Landtag
Nordrhein-Westfalen
17. Wahlperiode

Ausschussprotokoll
APr 17/641
16.05.2019

Ausschuss für Digitalisierung und Innovation

24. Sitzung (öffentlich)

16. Mai 2019

Düsseldorf – Haus des Landtags

14:00 Uhr bis 15:25 Uhr

Vorsitz: Marc Herter (SPD) (amt.)

Protokoll: Steffen Exner

Verhandlungspunkt:

Lehren aus Hackerangriff ziehen – IT-Sicherheit in NRW verbessern **3**

Antrag
der Fraktion der AfD
Drucksache 17/4803

sowie

IT-Sicherheit in NRW stärken – Freiheit sichern

Antrag
der Fraktion BÜNDNIS 90/DIE GRÜNEN
Drucksache 17/5056

– Anhörung von Sachverständigen *(s. Anlage)*

* * *

Amt. Vorsitzender Marc Herter: Ich begrüße Sie ganz herzlich zur 24. Sitzung des Ausschusses für Digitalisierung und Innovation – einer Anhörung von Sachverständigen.

Neben den Kolleginnen und Kollegen begrüße ich die Zuhörerinnen und Zuhörer, die Vertreter der Medien und natürlich in besonderer Weise die Sachverständigen, auf deren Urteil wir uns freuen.

Es wird Sie etwas wundern, dass ich hier sitze. Ich soll Sie herzlich vom Vorsitzenden, Herrn Schick, sowie vom stellvertretenden Vorsitzenden, Herrn Schneider, grüßen, die heute beide verhindert sind. Aus diesem Grunde werde ich heute die Sitzung leiten.

Die Einladung zur heutigen Sitzung ist Ihnen mit der Einladung E 17/744 zugegangen.

Lehren aus Hackerangriff ziehen – IT-Sicherheit in NRW verbessern

Antrag
der Fraktion der AfD
Drucksache 17/4803

sowie

IT-Sicherheit in NRW stärken – Freiheit sichern

Antrag
der Fraktion BÜNDNIS 90/DIE GRÜNEN
Drucksache 17/5056

– Anhörung von Sachverständigen *(s. Anlage)*

(Der Antrag der Fraktion der AfD – Drucksache 17/4803 – wurde am 24. Januar 2019 zur Federführung an den Ausschuss für Digitalisierung und Innovation und zur Mitberatung an den Innenausschuss sowie an den Ausschuss für Heimat, Kommunales, Bauen und Wohnen überwiesen.

Der Antrag der Fraktion Bündnis 90/Die Grünen – Drucksache 17/5056 – wurde am 22. Februar 2019 zur Federführung an den Ausschuss für Digitalisierung und Innovation und zur Mitberatung an den Innenausschuss, an den Wissenschaftsausschuss, an den Ausschuss für Schule und Bildung sowie an den Ausschuss für Wirtschaft, Energie und Landesplanung überwiesen.

Alle mitberatenden Ausschüsse beteiligen sich nachrichtlich an der Sachverständigenanhörung.)

Hinweisen möchte ich eingangs auf die vorab eingegangenen Stellungnahmen der Sachverständigen, für die ich mich herzlich bedanke. Überstücke der Stellungnahmen liegen im Eingangsbereich aus.

Zum weiteren Ablauf möchte ich noch einige Hinweise geben. Ein mündliches Statement der Sachverständigen zu Beginn der Anhörung ist nicht vorgesehen. Vielmehr

werden die Abgeordneten in Kenntnis der eingereichten Stellungnahmen direkt Fragen an die Sachverständigen richten.

Ich schlage vor, dass wir die Fragen der Fraktionen zunächst in einer ersten Runde sammeln, an der sich alle Fraktionen beteiligen können. Ich bitte die Abgeordneten, diejenigen Sachverständigen, an die Sie Ihre Fragen richten möchten, konkret zu benennen.

Rainer Matheisen (FDP): Liebe Herren Sachverständige, herzlichen Dank seitens der FDP-Fraktion für Ihre schriftlichen Stellungnahmen. Herzlichen Dank auch dafür, dass Sie heute hierhingekommen sind, um uns weitere Fragen zu beantworten.

Zunächst hätte ich eine Frage an das BSI. Könnten Sie erläutern, inwiefern Hersteller heute schon zu einer datenschutzfreundlichen Technikgestaltung verpflichtet sind und welche Verbesserungen durch weitere Vorgaben zu erreichen wären?

