integrität personenbezogener Daten frühestens auffallen?

Verlust der Verfügbarkeit

- Können bei einem Ausfall der Anwendung oder bei einer Störung der Datenübertragung personenbezogene Daten verloren gehen oder verfälscht werden, sodass der Betroffene in seiner gesellschaftlichen Stellung beeinträchtigt wird oder gar persönliche oder wirtschaftliche Nachteile zu befürchten hat?

Schadensszenario „Beeinträchtigung der persönlichen Unversehrtheit“

Die Fehlfunktion von IT-Systemen oder Anwendungen kann unmittelbar die Verletzung, die Invalidität oder den Tod von Personen nach sich ziehen. Die Höhe des Schadens ist am direkten persönlichen Schaden zu messen.

Beispiele für solche Anwendungen und IT-Systeme sind:

- medizinische Überwachungsrechner,

- medizinische Diagnosesysteme,
- Flugkontrollrechner und
- Verkehrsleitsysteme.

Fragen:

Verlust der Vertraulichkeit

- Kann durch das Bekanntwerden von Informationen eine Person physisch oder psychisch geschädigt werden?

Verlust der Integrität

- Können Menschen durch manipulierte Programmabläufe oder Daten gesundheitlich gefährdet werden?

Verlust der Verfügbarkeit

- Bedroht der Ausfall der Anwendung oder des IT-Systems unmittelbar die persönliche Unversehrtheit von Personen?

Schadensszenario „Beeinträchtigung der Aufgabenerfüllung"

Gerade der Verlust der Verfügbarkeit einer Anwendung oder der Integrität von Informationen oder Daten kann die Aufgabenerfüllung in einer Institution erheblich beeinträchtigen. Die Schwere des Schadens richtet sich hierbei nach der zeitlichen Dauer der Beeinträchtigung und nach dem Umfang der Einschränkungen der angebotenen Dienstleistungen.

Beispiele hierfür sind:

- Fristversäumnisse durch verzögerte Bearbeitung von Verwaltungsvorgängen,
- verspätete Lieferung aufgrund verzögerter Bearbeitung von Bestellungen,
- fehlerhafte Produktion aufgrund falscher Steuerungsdaten und
- unzureichende Qualitätssicherung durch Ausfall eines Testsystems.

Fragen:

Verlust der Vertraulichkeit

- Gibt es Informationen, deren Vertraulichkeit die Grundlage für die Aufgabenerfüllung ist (z. B. Strafverfolgungsinformationen, Ermittlungsergebnisse)?

Verlust der Integrität

- Können Veränderungen an Informationen die Aufgabenerfüllung in der Art einschränken, dass die Institution handlungsunfähig wird?
- Entstehen erhebliche Schäden, wenn die Aufgaben trotz verfälschter Informationen wahrgenommen werden? Wann werden unerlaubte Datenveränderungen frühestens erkannt?
- Können verfälschte Informationen in der betrachteten Anwendung zu Fehlern in anderen Anwendungen führen?
- Welche Folgen entstehen, wenn Daten fälschlicherweise einer Person zugeordnet werden, die diese Daten in Wirklichkeit gar nicht erzeugt hat?

Verlust der Verfügbarkeit

- Gibt es Informationen, bei denen eine Einschränkung der Verfügbarkeit schwerwiegende Auswirkungen auf die Institution oder deren Geschäftsprozesse hätte?
- Kann durch den Ausfall von Anwendungen die Aufgabenerfüllung der Institution so stark beeinträchtigt werden, dass die Wartezeiten für die Betroffenen nicht mehr tolerabel sind?
- Sind von dem Ausfall dieser Anwendung andere Anwendungen betroffen?
- Ist es für die Institution bedeutsam, dass der Zugriff auf Anwendungen nebst Programmen und Daten ständig gewährleistet ist?

Schadensszenario „Negative Innen- oder Außenwirkung"

Durch den Verlust einer der Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit in einer Anwendung können verschiedenartige negative Innen- oder Außenwirkungen entstehen, zum Beispiel:

- Ansehensverlust einer Institution,
- Vertrauensverlust gegenüber einer Institution,
- Demoralisierung der Mitarbeiter,
- Beeinträchtigung der wirtschaftlichen Beziehungen zusammenarbeitender Institutionen,
- verlorenes Vertrauen in die Arbeitsqualität einer Institution und
- Einbüßen der Konkurrenzfähigkeit.

Die Höhe des Schadens orientiert sich an der Schwere des Vertrauensverlustes oder des Verbreitungsgrades der Innen- oder Außenwirkung.

Die Ursachen für solche Schäden können vielfältiger Natur sein:

- Handlungsunfähigkeit einer Institution durch IT-Ausfall,
- fehlerhafte Veröffentlichungen durch manipulierte Daten,
- Fehlbestellungen durch mangelhafte Lagerhaltungsprogramme,
- Nichteinhaltung von Verschwiegenheitserklärungen,
- Schuldzuweisungen an die falschen Personen,
- Verhinderung der Aufgabenerfüllung einer Abteilung durch Fehler in anderen Bereichen,
- Weitergabe von Fahndungsdaten an interessierte Dritte und
- Zuspielen vertraulicher Informationen an die Presse.

Fragen:

Verlust der Vertraulichkeit

- Welche Konsequenzen ergeben sich für die Institution durch die unerlaubte Veröffentlichung von schutzbedürftigen Informationen?
- Kann der Vertraulichkeitsverlust von Informationen zu einer Schwächung der Wettbewerbsposition führen?
- Entstehen bei der Veröffentlichung von vertraulichen Informationen Zweifel an der Vertrauenswürdigkeit der Institution?

- Können Veröffentlichungen von Informationen zur politischen oder gesellschaftlichen Verunsicherung führen?
- Können Mitarbeiter durch die unzulässige Veröffentlichung von Informationen das Vertrauen in ihre Institution verlieren?

Verlust der Integrität

- Welche Schäden können sich durch die Verarbeitung, Verbreitung oder Übermittlung falscher oder unvollständiger Informationen ergeben?
- Wird die Verfälschung von Informationen öffentlich bekannt?
- Entstehen bei einer Veröffentlichung von verfälschten Informationen Ansehensverluste?
- Können Veröffentlichungen von verfälschten Informationen zur politischen oder gesellschaftlichen Verunsicherung führen?
- Können verfälschte Informationen zu einer verminderten Produktqualität und damit zu einem Ansehensverlust führen?

Verlust der Verfügbarkeit

- Schränkt der Ausfall von Anwendungen die Informationsdienstleistungen für Externe ein?
- Verhindert die Nichtverfügbarkeit von Informationen oder der Ausfall von Geschäftsprozessen die Erreichung von Geschäftszielen?
- Ab wann wird die Nichtverfügbarkeit von Informationen oder der Ausfall von Anwendungen oder Geschäftsprozessen extern bemerkt?

Schadensszenario „Finanzielle Auswirkungen“

Unmittelbare oder mittelbare finanzielle Schäden können durch den Verlust der Vertraulichkeit schutzbedürftiger Informationen, die Veränderung von Informationen oder den Ausfall von Anwendungen entstehen. Beispiele dafür sind:

- unerlaubte Weitergabe von Forschungs- und Entwicklungsergebnissen,
- Manipulation von finanzwirksamen Daten in einem Abrechnungssystem,
- Ausfall eines IT-gesteuerten Produktionssystems und dadurch bedingte Umsatzverluste,
- unerlaubte Einsichtnahme in Marketingstrategiepapiere oder Umsatzzahlen,
- Ausfall eines Buchungssystems einer Reisegesellschaft,
- Ausfall eines E-Commerce-Servers,
- Zusammenbruch des Zahlungsverkehrs einer Bank,
- Diebstahl oder Zerstörung von Hardware.

Die Höhe des Gesamtschadens setzt sich zusammen aus den direkt und indirekt entstehenden Kosten, etwa durch Sachschäden, Schadenersatzleistungen und Kosten für zusätzlichen Aufwand (z. B. Wiederherstellung).

Fragen:

Verlust der Vertraulichkeit

- Kann die Veröffentlichung vertraulicher Informationen Regressforderungen nach sich ziehen?

- Gibt es innerhalb von Geschäftsprozessen oder Anwendungen Informationen, aus deren Kenntnis ein Dritter (z. B. Konkurrenzunternehmen) finanzielle Vorteile ziehen kann?
- Werden mit Anwendungen Forschungsdaten gespeichert, die einen erheblichen Wert darstellen? Was passiert, wenn sie unerlaubt kopiert und weitergegeben werden?
- Können durch vorzeitige Veröffentlichung von schutzbedürftigen Informationen finanzielle Schäden entstehen?

