Ministerium des Innern
des Landes Nordrhein-Westfalen

Ministerium des Innern NRW, 40190 Düsseldorf

Präsidenten des Landtags
Nordrhein-Westfalen
Herrn André Kuper MdL
Platz des Landtags 1
40221 Düsseldorf

für die Mitglieder
des Innenausschusses

9. März 2022

Aktenzeichen
(bei Antwort bitte angeben)

Telefon 0211 871-
Telefax 0211 871-

Sitzung des Innenausschusses am 10.03.2022
Antrag der Fraktion der SPD vom 28.02.2022
„Abwehr von Cyberangriffen“ i.V.m.
Antrag der Fraktion Bündnis 90/Die Grünen vom 28.02.2022
„Schutz vor Cyberattacken und anderen hybriden Angriffen“

Sehr geehrter Herr Landtagspräsident,

zur Information der Mitglieder des Innenausschusses des Landtags übersende ich den schriftlichen Bericht zum TOP „Abwehr von Cyberangriffen“ i.V.m. „Schutz vor Cyberattacken und anderen hybriden Angriffen“.

Mit freundlichen Grüßen

Herbert Reul

Dienstgebäude:
Friedrichstr. 62-80
40217 Düsseldorf

Lieferanschrift:
Fürstenwall 129
40217 Düsseldorf

Telefon 0211 871-01
Telefax 0211 871-3355
poststelle@im.nrw.de
www.im.nrw

Öffentliche Verkehrsmittel:
Rheinbahnlinien 732, 736, 835,
836, U71, U72, U73, U83
Haltestelle: Kirchplatz

Ministerium des Innern
des Landes Nordrhein-Westfalen

Der Minister

Schriftlicher Bericht

des Ministers des Innern

für die Sitzung des Innenausschusses am 10.03.2022

zu dem Tagesordnungspunkt

„Abwehr von Cyberangriffen“

i.V.m.

„Schutz vor Cyberattacken und anderen hybriden Angriffen“

Antrag der Fraktion der SPD vom 28.02.2022 und
Antrag der Fraktion Bündnis 90/Die Grünen vom 28.02.2022

1. Lage und Auswirkungen

Am frühen Morgen des 24. Februars 2022 begann der militärische Angriff Russlands auf das Gebiet der Ukraine. Bereits im Vorfeld der militärischen Schläge konnten schon Cyberangriffe gegen Ziele in der Ukraine beobachtet werden. Zum einen wurden Angriffe zur Herabsetzung der Verfügbarkeit von Web-Angeboten (Distributed Denial of Service) beobachtet. Des Weiteren meldeten IT-Sicherheitsfirmen am 23. Februar 2022 Angriffe mit einer neuartigen Schadsoftware. Diese bewirkt eine unwiderrufliche Löschung aller Daten innerhalb des kompromittierten IT-Systems und zerstört dessen Funktionstüchtigkeit. Die Motivation für die Cyberangriffe wird dem Ziel der Destabilisierung der Ukraine zur Vorbereitung des geplanten Einmarsches zugeschrieben. Neben Desinformationskampagnen und gezielten militärischen Schlägen bilden Cyberangriffe einen wesentlichen Bestandteil einer hybriden Kriegsführung.

Nach Einschätzung des Verfassungsschutzes besteht auch weiterhin die Gefahr, dass Cyberangriffe in der Ukraine zu Kollateralschäden in westlichen Staaten führen. Dies gilt insbesondere in Bezug auf weltweit verbundene Firmennetzwerke mit Standorten in der Ukraine. Sofern der Aggressor seine Cyberangriffe auf westliche Staaten ausdehnt, könnte es, je nach Schwere der Angriffe, auch in Deutschland zu Auswirkungen kommen.

So könnten Cyberangriffe in der Ukraine zu einem weiter andauernden Ausfall der satellitengestützten Fernsteuerung von mindestens 3.000 Windkraftanlagen in Deutschland geführt haben, darunter auch eine nicht näher bekannte Anzahl in Nordrhein-Westfalen. Die Windräder produzieren weiterhin Strom, können jedoch nur noch vor Ort gesteuert werden.

Der Ausfall der Fernsteuerung ist eine Folge eines teilweisen Ausfalls des europäischen Satellitennetzwerks KA-SAT, der sich nahezu zeitgleich zum Beginn der Invasion am 24. Februar 2022 ereignete. KA-SAT wird von dem US-amerikanischen Anbieter Viasat betrieben, dieser soll Kommunikationsdienste auch für das Militär bereitstellen.