Dann habe ich eine Frage an Herrn Schuldzinski von der Verbraucherzentrale. Als Maßnahmen schlagen Sie zum Beispiel eine Herstellerpflicht zur datenschutzfreundlichen Technikgestaltung, eine Haftung für Sicherheitslücken sowie einen elektronischen Beipackzettel vor. Könnten Sie diese Maßnahmen näher erläutern?

Christina Kampmann (SPD): Herzlich willkommen und vielen Dank an die Sachverständigen für Ihre Gutachten. Ich habe keine Frage an das BSI, möchte aber sagen, dass ich es sehr positiv finde und mir nicht in der Größenordnung bekannt war, dass es schon so viele Kooperationen auf so vielen unterschiedlichen Ebenen in Nordrhein-Westfalen gibt.

Wir haben seitens der SPD zum einen eine Frage an Herrn Professor Dr. Meier von der Universität Bonn. Sie sagen, dass Sie Teil eines Forschungsprojekts mit dem Namen „Effektive Information nach digitalem Identitätsdiebstahl“ sind. Sie fordern die Politik auf, ein Warnsystem im Bereich des Identitätsdiebstahls einzurichten, was wir erst einmal als sehr interessanten Vorschlag ansehen. Es wäre schön, wenn Sie darlegen könnten, wie ein solches Warnsystem konkret aussehen könnte.

Dann habe ich noch zwei Fragen an Herrn Schuldzinski von der Verbraucherzentrale. Sie sagen zum einen, dass im Moment in 21 von 61 Beratungsstellen Beratungen zum Datenschutz stattfinden. Wäre es aus Ihrer Sicht wünschenswert, eine flächendeckende Beratung einzuführen? Was bräuchten Sie dafür von der politischen Seite?

Meine zweite Frage schließe ich an das an, was auch Rainer Matheisen schon gefragt hat. Sie sagen ganz deutlich, dass die aktuelle Rechtslage den derzeitigen Herausforderungen nicht gerecht wird – insbesondere in Bezug auf die Haftungslücken bei fehlenden Sicherheitsupdates. Wie könnte eine Regulierung aus ihrer Sicht konkret ausgestaltet werden?

Sven Werner Tritschler (AfD): Vielen Dank auch von unserer Seite für die Stellungnahmen. Die erste Frage richtet sich an Herrn Dr. Schabhüser von der Verbraucher-

zentrale sowie an Herrn Vieweg und Herrn Fischer von IT.NRW. Sie hatten zu unserem Vorschlag, weitere Ministerien und Landesbehörden nach ISO zu zertifizieren, geschrieben, dass die Ausweitung der bestehenden Zertifizierung nicht sinnvoll sei. Wir haben uns damals vielleicht missverständlich ausgedrückt. Die Frage war eher, ob man eine separate Zertifizierung anderer Landesbehörden und Ministerien in Betracht ziehen sollte, wie es zum Beispiel in Sachsen gemacht wird.

Daran anschließend: Mittlerweile bietet das BSI auch ein etwas niedrigschwelligeres Angebot an. Die Zertifizierung nennt sich „Testat nach der Basis-Absicherung“. Wäre das eventuell ein Modell für Ministerien und Landesbehörden und vielleicht auch für die Kommunen in NRW?

Die nächste Frage richtet sich an Herrn Schuldzinski und an Herrn Dr. Schabhüser. Sie haben in der Stellungnahme das Phishing-Radar hervorgehoben. Wir finden, das ist ein sehr spannendes Angebot. Mit wie vielen Mitarbeitern müssen Sie dabei auskommen? Wie hoch ist das Arbeitsaufkommen? Können Sie die Anzahl der Meldungen – das ist ja recht imposant: 200 bis 300 täglich – mit der Ausstattung, die Sie haben, bewältigen?

Matthi Bolte-Richter (GRÜNE): Auch seitens der Grünen-Fraktion ganz herzlichen Dank an die Sachverständigen, dass Sie uns schriftlich und mündlich mit Ihrem Sachverstand bereichern.

Ich würde gerne beim BSI bzw. Herrn Dr. Schabhüser beginnen. Sie schreiben in Ihrer Stellungnahme, dass Sie als BSI einerseits mit der Sicherheit der Regierungs- und Verwaltungsnetze befasst sind, andererseits als relativ neue Aufgabe aber auch Beratungsleistungen anbieten – für Verbraucherinnen und Verbraucher, für KMU usw. Wie sind diese beiden unterschiedlichen Komplexe hinsichtlich ihrer Ressourcen – personell und finanziell – ausgestattet?