Verlust der Integrität

- Können durch Datenmanipulationen finanzwirksame Daten so verändert werden, dass finanzielle Schäden entstehen?
- Kann die Veröffentlichung falscher Informationen Regressforderungen nach sich ziehen?
- Können durch verfälschte Bestelldaten finanzielle Schäden entstehen (z. B. bei Just-in-Time-Produktion)?
- Können verfälschte Informationen zu falschen Geschäftsentscheidungen führen?

Verlust der Verfügbarkeit

- Wird durch den Ausfall von Anwendungen oder Geschäftsprozessen die Produktion, die Lagerhaltung oder der Vertrieb beeinträchtigt?
- Ergeben sich durch den Ausfall von Anwendungen oder Geschäftsprozessen finanzielle Verluste aufgrund von verzögerten Zahlungen bzw. Zinsverlusten?
- Wie hoch sind die Reparatur- oder Wiederherstellungskosten bei Ausfall, Defekt, Zerstörung oder Diebstahl von IT-Systemen?
- Kann es durch den Ausfall von Anwendungen oder Geschäftsprozessen zu mangelnder Zahlungsfähigkeit oder zu Konventionalstrafen kommen?
- Wie viele wichtige Kunden wären von einem Ausfall der Anwendungen oder der Geschäftsprozesse betroffen?

12.2 Literaturverzeichnis

[27000] ISO/IEC 27000:2016, International Organization for Standardization (Hrsg.), Information technology – Security techniques – Information Security management systems – Overview and vocabulary, ISO/IEC JTC 1/SC 27, 2016

[27001] ISO/IEC 27001:2013, International Organization for Standardization (Hrsg.), Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC JTC 1/SC 27, 2013

[27002] ISO/IEC 27002:2013, International Organization for Standardization (Hrsg.), Information technology – Security techniques – Code of practice for information security controls, ISO/IEC JTC 1/SC 27, 2013

[27004] ISO/IEC 27004:2016, International Organization for Standardization (Hrsg.), Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation, ISO/IEC JTC 1/SC 27, 2016

[27005] ISO/IEC 27005:2011, International Organization for Standardization (Hrsg.), Information technology – Security techniques – Information security risk management, ISO/IEC JTC 1/SC 27, 2011

[820-2] DIN 820-2:2012, Anhang H, Gestaltung von Dokumenten – Verbformen zur Formulierung von Festlegungen, NA 173-00-02 AA, 2012

[BSI1] Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 200-1, Version 1.0, Oktober 2017, https://www.bsi.bund.de/grundschutz

[BSI3] Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 200-3, Version 1.0, Oktober 2017, https://www.bsi.bund.de/grundschutz

[BSIR] Informationssicherheitsrevision – Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz, BSI, Version 2.0, März 2010, https://www.bsi.bund.de/is-revision

[CSC] Leitfaden Cyber-Sicherheits-Check, BSI, ISACA, 07. 03. 2014, https://www.allianz-fuer-cybersicherheit.de

[DSGVO] Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Europäisches Parlament und der Rat der Europäischen Union, 27. April 2016

[GSK] IT-Grundschutz-Kompendium, BSI, jährlich neu, https://www.bsi.bund.de/grundschutz

[ISF] The Standard of Good Practice 2016, ISF – Information Security Forum, 2016, https://www.securityforum.org/tool/the-isf-standardrmation-security

[NIST53] NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, NIST, 2015, http://csrc.nist.gov/publications/PubsSPs.html

[RFC2119] RFC 2119 (Key words for use in RFCs to Indicate Requirement Levels), Network Working Group, Stand 1997, https://www.ietf.org/rfc/rfc2119.txt

[SDM] Standard-Datenschutzmodell (SDM), SDM-Methodik-Handbuch, Konferenz der Datenschutzbeauftragten des Bundes und der Länder, V1.0, kann von allen Webservern der deutschen Datenschutz-Aufsichtsbehörden heruntergeladen werden, z. B. https://www.datenschutz-mv.de/datenschutz/sdm/sdm.html

[ZERT] Informationen zur Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz, BSI, https://www.bsi.bund.de/iso27001-zertifikate

FINANZVERWALTUNG
des Landes Nordrhein-Westfalen

Ministerium der Finanzen
des Landes Nordrhein-Westfalen

Grundsteinlegung in Kaarst: Meilenstein für das neue Rechenzentrum der Finanzverwaltung

© Landmarken AG

23.10.2023

Grundsteinlegung in Kaarst: Meilenstein für das neue Rechenzentrum der Finanzverwaltung

In Kaarst bei Düsseldorf entsteht das neue Rechenzentrum der Finanzverwaltung (RZF) des Landes Nordrhein-Westfalen, ein Gebäudeensemble mit rund 37.000 Quadratmetern Fläche. Gemeinsam mit dem Minister der Finanzen des Landes Nordrhein-Westfalen, Dr. Marcus Optendrenk, und vielen Projektbeteiligten wurde jetzt feierlich der Grundstein gelegt.

Das Neubauensemble, welches von der Landmarken AG als Entwickler in Zusammenarbeit mit den Generalunternehmern ZECH Bau und ICT Facilities errichtet wird, wird neben dem Rechenzentrum auch Flächen für Büro- und Besprechungsräume, Lager und Werkstätten, eine Druckerei und eine Kantine

bieten. Das Gebäudekonzept bietet attraktive Arbeitsplätze für die Mitarbeitenden der Finanzverwaltung. Hinzu kommen gut 370 Pkw-Stellplätze in einem Parkhaus, ein Außenparkbereich, E-Ladeplätze und über 250 Fahrradstellplätze.

Im Objekt werden künftig rund 1.000 Landesbedienstete tätig sein. „Das neue Rechenzentrum in Kaarst wird das digitale Rückgrat unserer Finanzverwaltung sein“, sagt Dr. Marcus Optendrenk, Minister der Finanzen des Landes Nordrhein-Westfalen. „Wir schaffen mit dem topmodernen Neubau exzellente Arbeitsbedingungen für unsere IT-Profis und tragen mit hohen Anforderungen an die Nachhaltigkeit unserer Verantwortung für Umwelt- und Klimaschutz Rechnung. Das RZF wird ein Leuchtturm für die digitale, bürgerfreundliche Steuerverwaltung der Zukunft.“

„Dieses Projekt zeigt, wie sinnvoll die Zusammenarbeit zwischen öffentlicher Hand und Privatwirtschaft sein kann", sagte Landmarken-Vorstand Jens Kreiterling und ergänzte: „Der Nutzer bekommt bei uns alles aus einer Hand: von der Planung eines hocheffizienten und komplexen Nutzungskonzeptes mit einem im Betrieb klimaneutralen Energiekonzept über die Realisierung bis hin zum anschließenden Betrieb mit entsprechender Kostensicherheit. Über alle diese Phasen gibt es einen Ansprechpartner für den Nutzer – die Landmarken AG.“

Der Neubau in Kaarst zeichnet sich durch besondere Nachhaltigkeit aus. Das Land Nordrhein-Westfalen hat sich zum Ziel gesetzt, bis zum Jahr 2030 eine bilanziell klimaneutrale Landesverwaltung zu erreichen. Das neue Rechenzentrum der Finanzverwaltung wird bei der Erreichung dieses ambitionierten Klimaschutzziels einen wichtigen Beitrag leisten, denn abgesehen von wenigen Spitzenlasten wird das Ensemble CO2-neutral betrieben werden. Grund ist unter anderem der Einsatz von Geothermie zur Versorgung mit Wärme und Kälte. Dafür werden rund 50 Erdwärmesonden in etwa 150 m Tiefe installiert. Auch Abwärme aus dem Rechenzentrum wird genutzt.

Der Betrieb läuft über Wärmepumpen, für die ein Teil des benötigten Stroms über eine Photovoltaik-Anlage auf dem Dach erzeugt wird. Durch Einsatz von Ökostrom kann der Neubau klimaneutral betrieben werden. Der Wärme- und Kältebedarf wurde über eine komplexe technische Simulation berechnet, die Energiesysteme wurden entsprechend ausgelegt.

Nach einem Bombenfund auf dem Grundstück Anfang Mai und einer erneuten Kampfmittelsondierung konnten im Juni die Erdarbeiten und wenig später die Gründungsarbeiten beginnen. Im August startete die Erstellung der Bodenplatten, nun geht es an den Hochbau. Die Fertigstellung ist für 2026 geplant.