Im Rahmen der Desinformation dürften auch Angriffe auf Websites von Medien der Funke Mediengruppe und dem Ippen Media Netzwerk stehen, die am 26. Februar 2022 bekannt wurden. Insbesondere Websites der "Westdeutschen Allgemeinen Zeitung" (Funke Mediengruppe) sowie der "Frankfurter Rundschau" (Ippen Media Netzwerk) seien durch automatisierte Angriffe durch sogenannte "Bots" sowie durch vielfältige unsachgemäße Kommentare durch sogenannte "Trolle" gestört gewesen.

Im Übrigen besteht die Gefahr, dass die in der Ukraine aktive Hackergruppierung „GHOSTWRITER" auch in Deutschland erneut aktiv wird. Es deuten Indizien darauf hin, dass die Gruppierung eine Kampagne gegen die mit Flüchtlingsströmen aus der Ukraine befasste öffentliche Verwaltung in Europa durchführt. Mit den Angriffen verfolgte Ziele könnten sowohl Spionage als auch Desinformation sein. Die bislang bekannt gewordenen Angriffe erfolgen mittels E-Mails, die vermutlich von einem kompromittierten E-Mail-Konto einer ukrainischen Behörde verschickt werden und Bezug zu Flüchtlingen aufweisen. „GHOSTWRITER" steht seit längerem im Verdacht, Desinformationskampagnen zugunsten Russlands durchzuführen. Aktivitäten der Gruppierung wurden in Deutschland bereits im Vorfeld der Bundestagswahl 2021 festgestellt, als eine Phishing-Kampagne gegen Personen des politischen Lebens in Deutschland durchgeführt wurde.

Zu den besonders gefährdeten Stellen der IT-Infrastruktur zählen Organisationen und Einrichtungen der sogenannten „Kritischen Infrastruktur" (KRITIS). KRITIS haben eine wichtige Bedeutung für das staatliche Gemeinwesen, also z.B. Energie- oder Wasserversorger, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Der BSI-KritisV unterfallende Betreiber von KRITIS müssen aufgrund bundesrechtlicher Vorgaben IT-Sicherheit nach dem „Stand der Technik" umsetzen und deren Einhaltung regelmäßig gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nachweisen. Sofern Sicherheitsmängel aufgedeckt werden, darf das BSI deren Beseitigung anordnen. Die Betreiber müssen dem BSI erhebliche Störungen ihrer IT melden, sofern sie Auswirkungen auf die Verfügbarkeit kritischer Dienstleistungen haben können.

Neben Russland haben auch weitere ausländische Staaten seit Jahren Hackergruppierungen aufgebaut, die über exzellente technische Fähigkeiten verfügen. Cyberangriffe zum Zwecke der Spionage werden bewusst im Verborgenen durchgeführt. Anders als Cyber-Kriminelle verfolgen diese Angreifer in der Regel keine finanziellen Interessen. Bürgerinnen und Bürger als private Internetnutzer stehen in der Regel nicht im Fokus der Angreifer. Vielmehr zielen die Angriffe gegen Wirtschaftsunternehmen, politische sowie Regierungsinstitutionen. Daneben werden Cyberangriffe von ausländischen Staaten auch gegen Oppositionelle und Personen im Fokus der Öffentlichkeit durchgeführt. Als Kategorie für diese Art von Hackergruppierungen hat sich die Bezeichnung „Advanced Persistent Threat (APT)" – „Fortgeschrittene andauernde Bedrohung" etabliert.

Mit ihren Cyber-Angriffen verfolgen ausländische Staaten zumeist folgende Ziele: Zum einen soll Know-How über politische Ziele oder Zukunftstechnologien abgegriffen werden. Zum anderen nutzen ausländische Nachrichtendienste Cyberangriffe für Zwecke der Einflussnahme, Desinformation und Sabotage. Eine hohe Priorität der Angreifer besteht deshalb darin, möglichst lange unentdeckt in den Netzwerken der angegriffenen Unternehmen und Institutionen zu bleiben, um möglichst lange einen Wissensabfluss zu gewährleisten oder im besonderen Ereignisfall weitere Schäden zu bewirken.