Die zweite Frage ist: Was sind Ihrer Meinung nach die größten Hemmnisse, um Unternehmen mit Beratungs- oder Unterstützungsleistungen – egal, welcher Art – zu erreichen? In Ihrer Stellungnahme wird richtigerweise der IT-Grundschutz als Erfolgsmodell angesprochen. Das ist er sicherlich auch, aber wir wollen es natürlich auch noch in die Breite bringen. Was können wir da tun?

An IT.NRW bzw. Herrn Fischer möchte ich auch zwei Fragen richten. Sie haben in Ihrer Stellungnahme festgestellt, dass der Auftrag von IT.NRW sich nicht primär auf den privaten Bereich fokussiert. Der Auftrag des BSI ist ja gerade um diesen Bereich erweitert worden – also auch um die Förderung von Beratungsleistungen gegenüber Privaten. Wäre das auch eine mögliche Aufgabe für IT.NRW? Es gibt da ja viele mögliche Überlegungen, dass man die Unabhängigkeit, die man als Landesstelle hat, auch nutzen könnte – zum Beispiel für Maßnahmen zur Produktempfehlung etc.

Außerdem haben Sie noch einen inhaltlichen Punkt angesprochen, der auch für den privaten Bereich sinnvoll ist, nämlich die Sicherheit und Qualität kommerzieller Software. Welche Handlungserfordernisse sehen Sie in dieser Hinsicht?

An Herrn Schuldzinski von der Verbraucherzentrale: Sie nehmen auch das Thema „Produkthaftung“ in den Blick. Auch wir gehen darauf in unserem Antrag ein, und wir

begrüßen das Anliegen, dass es eine solche Haftung geben sollte. Wir sehen da Regulierungsbedarf. Gibt es dazu gute Beispiel aus anderen Staaten, an denen wir uns als Bundesrepublik Deutschland oder als Land Nordrhein-Westfalen orientieren könnten?

Herr Professor Dr. Meier, Sie schreiben, es bedürfe zur Verbesserung des Wissenstransfers weniger einer Verbesserung des Weiterbildungsangebots als der Schaffung von Anreizen für KMU, Mitarbeiter trotz Fachkräftemangel für die Teilnahme an IT-Sicherheitsweiterbildungen freizustellen. Das ist eine konkrete und aus meiner Sicht sehr interessante Maßnahme, die Sie vorschlagen. Welche weiteren Maßnahmen würden Sie uns empfehlen?

Herr Professor Dr. Holz und Herr Professor Dr. Meier, in der Debatte im Landtag haben wir das Thema „Offenhalten von Sicherheitslücken“ besprochen. Wir haben es auch in den Antrag aufgenommen. Ein Stichwort ist dabei – aktuell gerade hier in Nordrhein-Westfalen – die Quellen-TKÜ. Von einigen Rednerinnen und Rednern der Koalition sowie der Landesregierung wurde in Zweifel gezogen, dass die Einführung der Quellen-TKÜ und das damit verbundene Offenhalten von Sicherheitslücken ein Risiko für die IT-Sicherheit in Nordrhein-Westfalen sei.

Wir sind da anderer Meinung. Wir glauben sehr wohl, dass es zu einem Risiko für die IT-Sicherheit führen könnte. Wie ist Ihre Position aus Sicht der Wissenschaft dazu?

Florian Braun (CDU): Auch ich möchte meinen Dank an die Sachverständigen aussprechen, dass Sie sich heute Zeit nehmen, um uns an Ihrer Expertise teilhaben zu lassen. Ich möchte mich nicht an der politischen Einschätzung meines Vorredners beteiligen, sondern mich auf das Fragen fokussieren.

Herr Professor Dr. Holz, Sie forschen im Bereich IT-Sicherheit. Um es etwas größer zu fragen: Wie würden Sie zurzeit die IT-Sicherheitslage in Nordrhein-Westfalen beschreiben und analysieren? Welche Rolle kann und muss dabei KI spielen?