FINANZVERWALTUNG
des Landes Nordrhein-Westfalen

Ministerium der Finanzen
des Landes Nordrhein-Westfalen

Landesamt zur Bekämpfung der Finanzkriminalität nimmt die Arbeit auf

© FM

15.01.2024

Landesamt zur Bekämpfung der Finanzkriminalität nimmt die Arbeit auf

Neue Landesbehörde für die Steuerfahndung in Düsseldorf ist ab sofort nordrhein-westfälische Schaltzentrale für überregionale Großverfahren / Stephanie Thien als erfahrene Dienststellenleiterin übernimmt Leitung.

Als erstes Land hat Nordrhein-Westfalen die Kompetenzen und das Know-How seiner Steuerfahndung für den Kampf gegen internationale Steuerverbrechen in einer eigenen Landesbehörde gebündelt. Das Landesamt zur Bekämpfung der Finanzkriminalität (LBF NRW) hat zum Start ins neue Jahr in einem Interimsgebäude in Düsseldorf seine Arbeit unter der erfahrenen Dienststellenleiterin Stephanie Thien aufgenommen.

„Die Gründung des LBF NRW ist eine logische Antwort auf die Einrichtung einer Europäischen Staatsanwaltschaft und die Vorbereitung auf eine intensivere Ermittlungszusammenarbeit im Rahmen der von Finanzminister Lindner angekündigten neuen Bundesbehörde“, erklärt Minister der Finanzen Dr. Marcus Optendrenk. „Die Welt ändert sich, und die Welt der professionellen Finanzkriminalität ändert sich sogar noch rasanter – sie wird internationaler, verzweigter, digitaler. Um Steuerbetrügern und

Geldwäschern über Staatengrenzen und durchs Netz auf den Fersen zu bleiben, brauchen wir schlanke, agile Strukturen in der Fahndung. Deshalb gehen wir in Nordrhein-Westfalen einen ganz neuen Weg: Wir bleiben mit unserer Steuerfahndung und den Stellen für Straf- und Bußgeldsachen in der Fläche präsent, ziehen aber Spezialwissen zu Kriminalitätsphänomenen und überregionale Großverfahren im neuen Landesamt zusammen, bauen dort zudem ein IT-Kompetenzzentrum auf und bringen neue Ermittlungsmethoden in den Einsatz."

Der Aufbau des LBF NRW erfolgt in zwei Stufen, von denen die erste mit dem Jahreswechsel gezündet wurde: Die neue Behörde tritt neben die zehn bestehenden Finanzämter für Steuerstrafsachen und Steuerfahndung (STRAFA-FÄ) im Land. Es bündelt dann im ersten Schritt die bisherigen Sondereinheiten der Steuerfahndung mit überregionalem Bezug wie die Task Force *zur Bekämpfung von Finanzierungsquellen Organisierter Kriminalität und Terrorismus* oder die Zentralstelle Umsatzsteuerbetrugsbekämpfung. Mit dem nächsten Jahreswechsel werden die STRAFA-FÄ dann unter Beibehaltung der bisherigen Standorte organisatorisch in das LBF NRW integriert.

„Die Herausforderungen unserer Fahnderinnen und Fahnder haben sich in den vergangenen Jahren stark gewandelt", erklärt Stephanie Thien, Leiterin des neuen LBF NRW. „Mit Ankauf und Auswertung von Datenträgern ist es nicht mehr getan, mehr und mehr sind wir mit organisierten Banden konfrontiert, die ihre Betrugsgeschäfte gezielt international aufbauen, Spuren gekonnt verwischen und sich verstärkt im virtuellen Raum bewegen sowie Kryptowährungen nutzen. Die Erfahrung mit hochkomplexen Ermittlungen in der jüngsten Vergangenheit hat uns klargemacht, dass wir uns operativ neu aufstellen müssen: Wir müssen aus Nordrhein-Westfalen heraus Großverfahren mit Verdächtigen sowie beteiligten Behörden in mehreren anderen Staaten führen können. Das LBF NRW nimmt organisierte Tätergruppen ins Visier, für die Steuerkriminalität nur einer ihrer verbrecherischen Geschäftszweige ist, und zieht sie nach dem Al-Capone-Prinzip aus dem Verkehr."

Die 60-jährige Juristin Thien arbeitet seit mehr als 30 Jahren in der nordrhein-westfälischen Finanzverwaltung, war in verschiedenen Finanzämtern quer durch das Ruhrgebiet eingesetzt, bevor sie ihre berufliche Heimat in der Steuerfahndung fand: Sie leitete von 2014 bis 2017 das Finanzamt für Steuerstrafsachen und Steuerfahndung in Düsseldorf, zuletzt jenes in Bochum mit der Zentralstelle für Kryptologie der nordrhein-westfälischen Steuerfahndung.

„Mit dem Aufbau der neuen Landesbehörde gegen Finanzkriminalität stellen wir unter Beweis, dass die öffentliche Verwaltung flexibel auf ein dynamisches Umfeld reagieren und ihre Strukturen den Anforderungen anpassen kann", betont Minister Dr. Optendrenk. „Wenn wir entdecken, dass Verbrechernetzwerke gezielt Grenzen von Zuständigkeiten und Staaten ausnutzen, um sich am Geld der Gemeinschaft zu bereichern, schaffen wir an diesen Grenzen die Schnittstellen, um der Spur des Geldes nahtlos bis zu den Drahtziehern folgen zu können. Nordrhein-Westfalen, das für seine herausragende Steuerfahndung bekannt ist, ist prädestiniert, diesen Ball aufzunehmen, ihn nach vorne zu spielen und auf deutscher wie europäischer Ebene das Passspiel vor dem Tor voranzubringen. Im Kampf gegen Steuerhinterziehung und Geldwäsche ist Teamplay unerlässlich. Unser Ziel ist die Zerschlagung krimineller Strukturen und die Absicherung der finanziellen Grundlage unserer Gesellschaft – das LBF NRW wird hier jetzt zum Spielmacher."

Ministerium der Finanzen
des Landes Nordrhein-Westfalen
Der Minister

LANDTAG
NORDRHEIN-WESTFALEN
18. WAHLPERIODE

VORLAGE
18/1482

A07, A07/1

12.08.2023"

Frau Fischer
Telefon 0211 4972-2282

Vorlage
an den Haushalts- und Finanzausschuss
des Landtags Nordrhein-Westfalen

Modernisierungsprogramm „Finanzverwaltung *für* Nordrhein-Westfalen“

Sitzung des Haushalts- und Finanzausschusses des Landtags Nordrhein-Westfalen am 17. August 2023

Mit dem Modernisierungsprogramm „Finanzverwaltung *für* Nordrhein-Westfalen“ soll die Verwaltung noch leistungsstärker, digitaler, beschäftigtenfreundlicher und serviceorientierter werden. Es handelt sich um einen fortlaufenden Entwicklungsprozess, in dem besonders mehrwertstiftende Projekte für unsere Finanzverwaltung umgesetzt werden.

In diesem Prozess werden die sich veränderten äußeren und inneren Rahmenbedingungen der Verwaltung bspw. in Folge der Digitalisierung, der Nachwuchsgewinnung in Zeiten des demographischen Wandels und des sich verschärfenden Wettbewerbs um Talente sowie weiterer Themen berücksichtigt, die die Finanzverwaltung fordern und Chancen bieten, sich weiter zu entwickeln.

Mit der Programmarbeit wird an Ergebnisse des Lenkungskreises der vergangenen Legislaturperiode „*Finanzverwaltung für Nordrhein-Westfalen*“ angeknüpft. Dieser hat sich vertieft mit Verbesserungspotenzialen für die Finanzverwaltung befasst sowie Lösungs- und Veränderungsvorschläge für die Zukunft erarbeitet.

Dienstgebäude und
Lieferanschrift:
Jägerhofstr. 6
40479 Düsseldorf
Telefon (0211) 4972-0
Telefax (0211) 4972-1217
Poststelle@fm.nrw.de
www.fm.nrw.de

Öffentliche Verkehrsmittel:
U74 bis U79
Haltestelle
Heinrich Heine Allee

Diese Ideen werden jetzt weiter in die Umsetzung gebracht. In der Vorbereitungsphase ab November 2022 wurden die Handlungsbedarfe, die Zielrichtung und die strategischen Schwerpunkte für das Programm identifiziert und für die Umsetzung organisiert. Zudem wurde eine für die Umsetzung geeignete projektförmige interne Programmstruktur etabliert. Darauf aufbauend wurde bis zum Ende des 1. Quartals 2023 die inhaltliche Ausgestaltung von Programmthemen und -vorhaben erarbeitet.