Neben der Bedrohung durch staatlich gesteuerte Cyberangriffe hat auch die Bedrohung durch Cyberkriminalität zugenommen. Aus der Polizeilichen Kriminalstatistik (PKS) ergibt sich ein stetiger Anstieg der Anzahl erfasster Cyberstraftaten im engeren Sinne, also Angriffe auf IT-Systeme. Eine Zuordnung der Opfer zu bestimmten Gruppen bildet die PKS nicht ab. Die Sicherheitsbehörden richten ihre Tätigkeit an der verschärften Bedrohungslage durch Cyberangriffe aus.

Jahr	Erfasste Fälle	Veränderung zum Vorjahr in %	aufgeklärte Fälle	Aufklärungsquote
2018	19 693	-14,15	6 994	35,52%
2019	20 118	2,16	5 911	29,38%
2020	24 294	20,76	6 963	28,66%
2021	30 115	23,96	8 020	26,63%

2. Maßnahmen des Verfassungsschutzes

Hinsichtlich der Bedrohungslage von politischen bzw. staatlichen Institutionen, Unternehmen und KRITIS hat der nordrhein-westfälische Verfassungsschutz sowohl präventive als auch reaktive Maßnahmen ergriffen. So bietet der Wirtschaftsschutz seit jeher Vorträge zur Sensibilisierung gegen Spionage, Sabotage oder Datendiebstahl an. Sobald sich Hinweise auf konkrete Cyberangriffe ergeben, stellt die Cyberabwehr möglichen Opfern Informationen zur Erkennung des Angriffs zur Verfügung. Warnhinweise des Verfassungsschutzverbundes vor den Aktivitäten staatlich gesteuerter Hackergruppierungen, wie z.B. der Cyberangriffsgruppierung „APT 27" oder der Gruppierung „GHOSTWRITER", werden zielgerichtet an gefährdete Institutionen, Unternehmen und die öffentliche Verwaltung gesteuert, im Vorfeld der Bundestagswahl 2021 sowie aus Anlass des Krieges in der Ukraine auch an den nordrhein-westfälischen Landtag. Vor dem Hintergrund der aktuellen Konfliktlage hat der nordrhein-westfälische Verfassungsschutz im Rahmen seiner Zuständigkeit relevante Stellen im Hinblick auf die IT-Infrastruktur sensibilisiert. Alle relevanten öffentlichen Stellen des Landes stehen in einem stetigen Austausch zur Lageentwicklung.

3. Maßnahmen der Polizei

Im Rahmen der vom LKA NRW eingerichteten Informationssammelstelle „Ukraine 2022" findet ein tägliches, landesweites Monitoring von Straftaten im Zusammenhang mit dem Ukrainekonflikt statt. Ein Fallzahlenanstieg konnte bisher nicht festgestellt werden. Im Darknet wurde allerdings jüngst interne Kommunikation der pro-russischen Ransomware-Cybergruppierung „Conti" durch ein ukrainisches Mitglied geleaked. Die Daten liegen dem Bundeskriminalamt vor. Ferner werden gezielte kursorische OSINT-Recherchen im Internet zum Ukrainekonflikt durchgeführt.

In der Bekämpfung der Cyberkriminalität verfolgt die Polizei NRW präventive und repressive Ansätze, um Straftaten zu verhindern bzw. aufzuklären. Die zunehmende Professionalisierung der Täter stellt die Strafverfolgungsbehörden dabei vor besondere Herausforderungen. Sobald der Polizei NRW Straftaten bekannt werden, werden die Ermittlungen aufgenommen und zudem gefahrenabwehrende Maßnahmen eingeleitet. In herausragenden Fällen der Cyberkriminalität unterstützen Spezialistinnen und Spezialisten des LKA NRW die örtlich zuständigen Kreispolizeibehörden und können komplexe Daten und Serversysteme ohne Zeitverzug sichern, forensisch untersuchen und zur weiteren Bearbeitung in die polizeilichen Systeme übertragen.