An IT.NRW gerichtet: Sie haben zum einen mit dem White-Box-Test ein Modell zur Erkennung von Sicherheitslücken benannt. Könnten Sie das noch einmal ausführen? Zum anderen haben Sie die Kooperation sowohl mit dem Bund als auch mit den Bundesländern als durchaus positiv beschrieben. Vielleicht könnten Sie im Detail erläutern, wie dort die operative Zusammenarbeit läuft bzw. wie oft und wie eng man sich austauscht.

Amt. Vorsitzender Marc Herter: Wir steigen damit in die erste Antwortrunde ein. – Herr Schuldzinski hat das Wort.

Wolfgang Schuldzinski (Verbraucherzentrale NRW): Vielen Dank für die Einladung und für die Fragen. Ich versuche, alles einigermaßen zu sortieren, wobei Teile auch von anderen mit beantwortet werden können.

Ich beginne mit der Frage von Herrn Matheisen nach dem Beipackzettel. Im Prinzip ist das eine Idee des BSI, insofern kann Herr Dr. Schabhüser gleich vielleicht noch etwas

ergänzen. Im Grunde geht es darum, dass Produkthersteller ihre Produkte auf freiwilliger Basis mit einem QR-Code versehen. Begonnen werden soll mit den Routern, weil diese bekanntlich eines der großen Einfallstore im privaten Bereich sind. Aus den QR-Codes kann man dann ablesen, welche Sicherheitsfeatures die Produkte haben. Theoretisch kann man diese Idee auf Handys und andere Geräte erweitern.

Für den Interessierten bietet das eine weitere Informationsquelle; insofern ist es zu begrüßen. Für denjenigen, der sich nicht interessiert, bietet es natürlich keine zusätzliche Information. Das liegt ja auf der Hand.

Wir haben Forderungen, die sich „Privacy by Design“ nennen. Das bedeutet im Prinzip, dass die Hersteller von Hardware und letztlich auch von Software die Grundeinstellungen bereits so setzen müssen, dass nicht der Verbraucher sie in einen sichereren Zustand bringen muss, sondern dass sie bereits auf „sicher“ gestellt sind. Falls es erforderlich ist, kann der Verbraucher entscheiden, ob er bestimmte Features, die vielleicht etwas weniger sicher sind, einschaltet oder freiwillig wählt.

Dazu gehört aber auch so etwas wie bestimmte Passwörter nicht vergeben zu dürfen. „1234“ funktioniert dann einfach nicht als Passwort. Mittlerweile muss man sich auf fast jeder Internetseite einloggen, und Sie alle wissen, dass es Vorrichtungen gibt, die so etwas ausschließen. In anderen Fällen ist es aber völlig egal, was man als Passwort wählt. Natürlich sind auch das immer Einfallstore, und das könnte man gesetzlich regeln.

Das Nächste ist die Frage der Haftung. Letztlich handelt es sich um eine zivilrechtliche Diskussion. Das BGB stammt aus dem Jahr 1900, und nun gibt es diese Entwicklungen. Ich würde als Jurist immer sagen, dass man viele dieser Entwicklungen durchaus auch mit dem BGB fassen kann, man muss aber schauen, wo genau die Anwendung gelingt.

Bei sozusagen zusammengesetzten Produkten wie einem Kühlschrank, der auch „smart“ ist, ist die Frage, wie weit die Haftung reicht. Wenn der Kühlschrank kaputt ist, ist klar, was passiert, aber wenn zum Beispiel nur ein Sicherheitsfeature bei der Vernetzung des Kühlschranks mit dem Heimrouter nicht funktioniert, hat das aktuell keinerlei zivilrechtliche Konsequenzen. Man kann weder das Gerät zurückgeben noch leiten sich daraus Haftungsfolgen ab. In der heutigen Zeit ist das meines Erachtens nicht mehr angemessen.

Das Problem für den Hersteller ist natürlich häufig, dass er Produkte zukauft und gar nicht alles selbst herstellt. Er muss dann schauen, wie er alles sicherstellen kann. Das ist aber ein anderes Problem der Haftung. In der einen oder anderen Konstellation gibt es Haftungen der Händler, aber nicht Haftungen der Hersteller. Auch daran kann man weiterarbeiten.

Eine andere Frage bezog sich darauf, dass wir in unserer Stellungnahme geschildert haben, dass wir sehr viel im Bereich der Information tun, konkrete Beratung und Unterstützung aber nur in 21 unserer 61 Beratungsstellen anbieten können. Das ist natürlich dem Umstand geschuldet, dass wir im Moment aufgrund der finanziellen Möglichkeiten mehr nicht umsetzen können. Das alles zieht immer Schulungen, Backoffice

und Unterstützungen nach sich. Mehr ist da einfach im Moment nicht drin. Sinnvoll wäre natürlich, wenn man es flächendeckender machen könnte.