Die etablierte Programmstruktur sieht vor, die Umsetzung der identifizierten Projekte in vier Teilprogrammen „Struktur- und Prozessoptimierung", „Personalgewinnung und -bindung", „Serviceorientierung" sowie „Digitalisierung" zu steuern und zu begleiten. Die zur Umsetzung vorgesehenen Projekte besitzen häufig Anknüpfungspunkte in mehreren Teilprogrammen. Die Programmstruktur dient daher in besonderer Weise auch der Verzahnung der befassten Fachbereiche des Ministeriums der Finanzen (FM), der Oberfinanzdirektion (OFD), der Finanzämter, der Hochschule der Finanzen, der Landesfinanzschule, der Fortbildungsakademie der Finanzverwaltung und des Rechenzentrums der Finanzen (RZF) sowie der fortlaufenden Einbindung von Hauptpersonalvertretungen sowie Gleichstellungs- und Inklusionsbeauftragten. Die nachfolgende Darstellung gibt einen Überblick über die Ziele der vier Teilprogramme und über eine Auswahl der zur Umsetzung vorgesehenen Projekte:

- **Struktur- und Prozessoptimierung**: Das Ziel des Teilprogramms ist, bestehende Arbeitsstrukturen und -prozesse in den Finanzämtern weiter zu standardisieren und zu digitalisieren. Dies ist auch die Grundlage für eine flexible Fallsteuerung und (räumliche) Flexibilisierung der Arbeit. Dies dient dem Ziel, die Arbeit zum Personal zu bringen und eine Spezialisierung durch Zentralisierungen in einer dezentralen Ämterstruktur zu unterstützen. Dabei ist sicherzustellen, dass die Finanzverwaltung mit Standorten in der Fläche erhalten bleibt, um für Steuerpflichtige einen guten Service vor Ort und für die Beschäftigten ein attraktives Umfeld zu gewährleisten.
  Gleichzeitig soll die Steuerveranlagung noch risikoorientierter erfolgen und mittelfristig durch eine Steigerung der Autofallquote das „Massengeschäfts" rechtssicher möglichst weitgehend automatisiert werden. Auf diese Weise soll die Bearbeitung steuerehrlicher Fälle beschleunigt werden und Risikofälle zur personellen Bearbeitung identifiziert werden.

Im Rahmen eines ausgekoppelten Schnellboot-Projektes zur Struktur und Prozessoptimierung bei der Steuerstraffahndung und -verfolgung wird das Landesamts zur Bekämpfung der Finanzkriminalität in Nordrhein-Westfalen (LBF NRW) gegründet. Erleichterungen für Steuerehrliche und Erschwernisse für nicht Steuerehrliche werden mit diesen Maßnahmen forciert.

- **Personalgewinnung und -bindung:** Das Ziel des Teilprogramms ist, weiterhin qualifiziertes Personal für die Finanzverwaltung des Landes Nordrhein-Westfalen zu gewinnen und langfristig zu binden.
  Die Nachwuchsgewinnung ist für unsere Verwaltung und unser Land essentiell. Im Rahmen des Programms wurde der Einstieg in den Bewerbungsprozess optimiert und das Bewerbungstool umfangreich umprogrammiert. So ist zum Beispiel eine Bewerbung seit Juni problemlos über das Smartphone möglich. Dies wird dem Trend gerecht, dass immer mehr junge Menschen überwiegend mobil online sind. Außerdem wurden vereinfachte Voraussetzungen für die Zulassung zum Vorstellungsgespräch geschaffen.
  Begleitet werden soll die Nachwuchsgewinnung u. a. durch innovative Nachwuchswerbung und durch Maßnahmen für ein passgenaues Onboarding. Neue Kolleginnen und Kollegen sollen sich frühzeitig mit der Finanzverwaltung verbunden fühlen.
  Um bspw. den Studierenden und Auszubildenden die fachliche Vielseitigkeit unserer Verwaltung greifbar zu machen und nachhaltig von den hohen fachlichen Entwicklungsmöglichkeiten zu überzeugen, führen wir seit dem Regierungswechsel *Campusmessen* durch. Auf einer *Campusmesse* stellen sich die einzelnen Stellen und Einsatzgebiete der gesamten Finanzverwaltung vor, um den Nachwuchskräften bereits zu Beginn Orientierung und einen vertieften Einblick in die vielfältigen Einsatzmöglichkeiten nach der Ausbildung bzw. dem Studium zu geben.

  Ein weiterer Schwerpunkt ist es, die fachtheoretische Ausbildung bzw. das Studium enger mit der Praxis zu verzahnen und die Unterstützung der Auszubildenden und Studierenden zu verbessern.

  Um insgesamt eine gute praxisorientierte Analyse über die notwendigen Handlungsfelder zu erhalten, die im Bereich der Aus-

und Fortbildung zu reformieren sind, bringen auch die Beschäftigten Ideen, Ansätze und Expertise für neue Lösungen und Veränderungsprozesse ein. Bspw. wurden sie in der ersten Jahreshälfte 2023 im Rahmen von Zukunftskonferenzen mit agilen Arbeitsmethoden einbezogen, um eine größtmögliche Perspektivenvielfalt zu gewährleisten. Mitarbeitende, die einen Bezug zum jeweiligen Schwerpunktthema haben und die von den Auswirkungen betroffen sein werden, erarbeiteten neben gemeinsamen Werten, Visionen und Zielen zu den komplexen Problemen insbesondere einen Aktionsplan für die zukünftige konkrete Umsetzung (*„future search"*).

Nach dem Berufseinstieg erfolgt die Förderung, Weiterentwicklung und Qualifizierung der Beschäftigten auf Grundlage eines neuen Personalentwicklungskonzepts für die LG 1 zw. eines evaluierten Personalentwicklungskonzepts für die LG 2, die beide aktuell in Zusammenarbeit mit den Personalvertretungen er- bzw. überarbeitet werden.

Darüber hinaus ist die Unterstützung der erfahrenen Kräfte der Finanzverwaltung ein besonderes Anliegen im Programm. Es sollen Angebote unterbreitet werden, die die Kolleginnen und Kollegen der Finanzverwaltung durch Veränderungen begleiten. Eine bedarfsgerecht gestaltete Fortbildung soll hierbei den Weg der Kolleginnen und Kollegen begleiten und unterstützen. Die bereits jetzt angebotenen vielfältigen Fortbildungsmöglichkeiten untersuchen wir auf ihre Attraktivität, probieren neue Wege aus und bauen passgenaue, individuelle Angebote weiter aus.

- **Serviceorientierung:** Das Ziel des Teilprogramms ist es, die Services für Bürgerinnen und Bürger sowie Unternehmen weiterzuentwickeln. Die Finanzverwaltung soll noch einfacher und im Idealfall ressourcenschonend erreichbar gemacht werden. Die Leistungen der Finanzverwaltung sollen noch effizienter, digitaler und anwenderfreundlicher werden. Von verbesserten Abläufen sollen auch die Mitarbeiterinnen und Mitarbeiter der Finanzverwaltung profitieren, die in der täglichen Arbeit im Austausch mit Bürgerinnen und Bürger und Unternehmen stehen.

Im Jahr 2022 startete der Pilot des telefonischen Service und des Service vor Ort. Dieser wurde seitdem sukzessive auf insgesamt 32 Ämter erweitert. Die Lösungsquote im telefonischen Service liegt bei über 80 % und im Service vor Ort bei 99 %. Damit ist eine deutliche Entlastung des BackOffice Bereichs gegeben. Der Abschluss des Flächenrollouts ist für Mitte 2024 vorgesehen.

Ein weiteres Vorhaben in diesem Teilprogramm ist die fortlaufende Weiterentwicklung und Optimierung der Regelungen zur Mobilen Arbeit in den Dienststellen der Steuerverwaltung. Die Arbeitsform der Mobilen Arbeit ermöglicht den Beschäftigten ihre Arbeit zeitlich und örtlich zu flexibilisieren und berufliche und familiäre Interessen besser miteinander zu vereinbaren. Die Mobile Arbeit in den Finanzämtern hat sich während einer Pilotierungsphase bewährt und soll sich auch zukünftig fest in die Arbeitswelt der Finanzämter einfügen.

Weitere mittelfristige zentrale Vorhaben der Serviceorientierung sind der Ausbau barrierefreier und digitaler Informationsangebote sowie verwaltungsinterne Verbesserungen durch die Modernisierung von Raum- und Arbeitskonzepten.