Zusätzlich monitort das Cybercrimekompetenzzentrum des LKA NRW Seiten im Darknet, auf denen bekannte Hacker- und Ransomwaregruppierungen Daten zu Opfern veröffentlichen. Der Single Point of Contact des Cybercrimekompetenzzentrums ist rund um die Uhr für geschädigte privatwirtschaftliche Unternehmen und Behörden erreichbar. Dabei informieren und beraten das Cybercrimekompetenzzentrum des LKA NRW, aber auch die Kreispolizeibehörden, neben Bürgerinnen und Bürgern auch Unternehmen. Die Polizei NRW greift dabei in der Zusammenarbeit mit den in Nordrhein-Westfalen ansässigen Wirtschaftsunternehmen auf ein bewährtes Netzwerk unterschiedlichster Kooperationspartner zurück. Die Informations- und Wissensvermittlung umfasst neben den Möglichkeiten zum Schutz vor Angriffen auch die Sensibilisierung zur Notwendigkeit der Vorbereitung auf den „Ernstfall".

Durch die Zusammenarbeit mit Verbänden und der parallelen Pressearbeit ist eine schnelle Information der Wirtschaft gewährleistet. Gleichwohl liegt es auch in der Verantwortung der Wirtschaft, diese Informationen in eigene Sicherheitsmaßnahmen umzusetzen und dabei auch die Anzeigebereitschaft zu steigern.

4. Maßnahmen der Koordinierungsstelle Cybersicherheit

Die Koordinierungsstelle Cybersicherheit (KoSt. Cybersicherheit) im Ministerium des Innern bündelt für die Cybersicherheit relevante Informationen von Bund und Ländern, bereitet diese zielgruppengerecht auf und macht sie für die Landesverwaltung sowie die Öffentlichkeit und damit jeden Bürger nutzbar. Allgemeine Informationen und Sicherheitshinweise finden sich z.B. auf www.cybersicherheit.nrw.

Insbesondere durch die Mitarbeit in bundesweiten Gremien kann Nordrhein-Westfalen auf aktuelle Informationen zum Themenfeld der hybriden Bedrohungen zugreifen und somit die eigene Abwehrfähigkeit erhöhen. KoSt. Cybersicherheit und Verfassungsschutz Nordrhein-Westfalen arbeiten Hand in Hand und ergänzen sich hierbei.

Die KoSt. Cybersicherheit ist seit dem 14. Februar 2022 intensiv in die Kommunikationsflüsse der zuständigen Bundes- und Landesbehörden bezüglich des Ukraine-Konflikts eingebunden und sorgt für eine zielgerichtete Informationssteuerung innerhalb der Landesverwaltung. Dazu gehört insbesondere das regelmäßige Steuern von Warnmeldungen an alle Ressorts, auch zwecks Weitergabe der Informationen an Betreiber von KRITIS, soweit diese nicht bereits unmittelbar durch das BSI informiert werden. Erste Informationen über eine sich zuspitzende Cyberlage

wurden bereits am 14. Februar 2022 verteilt, ergänzt um IT-Sicherheitshinweise des nationalen IT-Lagezentrums des BSI sowie einen Maßnahmenkatalog zur Prävention von sog. „Ransomware-Attacken". Bis zum 7. März 2022 erfolgten sechs Fortschreibungen.

Als besondere Strukturen für einen zielgerichteten Austausch hat die KoSt. Cybersicherheit die „Interministerielle Arbeitsgruppe Cyber" (IMA Cyber) und den „Operativen Austausch Cybersicherheit" (OAC) initiiert, ein Forum für Vertreter von Polizei und Verfassungsschutz, der Zentralen Ansprechstelle Cybercrime der Staatsanwaltschaft Köln, des Chief Information Security Officers (NRW CISO) und des Computer Emergency Response Teams (CERT NRW).

Die Sicherheit der Netze der Landesverwaltung wird durch den für die Landesverwaltung zuständigen NRW CISO beim Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie sowie das CERT NRW zentral gewährleistet und damit verbundene Maßnahmen stetig der Bedrohungslage angepasst.

Das Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie (MWIDE) betont, dass aufgrund von vermehrter krimineller und zerstörerischer Aktivität im digitalen Raum Vorsicht und Aufmerksamkeit ganz besonders wichtig sind. Die Unternehmen sind gut beraten, ihre eigenen Cybersichersicherheitsmaßnahmen regelmäßig zu überprüfen.

Wichtige Hilfestellungen zur digitalen Selbstverteidigung können zum Beispiel auch der kostenlose Warn- und Informationsdienst von CERT BUND (https://www.cert-bund.de/wid) oder auch die Angebote des – vom MWIDE bereitgestellten – Kompetenzzentrums Digital.Sicher.NRW (https://www.digital-sicher.nrw/) geben.