Das Phishing-Radar ist etwas, was sehr stark nachgefragt wird. Wir erhalten in der Tat rund 300 Meldungen von Verbraucherinnen und Verbrauchern pro Tag. Die leiten uns dann einfach ihre Phishing-Mail weiter. Ich schäme mich fast zu sagen: Das macht bei uns letztlich eine studentische Hilfskraft, die es händisch in Listen einträgt. Natürlich ist das nicht mehr State of the Art.

Wir haben sehr gute Kooperationen – auch mit einigen der Anwesenden; unter anderem mit dem BSI. Das BSI hat zum Beispiel Interesse daran, dass wir die Daten in einer bestimmten Art und Weise aufbereiten, damit man sie besser auswerten kann. Das ist für uns eigentlich fast nicht möglich. Im Moment ist es nur ein Sammeln.

Wir warnen dann davor – wir haben eine starke Nachfrage von Verbrauchern, die uns abonniert haben –, welche Phishing-Meldungen es aktuell gibt. Aber viel mehr können wir damit aktuell nicht machen. Man könnte aber sehr viel mehr machen. Man könnte die Warnungen auswerten oder Folgen ableiten. Man könnte spannende Sachen machen, und das BSI hätte daran auch ein großes Interesse.

Prof. Dr. Michael Meier (Rheinische Friedrich-Wilhelms-Universität Bonn; Institut für Informatik): Vielen Dank auch von meiner Seite für die Einladung. – Ich beginne mit der Frage der Frau Abgeordneten Kampmann zu dem Projekt „EIDI – Effektive Information nach digitalem Identitätsdiebstahl“. Ich führe kurz aus, worum es dabei geht.

Es handelt sich um ein Projekt, bei dem es um genau solche Phänomene geht, wie sie uns über den Jahreswechsel sehr plakativ vorgeführt worden sind. Das heißt: Zugangsdaten von Bürgerinnen und Bürgern zu Onlinediensten gehen abhanden. Das sind in der Regel E-Mail-Adressen, die als Nutzerkennung bei einem Onlinedienst genutzt werden, sowie das Passwort oder Informationen über das Passwort.

Ziel dieses Projekts ist es, dieses Phänomen aufzugreifen, festzustellen, dass bei einem Bürger derartige Informationen abhandengekommen sind, und ihn dann zu warnen – also auf ihn zuzugehen und nicht darauf zu warten, dass er sich selbst kümmert; denn er bemerkt erst einmal gar nicht, dass da irgendetwas schiefgelaufen ist.

Tatsächlich bestätigen die Vorfälle über den Jahreswechsel, dass dieser Ansatz aus unserer Sicht richtig ist. Denn viele der dort verwendeten und über die Weihnachtszeit veröffentlichten Informationen waren bereits relativ lange Zeit vorher öffentlich im Internet zugreifbar. Hätte man also als eine Instanz, die einen solchen Warndienst betreibt, bereits kritische Informationen zur Kenntnis bekommen, wäre man auf die Betroffenen zugegangen, und es wäre wahrscheinlich schon längst auf die Phänomene reagiert worden, bevor im Dezember Effekte bzw. Auswirkungen hätten eintreten können.

Das Projekt an sich ist relativ interdisziplinär aufgestellt, weil es viele Aspekte berührt. Es sind auch Wahrnehmungspsychologen beteiligt; denn Warnungen müssen ja von Menschen verarbeitet werden, und es muss entsprechend reagiert werden. Es waren

also auch Handlungsoptionen enthalten. In dem Teilprojekt geht es insbesondere darum, wie man das macht; wen man also wie anspricht, sodass er tatsächlich adäquat reagiert.

Das wirft eine ganze Reihe juristischer bzw. datenschutzrechtlicher Fragen auf. Es sind personenbezogene Daten, die wir da verarbeiten. Der Betroffene hat natürlich nicht eingewilligt, dass wir das tun, sondern er ist letztlich ja Opfer einer Straftat geworden, sodass diese Informationen angefallen sind. Es geht auch darum, in welchen Rahmenbedingungen das passieren kann. Das sind Betrachtungen, die von datenschutzrechtlichen bzw. juristischen Experten geleistet werden.