- **Digitalisierung:** Das Ziel des Teilprogramms ist, die sich aus der Digitalisierung ergebenden Chancen und Möglichkeiten für die Finanzverwaltung nutzbar zu machen und mehrwertstiftend einsetzen – im Interesse der Bürgerinnen und Bürger sowie der Beschäftigten. Für das Teilprogramm Digitalisierung bestehen viele Anknüpfungspunkte zu den übrigen Teilprogrammen, bei denen die IT-Fachbereiche mit der Entwicklung geeigneter digitaler Lösungen unterstützen. Darüber hinaus werden im Rahmen des Teilprogramms federführend eigene weitere zentrale Vorhaben verfolgt: Bspw. wird das Ziel verfolgt, die Aufbau- und Ablauforganisation im RZF zu optimieren, indem Softwareentwicklung und Betrieb stärker miteinander verbunden werden, um die Produktivität und Agilität weiter zu verbessern. Die agile Softwareentwicklung ist Gegenstand eines weiteren Vorhabens, um digitale Lösungen über eine agile IT-Wertschöpfungskette schneller in Schritten bereitstellen zu können und so die Anpassungsfähigkeit an neue rechtliche und fachliche Entwicklungen zu steigern. Insbesondere die weitere Umsetzung des gemeinsam von Bund und Ländern

betriebenen Vorhabens KONSENS hat Auswirkungen auf die IT-Strukturen und die Digitalisierung unserer Finanzverwaltung. Gegenstand von KONSENS ist die fortlaufende Entwicklung, Einführung und Pflege der bundesweit einheitlichen Steuer-IT. Dabei koordiniert das Programm KONSENS@NRW die Ablösung bestehender Verfahren in Nordrhein-Westfalen durch IT-Produkte, die durch KONSENS bereitgestellt werden. Vor dem Hintergrund eines Berichts des Bundesrechnungshofes von Mai 2023 sowie in Folge der Augsburger Erklärung zu KONSENS der Konferenz der Präsidentinnen und Präsidenten der Rechnungshöfe des Bundes und der Länder von Oktober 2022 hat die Finanzministerkonferenz im Juni 2023 die Einrichtung einer Bund-Länder-Arbeitsgruppe auf Staatssekretärsebene beschlossen. Gemeinsam mit dem Bund koordiniert Nordrhein-Westfalen als derzeitiges Vorsitzland der Finanzministerkonferenz die Arbeitsgruppe, deren Auftrag es ist, bis Ende des Jahres 2023 die Strukturen und Prozesse von KONSENS zu evaluieren und Vorschläge zur Weiterentwicklung der Strukturen und Prozesse zu erarbeiten. Die mit der Einrichtung der Arbeitsgruppe angestrebte Evaluierung und Weiterentwicklung von KONSENS ist im Sinne der weiteren Digitalisierung unserer Finanzverwaltung von großer Bedeutung.

Die Aufnahme weiterer Vorhaben in die Programmstruktur wird regelmäßig geprüft.

Dr. Marcus Optendrenk

LANDTAG
NORDRHEIN-WESTFALEN
18. WAHLPERIODE

VORLAGE
18/1665

A07

Ministerium der Finanzen
des Landes Nordrhein-Westfalen
Der Minister

21.09.2023

Aktenzeichen
B 1402 - P H5

Helena Becker
Telefon 0211 4972-2188

Vorlage
an den Haushalts- und Finanzausschuss
des Landtags Nordrhein-Westfalen

Erläuterung zur Verpflichtungsermächtigung im Haushaltsplanentwurf 2024, Einzelplan 20, zur Finanzierung des Neubauvorhabens Verwaltungszentrum Haroldstraße 5 in Düsseldorf

Anlage: Zusätzliche Informationen zum Neubauprojekt Verwaltungszentrum Haroldstraße 5 in Düsseldorf

Mit der Neubebauung der Liegenschaft Haroldstraße 5 soll die Ausgestaltung eines neuen identitätsstiftenden Stadtbausteins an dieser stadträumlich prominenten Stelle der Landeshauptstadt Düsseldorf zur Realisierung eines ersten Bausteins aus den prämierten Ideen des städtischen Wettbewerbs „Blaugrüner Ring“ umgesetzt werden. Das Neubauvorhaben Verwaltungszentrum Haroldstraße 5 ist ein zentrales Projekt, um im Rahmen der Quartiersentwicklung in der Landeshauptstadt Düsseldorf den Autoverkehr von der bisherigen Haroldstraße zu verlagern und stattdessen eine „Grüne Haroldbucht“ sowie den Ausbau von Fahrradwegen zu realisieren.

Die Quartiersentwicklung und die Verwirklichung städtebaulicher Ziele wird bereits seit den 1990er Jahren immer wieder in der Landeshauptstadt und auch durch die vormaligen Landesregierungen diskutiert. Schon bei dem aktuellen Bebauungsplan von 1999 wurde als Planungsziel die bauliche und stadtgestalterische Komplettierung des Regierungsviertels und des „Grünen Kranzes“ um die Düsseldorfer Altstadt entsprechend eines städtebaulichen Ideenwettbewerbs von 1995 verfolgt. Konkret sieht dieser Bebauungsplan neben dem aktuellen Baukörper Baurecht für weitere Ministerien in einem runden Hochhaus und einem Atriumgebäude vor. Die Art der Nutzung wird als Fläche für den Gemeinbedarf,

Dienstgebäude und
Lieferanschrift:
Jägerhofstr. 6
40479 Düsseldorf
Telefon (0211) 4972-0
Telefax (0211) 4972-1217
Fehler! Unbekannter Name für Dokument-Eigenschaft.

Öffentliche Verkehrsmittel:
U74 bis U79
Haltestelle
Heinrich Heine Allee

Verwaltungsgebäude der Landesregierung Nordrhein-Westfalen festgesetzt.

Die Realisierung eines Regierungsviertels in Landtagsnähe ist immer wieder vielfältig thematisiert worden. In Folge der jahrzehntelangen Diskussionen hat am 26. Februar 2019 die vorherige Landesregierung Leitentscheidungen hinsichtlich zentraler Unterbringungsfragen in Düsseldorf getroffen und in diesem Zusammenhang auch einen Beschluss zur Nachnutzung der Landesliegenschaft „Haroldstraße 5" gefasst. Demnach sollten zunächst auf dieser Liegenschaft künftig das Ministerium der Finanzen und die NRW.BANK untergebracht werden. Ferner wurde das Ziel formuliert, das Grundstück für Zwecke der Landesregierung optimal auszunutzen. Nach Durchführung eines städtebaulichen Wettbewerbs in 2020 und eines hochbaulichen Realisierungswettbewerbes in 2021, hat die vorherige Landesregierung am 15. Februar 2022 einen weiteren Kabinettbeschluss zum Neubauprojekt Verwaltungszentrum „Haroldstraße 5" gefasst. Demnach sollen in dem neu zu errichtenden Verwaltungszentrum für die Landesregierung Nordrhein-Westfalen künftig das Ministerium der Finanzen und weitere Ministerien, die in den angemieteten Liegenschaften „Stadttor 1" und „Emilie-Preyer-Platz 1" untergebracht sind, einziehen. Der Neubau Verwaltungszentrum H5 für die Landesregierung ist daher aktuell geplant als Ersatz für drei Liegenschaften von Ministerien sowie zusätzlich auch als Ersatz für das Parkhaus Moselstraße. Das primäre Ziel ist die Errichtung eines modernen, flexibel nutzbaren Verwaltungsgebäudes für die Landesregierung, welches sich zur Unterbringung mehrerer Ministerien eignet.

Mit Vorlage 18/598 vom 14. Dezember 2022 wurde der Haushalts- und Finanzausschuss und der Hauptausschuss über das Neubauvorhaben Haroldstraße 5 in Düsseldorf (Projekt Neubau H5) informiert. Der dieser Vorlage beigefügten Anlage können zusätzliche Informationen zum bisherigen Planungsprozess und der geplanten Projektumsetzung entnommen werden.

Das Neubauprojekt Verwaltungszentrum H5 befindet sich aktuell in Leistungsphase 3 (LPH 3, Entwurfsplanung) nach der Honorarordnung für Architekten und Ingenieure (HOAI). Nach dem Terminplan ist ein Baubeginn in 2025 und ein Bezug des Neubaus in 2029 vorgesehen. Für die Umsetzung dieses Terminplans ist es erforderlich eine Verpflichtungsermächtigung (VE) für die perspektivisch nach Fertigstellung benötigte Gesamtmiete H5 im Haushalt 2024 zu veranschlagen, damit in 2024 gegenüber dem Bauherrn BLB NRW eine Refinanzierungszusage für die Bauausführung erteilt werden kann.

Auf Basis der Ende LPH 2 (Vorplanung) nach der HOAI ermittelten Investitionskosten hat der BLB NRW Ende März 2023 ein unverbindliches Mietangebot für das Gesamtprojekt vorgelegt, wonach sich eine Jahreskaltmiete i.H.v. ca. 50 Mio. Euro für das gesamte Gebäude inklusive aller Stellplätze in 2029 ergibt.

Dieser Mietkalkulation liegen folgende Gesamtkosten zugrunde:

Kosten	**Stand LPH 2**	**Risikozuschlag**	**Gesamt**
Herstellung Neubau Landesregierung	598,6 Mio. Euro	190,5 Mio. Euro	789,1 Mio. Euro
Abriss Bestand[1]	18,5 Mio. Euro	5,5 Mio. Euro	24 Mio. Euro
Standortentwicklung[1]	19 Mio. Euro	6,1 Mio. Euro	25,1 Mio. Euro
			838,2 Mio. Euro

[1] ohne Anteil NRW.BANK

Aufwandsanteile der Gesamtmaßnahme, die anteilig für das künftige Teilgrundstück der NRW.BANK anfallen (z.B. Kosten aus dem Bebauungsplanverfahren, Abrisskosten) werden hier nicht berücksichtigt, da diese dem BLB NRW von der NRW.BANK gesondert erstattet werden. Die neuen Gebäude der NRW.BANK und der Landesregierung sollen jeweils separat und von den Bauherren NRW.BANK und BLB NRW eigenständig geplant und errichtet werden.

Das kalkulatorische Risiko entspricht in etwa 30 Prozent der kalkulierten Herstellungskosten und wird nach den einschlägigen Vorschriften grundsätzlich in einer Kalkulation zu einer so frühen Planungsphase berücksichtigt und ist daher in den oben aufgeführten Kosten enthalten. Das kalkulatorische Risiko setzt sich aus Planungs- und Bauausführungsrisiken zusammen. Die unverbindliche Miete wird wie üblich im weiteren Projektverlauf konkretisiert. Auf Grundlage einer abgeschlossenen Planung der LPH 5/6 (Ausführungsplanung, Vorbereitung der Vergabe) nach der HOAI wird der BLB NRW ein verbindliches Mietangebot mit einer bis dahin weiter konkretisierten Jahresmiete unterbreiten. Bis zu diesem Zeitpunkt werden die eingetretenen Planungsrisiken bereits in der verbindlichen Miete weitestgehend berücksichtigt und der prozentuelle Zuschlag für das kalkulatorische Risiko insgesamt reduziert sein.

Unter der Position Standortentwicklung werden alle Kosten zur Umsetzung des Bebauungsplanverfahrens und der hier von der Landeshauptstadt Düsseldorf geforderten Umfeldmaßnahmen wie zum Beispiel die

Herstellung der grünen Haroldbucht, Rückbau der Haroldstraße, die Errichtung einer neuen Planstraße sowie der Ausbau von Fahrradwegen zusammengefasst.

Im Neubau Verwaltungszentrum H5 werden insgesamt ca. 70.000 m² Mietfläche inkl. der Flächen für 700 PKW-Stellplätze und 300 Fahrradstellplätze realisiert. Das gesamte Bauvolumen liegt bei ca. 87.000 m² Bruttogrundfläche (BGF).

Vor dem Hintergrund der mit Kabinettbeschluss vom 15. Februar 2022 festgelegten Federführung des Ministers für Finanzen bei der Umsetzung dieses Projektes und der erst perspektivisch vorzunehmenden Festlegung der weiteren Nutzer vom Verwaltungszentrum H5 wurde die benötigte Gesamt-VE i.H.v. 870 Mio. Euro zunächst im Einzelplan 20 veranschlagt. Grundlage für die Berechnung der VE ist die vom BLB NRW mit dem unverbindlichen Mietangebot kalkulierte Jahreskaltmiete i.H.v. ca. 50 Mio. Euro und einer Mietvertragslaufzeit von 25 Jahren (insgesamt 1,25 Mrd. Euro) abzüglich der bereits im Haushalt aktuell veranschlagten Mieten i.H.v. insgesamt ca. 380 Mio. Euro.

Die der Mietkalkulation zugrundeliegende Kostenschätzung erfüllt nach Angaben des BLB NRW die Anforderungen an eine Kostenschätzung nach Abschluss der LPH 2. Die Aufteilung der Kosten für den Rückbau, die Standortentwicklung und den Neubau erfolgte im Sinne einer transparenten Darstellung. Die prognostizierten Kosten von 3.405 Euro/m² BGF netto für die Kostengruppen 300 (Baukonstruktionen) und 400 (Technische Anlagen) wurden vom BLB NRW mit Vergleichsprojekten ins Verhältnis gesetzt und liegen auf dem Niveau vergleichbarer Neubauprojekte. Bei einem entsprechenden Kostenvergleich sind zudem die baufachlichen und lagebedingten Sondertatbestände des Neubaus Verwaltungszentrum H5 zu berücksichtigen, insbesondere der Aspekt der Nachhaltigkeit und die besondere städtebauliche Situation. Insgesamt konnte aus den durchgeführten Vergleichen abgeleitet werden, dass sich die prognostizierten Herstellungskosten in einem realistischen, angemessenen und marktüblichen Rahmen bewegen.

Berechnet man die vom BLB NRW kalkulierte Jahreskaltmiete auf den Quadratmeter Mietfläche, ergibt sich aktuell ein perspektivischer Mietzins für das Jahr 2029 von 58,84 Euro/m². Bei der Mietkalkulation wurde der Baupreisindex des 3. Quartals 2022 (15 %) berücksichtigt und gemäß den zentralen Vorgaben des BLB NRW in der Kalkulation bis zur Mitte der Bauzeit indexiert (2023: 6 %, 2024: 4,8 %; 2025 ff: 3,5 %). Bei einem Vergleich mit aktuellen Marktmieten sind folgende Aspekte zu berücksichtigen:

- Die Mietkalkulation des BLB NRW bezieht sich auf einen angemessenen Neubau mit voraussichtlichem Bezug im Jahr 2029. Für einen Vergleich muss eine Prognose hinsichtlich mietrelevanter Preissteigerungen bis 2029 bei den Markmieten berücksichtigt werden. Auf Basis der Preissteigerungsprognosen der Bundesbank kann eine kumulierte Erhöhung von 31,1 Prozent bis zum Jahr 2028 angenommen werden.[1]

- Der BLB NRW berechnet Vollkostenmieten. Konkret ist bei der vorliegenden Mietkalkulation eine Refinanzierung der gesamten Herstellungskosten über 40 Jahre vorgesehen, da von einer Drittverwendungsfähigkeit ausgegangen werden kann. Über den ersten Mietvertrag mit der Laufzeit von 25 Jahren werden 75 Prozent der Kosten refinanziert und die verbleibenden 25 Prozent über den folgenden Mietvertrag mit einer maximalen Laufzeit von 15 Jahren. Nach Aussage des BLB NRW kann nach heutigen Erkenntnissen der Anschlussmietvertrag zu einer geringeren Miete führen – sofern keine größeren baulichen Änderungen und zusätzliche Bedarfe nutzerseitig angemeldet werden – da zu diesem Zeitpunkt die Herstellungskosten für das Gebäude bereits zu 75 Prozent refinanziert wurden.

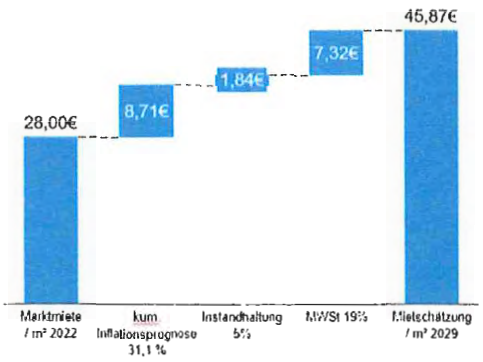
- Das Mietangebot des BLB NRW umfasst eine Komplettmiete für das gesamte Gebäude mit Stellplätzen, Grundstück sowie zusätzlich den Instandsetzungsaufwand für das Mietobjekt während der Mietdauer. Mietangebote des freien Marktes unterstellen hierfür zumeist eine Kostenbeteiligung des Mieters in Höhe von ca. 3 bis 6 Prozent der jeweils gültigen Jahresmiete. Mietangebote des freien Marktes sind zumeist Nettomieten. Die zu zahlende Miete erhöht sich daher um den jeweils gültigen Mehrwertsteuersatz bzw. um einen entsprechenden Ausgleichsbetrag des Entwicklers für Neubauprojekte. Auch ist von Zusatzmieten für Stellplätze auszugehen.