Wir als Uni Bonn und ganz konkret meine Arbeitsgruppe leisten den sicherheitstechnischen Beitrag zu diesem Projekt. Wir überlegen uns also, wie wir konkret vorgehen können. Das betrifft insbesondere den Bereich, wie wir eigentlich herausfinden können, dass irgendwo im Internet oder an anderen Stellen auf dieser Welt solche Datenbestände auftauchen – also typischerweise über kriminelle Aktivitäten abgeflossene Daten. Zum Teil stammen die Daten aber auch aus Polizeimaßnahmen, wenn die Polizei beispielsweise eine Botnetz-Infrastruktur beschlagnahmt und im Zuge dessen solche Datenbestände findet. Das können Millionen E-Mail-Adressen und Passwörter sein. Die Frage ist dann, was damit gemacht wird. Gäbe es einen solchen Warndienst, wäre diese Frage leicht beantwortet. Zu überlegen, wie man es schafft, frühzeitig an solche abgeflossenen Informationen zu kommen, wie man sie verarbeitet, wie man eine Warnung realisieren kann und welche Kanäle dafür infrage kommen sind Aspekte, denen sich meine Arbeitsgruppe widmet.

Als Partner arbeiten wir mit XING, dem Betreiber eines sozialen Netzwerks zusammen. XING fungiert als Stellvertreter für Betreiber solcher Diensteplattformen. Auch der Aspekt, wie man diese Betreiber mit ins Boot holen kann und welche Teilaufgaben sie in diesem Szenario zu übernehmen bereit sind, spielt also eine Rolle. Auch die Verbraucherzentrale ist hinsichtlich dieses Aspekts involviert, und wir haben als assoziierten Partner auch das BSI mit an Bord.

Wie kann der Warndienst aussehen? – Man kann sich verschiedene Warnkanäle vorstellen. Man könnte zum Beispiel sagen, wir schicken einfach eine E-Mail an die betroffene Adresse – wobei wahrscheinlich offensichtlich ist, dass das ein ungeeigneter Weg ist, wenn man sich das eigene E-Mail-Verhalten vor Augen führt. Schickt die Uni Bonn – oder wer auch immer Betreiber eines solchen Systems sein könnte; dazu sage ich später noch etwas – eine E-Mail, der betroffene Bürger kennt diesen Betreiber aber nicht, stellt sich die Frage, wie man mit Warn-E-Mails von unbekannter Quelle umgeht. Es ist klar, dass das nicht der richtige Weg ist.

Man könnte sich auch vorstellen, ganz andere Kanäle zu wählen. Was sich aktuell abzeichnet – das Projekt läuft noch; wir haben im Januar 2017 begonnen und sind noch bis Ende dieses Jahres, eventuell bis Mitte des nächsten Jahres dabei –: Wir wollen die Anbieter der Onlinedienste mit ins Boot holen. Die Identität, die abgeflossen ist, gehört ja zu einem Onlinedienst. Da wäre natürlich dann die Frage, ob man nicht gesetzgeberisch erweiternde Pflichten an diese Dienstebetreiber definieren müsste, dass sie an einem solchen Warnsystem mitwirken müssen. Wenn wir also feststellen, dass ein Dienst betroffen ist und welche Identitäten dies betrifft, dann gehen wir auf

den Dienst zu und sagen: Weil er eine Geschäftsbeziehung zu dem betroffenen Kunden pflegt – diese hat der Betreiber des Warndienstes wahrscheinlich nicht –, soll er eine Warnung an den Kunden aussprechen. Das hat unserer Einschätzung nach eine adäquate Wirkung.

Wer kann ein solches System betreiben? – Man könnte sagen, jemand könnte doch eine Firma gründen und damit reich werden. Das wird aber nicht funktionieren, weil unsere juristischen und datenschutzrechtlichen Partner da intervenieren. Tatsächlich ist so etwas für Unternehmen zunächst einmal eigentlich nur zulässig, wenn es um eigene Kunden oder um die eigene Infrastruktur geht. Aber dazu, einen solchen Dienst für ganz Deutschland oder für die ganze Welt zu betreiben, bestehen große Bedenken bzw. die Kollegen aus der juristischen Fakultät sagen uns, dass es so nicht geht. Also muss im Prinzip ein öffentliches Mandat her. Da kann man sich vorstellen, es beim Verbraucherschutz anzudocken. Man kann es auch bei den Datenschutzbehörden andocken, man kann es aber auch beim BSI andocken. Auch da gibt es verschiedene Überlegungen, und es laufen Gespräche, um es abzuklären.