In 2022 sind in der Innenstadtlage in Düsseldorf Durchschnittsmieten i.H.v. 28 Euro/m² und in „Central Business District" (CBD) i.H.v. 34,50 Euro/m² für Büroimmobilien angefallen. Unter Berücksichtigung der zuvor genannten Aspekte hat der BLB NRW folgende Gegenüberstellung für eine Vergleichbarkeit zwischen der nach heutigem Stand für 2029 prognostizierten Marktmiete und der von ihm vorgelegten Mietkalkulation vorgenommen:

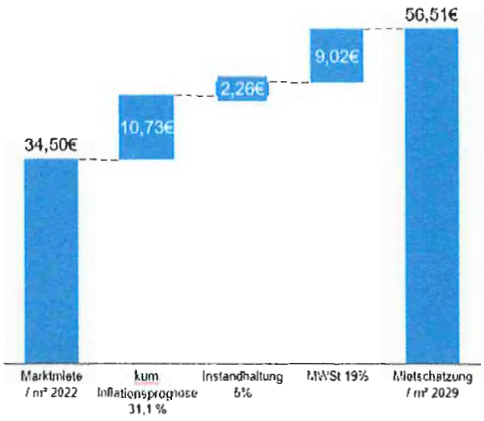
---

[1] Annahme Prognose 2025 für 2026, 2027, 2028, Quelle: Deutsche Bundesbank, Perspektiven der deutschen Wirtschaft für die Jahre 2023 bis 2025. Monatsbericht. Dez. 2022. S. 18. abrufbar unter: https://www.bundesbank.de/resource/blob/892964/bbd7cffb91f93da1255b118db7bf6da5/mL/2022-12-prognose-data.pdf

Innenstadt



CBD



Die tatsächliche Entwicklung der prognostizierten Marktmieten unter Berücksichtigung der fortschreitenden Digitalisierung kann nicht belastbar eingeschätzt werden.

Die bereits im Planungsprozess angefallenen Kosten bzw. Kosten für beauftragte Planungsleistungen sind ebenfalls zu berücksichtigen. Der Schadstoffrückbau und der Abriss der Bestandsbebauung der Liegenschaft ist bereits beauftragt und Anfang 2023 gestartet worden.

Die Umsetzung des Neubauprojektes Verwaltungszentrum H5 hat folgende weitere Auswirkungen, die nicht Gegenstand der zuvor dargestellten Kosten- und Mietberechnung sind:

- Die geplanten Bauvorhaben führen zu einer erheblichen Aufwertung des Standortes. Während sowohl das auf dem Grundstück überwiegend leerstehende ehemalige Gebäude des Ministeriums des Innern (einige Etagen werden im Rahmen einer interimistischen Unterbringung durch die Polizei genutzt) als auch das Grundstück selbst ohne städtebauliche Entwicklung keinen nennenswerten Wert darstellt – entstehen hier für das Landesvermögen nachhaltig zu nutzende Immobilien, die neben dem gesteigerten Grundstückwert auch einen deutlichen Wertzuwachs für das Landesportfolio darstellen. Das neue Planungsrecht wird eine Erhöhung der Bebaubarkeit ermöglichen und zudem eine qualitative Quartiersentwicklung sicherstellen. Nach einem Gutachten von NRW.URBAN wird der Grundstückswert des beim BLB NRW verbleibenden Grundstücksteils nach Änderung des Bebauungsplanes auf 116,6 Mio. Euro taxiert (der derzeitige Buchwert der Immobilie beträgt 12,4 Mio. Euro).

- Gemäß Kabinettbeschluss vom 26. Februar 2019 soll der aktuelle Standort des FM (BLB-Liegenschaft „Jägerhofstraße"), der unmittelbar an den Hofgarten angrenzt, nach Auszug veräußert werden. Die Aufgabe des Standorts Jägerhofstraße wird eine städtebauliche Entwicklung des Areals eröffnen, die auch im Interesse der Landeshauptstadt Düsseldorf liegt.

- Nach einer in 2019 abgeschlossenen Rahmenvereinbarung zwischen der Landeshauptstadt Düsseldorf, dem Landtag und der Landesregierung besteht Einigkeit, die Voraussetzungen für den Abriss des Parkhauses an der Moselstraße zu schaffen. Vor dem Abriss müssen die wegfallenden Stellplätze in ausreichender Anzahl an anderer Stelle realisiert werden. Die im Parkhaus Moselstraße zur Verfügung stehenden 500 Stellplätze werden aktuell von den Beschäftigten verschiedener Ministerien genutzt, da die im unmittelbaren Umfeld gelegenen Liegenschaften der Ministerien im Bestand nur über wenige Stellplätze vor Ort verfügen. Bereits zu Beginn des städtebaulichen Wettbewerbs wurde mit der Landeshauptstadt Düsseldorf vereinbart, dass im Neubau Verwaltungszentrum H5 ca. 300 Stellplätze als Ersatz für das Parkhaus Moselstraße vorgesehen werden sollen (unter Berücksichtigung einer Reduzierung i.H.v. 200 Stellplätzen mit dem Ziel, nachhaltige Mobilität zu fördern). Ohne den Neubau Verwaltungszentrum H5 gibt es nach aktuellem Stand keine Alternative für die Ersatzstellplätze und das Parkhaus Moselstraße müsste bis auf Weiteres erhalten werden.

- Mit dem Neubau Verwaltungszentrum H5 werden die Ziele der klimaneutralen Landesverwaltung (EH/EG 40, BNB Silber Zertifizierung, Flächenreduktion, Nutzung nachwachsender Rohstoffe, Regenwassernutzung, Photovoltaik, Geothermie, etc.) sowie aktuelle Sicherheitsanforderungen (Hochwasserschutz, BSI-Grundschutz, KRITIS, Netzersatzanlage, etc.) erfüllt. Damit wird der strategischen Portfolioentwicklung des Landes Rechnung getragen, zukunftsfähige Immobilien im Portfolio zu haben und weniger Zukunftsfähige aufzugeben – wie z.B. die derzeit genutzten Bestandsimmobilien. Darüber hinaus würde eine Erfüllung der Anforderungen der Klimaneutralen Landesverwaltung in den Bestandsanmietungen eine zusätzliche Finanzierung neben der Bestandsmiete erforderlich machen und wäre aus baulichen und technischen Gründen nicht vollumfänglich möglich.

Der bauliche Zustand der Liegenschaft des Ministeriums der Finanzen „Jägerhofstraße" liegt mindestens 30 Jahre hinter einem aktuellen Neubauzustand (Baujahr 1953 mit Teilsanierungen). Der BLB NRW hat bereits in 2018 mitgeteilt, dass diese Liegenschaft aus baulichen Gründen

mittelfristig nicht ohne Durchführung einer Kernsanierung weiter genutzt werden kann.

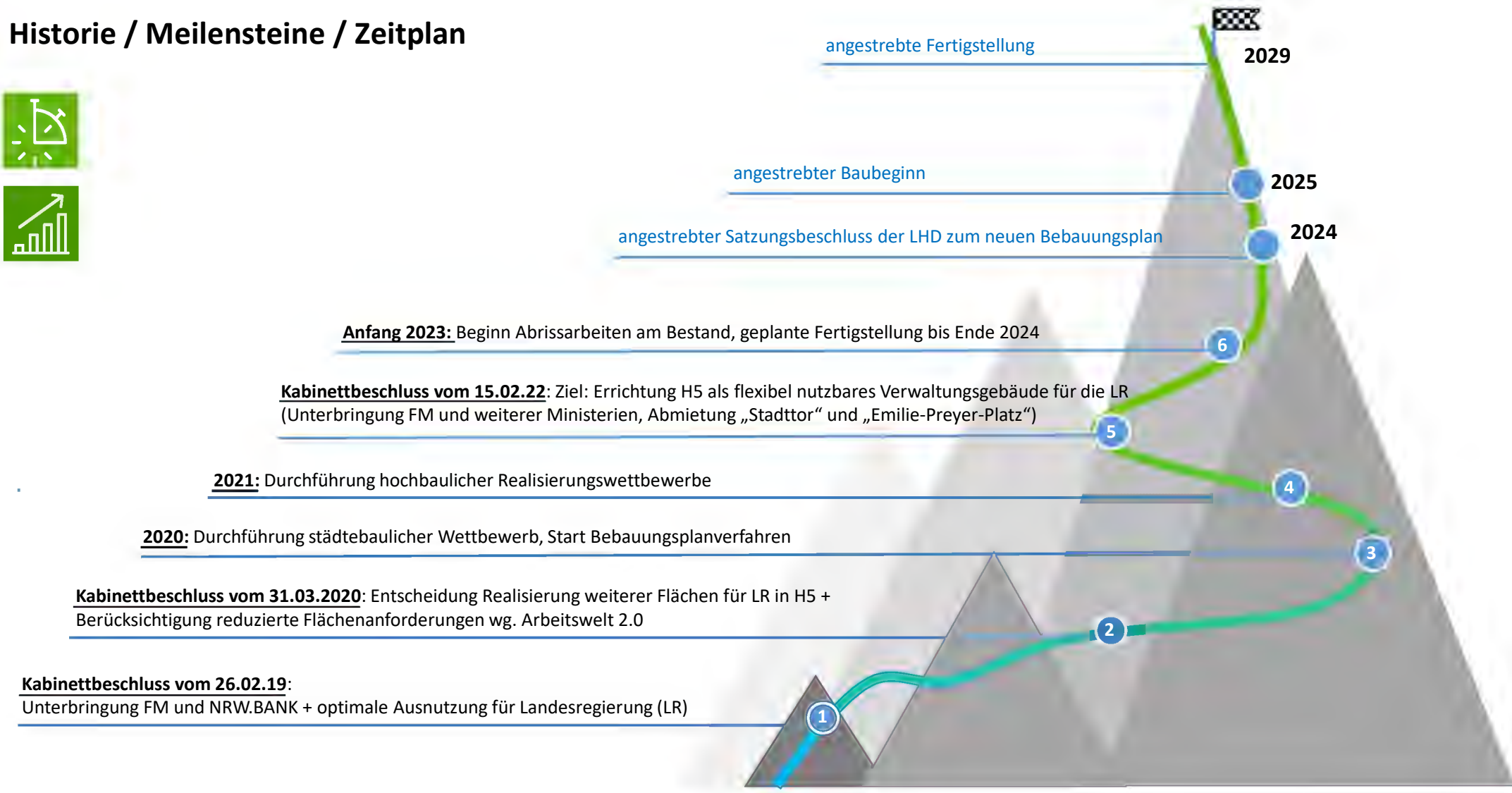
- Durch die Zielsetzung mit dem Neubau Verwaltungszentrum H5 ein modernes, flexibel nutzbares Verwaltungsgebäude für die Landesregierung zu errichten, ermöglichen die in der Planung berücksichtigte einheitliche Bürokonzeption und die zentralen Shared-Service-Flächen eine flächeneffiziente und flexible Nutzung des Gebäudes über die gesamte Lebensdauer. Die flexible Planung ermöglicht perspektivisch eine Unterbringung weiterer Beschäftigter/ Ministerien durch Anpassung der Desk-Sharing-Quote. In den nächsten Jahrzehnten werden weitere Liegenschaften der Ministerien saniert werden müssen. Der Neubau Verwaltungszentrum H5 stellt eine flexibel nutzbare Unterbringungsoption für die Landesregierung für die nächsten Jahrzehnte dar und wird mit Blick auf mögliche Flächeneinsparungen auch insgesamt eine Optimierung der Unterbringungssituation bei den Ministerien ermöglichen. Die zentrale Lage der Landesliegenschaft im Regierungsviertel bietet zudem einen Mehrwert für die gesamte Landesregierung unter anderem durch ein Konferenzzentrum und die Ermöglichung effizienten Arbeitens durch sehr kurze Entfernungen zu anderen Ministerien, Staatskanzlei und Landtag.

Dr. Marcus Optendrenk

Ministerium der Finanzen
des Landes Nordrhein-Westfalen

Zusätzliche Informationen zum Neubauprojekt Verwaltungszentrum Haroldstraße 5 in Düsseldorf

Historie / Meilensteine / Zeitplan



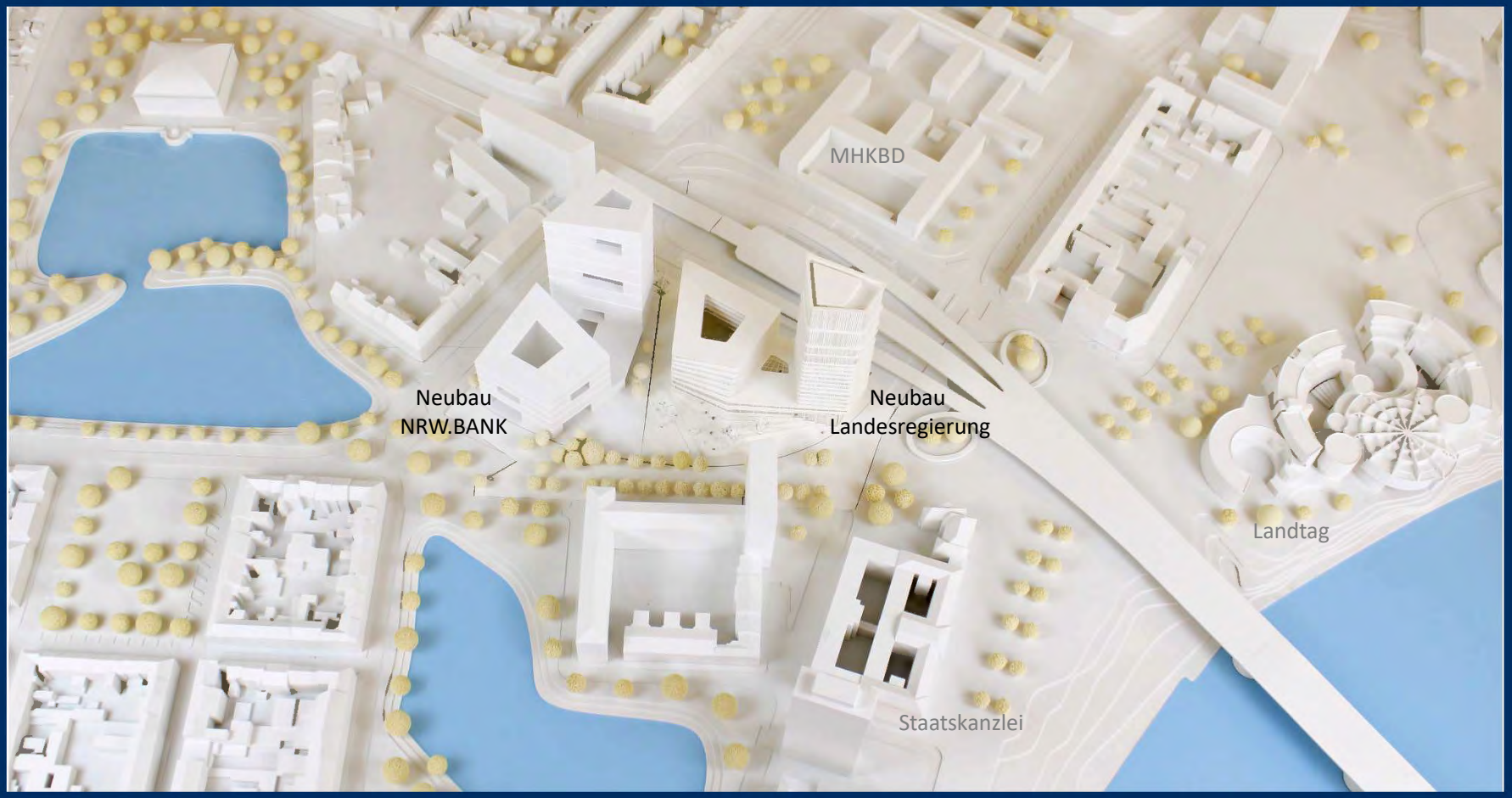
Projektziel

Neubau Verwaltungszentrum Haroldstraße 5 für die Landesregierung, aktuell geplant als Ersatz für:

- BLB Liegenschaft „Jägerhofstr.“ (FM)
- Fremdanmietung „Stadttor“ (MLV, z.T. StK)
- Fremdanmietung „Emilie-Preyer-Platz“ (MUNV)
- Parkhaus Moselstraße

Aktuelle städtebauliche Situation

Ergebnis Planungswettbewerbe



Lageplan – Grundlage neues Planungsrecht

Projektziele:

- Quartiersentwicklung
  - Rückbau Haroldstraße
  - Realisierung grüne Haroldbucht
  - Ausbau Fahrradwege
  - Bau einer neue Planstraße parallel zur Rheinufertunnelabfahrt
- Optimale Ausnutzung aus Landessicht
  - Errichtung eines zeitgemäßen, flächeneffizienten, flexibel nutzbaren Verwaltungsgebäudes
  - Umsetzung eines Regierungsviertels mit Infrastruktur für die gesamte Landesregierung

Planungsansichten Neubau Landesregierung

Ansicht vom
Spee´schen Graben,
Blickrichtung Süd-West

Ansicht von
Rheinkniebrücke,
Blickrichtung Osten