Ich möchte noch etwas zur Größenordnung sagen, da ich nicht weiß, ob sie Ihnen bekannt ist. Wir sammeln im Rahmen des Projekts seit Anfang 2017 gestohlene Identitäten. Wir haben 8 Milliarden Datensätze, also 8 Milliarden E-Mail-Adressen plus Passwortinformationen dazu. Sie können sich vorstellen, wie wir auf diese 1.000 betroffenen öffentlichen Persönlichkeiten im Dezember geschaut haben. Das ist sicherlich nur die Spitze des Eisbergs.

Ich komme dann zur Frage von Herrn Bolte-Richter zum Wissenstransfer. Der Vorschlag im Antrag war, das Angebot zu erweitern. Tatsächlich ist es so, dass ich neben meiner Rolle an der Uni Bonn auch noch eine Rolle beim Fraunhofer-Institut FKIE einnehme. Wir sind an einem gemeinsamen Weiterbildungsprogramm beteiligt, bei dem verschiedene Fraunhofer-Institute gemeinsam mit Fachhochschulen Weiterbildung anbieten. Meine persönliche Erfahrung – sie ist nicht systematisch und methodisch fundiert erhoben – aus dem Bereich ist, dass es eigentlich nicht daran liegt, dass das Weiterbildungsangebot nicht groß genug ist. Aber aus irgendeinem Grund werden die angebotenen Dinge von denjenigen, die sich weiterbilden sollten, einfach nicht genutzt.

Wenn ich nach Erklärungsgründen dafür suche oder auch Gespräche dazu führe, ist es so, dass es meiner Wahrnehmung nach auch nicht am Preis dieser Maßnahmen liegt. Natürlich muss man eine Weiterbildung auch bezahlen, aber wahrscheinlich fehlt die Zeit. Das korreliert meiner Meinung nach mit dem aktuell vorherrschenden Effekt des Fachkräftemangels. Es ist aus Sicht der Unternehmen sicherlich auch nachvollziehbar, dass man sich die Frage stellt, ob man bei vollen Auftragsbüchern Mitarbeiter für eine Woche zu einer Schulung schicken soll. Das ist meine persönliche Überlegung zu dem Thema, die mich auch zu meiner Aussage in meiner schriftlichen Stellungnahme veranlasst hat.

Herr Bolte-Richter, Sie fragen nun nach zusätzlichen Maßnahmen, wie man diesen Wissenstransfer verbessern kann. Dazu habe ich vielleicht einen paar lose Ideen. Mei-

ner Ansicht nach ist es wichtig, dass jedem Bürger und insbesondere jedem Unternehmer auf dieser Welt eine gewisse digitale Überlebenskompetenz vermittelt werden muss. Das kann im Rahmen der Berufsausbildung oder des Studiums geschehen.

Die Schwierigkeit ist, dass alles, was Digitales betrifft, eine ganz kurze Lebenszeit hat. Sie alle kennen es aus dem persönlichen Bereich: Alle fünf Jahre funktionieren die Dinge ganz anders, die Sicherheit hat sich weiterentwickelt, aber auch die Vorgehensweisen der Angreifer haben sich weiterentwickelt. Das heißt, das Wissen veraltet sehr schnell. Dagegen muss man kontinuierlich – ich sage mal: alle fünf Jahre – nachbessern und sozusagen ein Update in die Köpfe einspielen.

Dazu, wie man das schafft, habe ich keine echte Lösung parat, aber ich habe so etwas wie eine Version. Vielleicht halten Sie sie für naiv, aber ich möchte sie trotzdem mit Ihnen teilen.

Der Gesetzgeber verpflichtet alle Unternehmen, sich gegen Cyberrisiken zu versichern, und die Versicherer regeln es dann schon über die Prämie. Die Versicherer prüfen dann, ob die Unternehmen Maßnahmen zur Reduzierung des Risikos ergreifen, indem sie zum Beispiel ihre Mitarbeiter schulen. Wenn Sie dies tun, erhalten sie einen Prämiennachlass. Wenn sie es nicht tun, werden sie entsprechend umfangreich zur Kasse gebeten, um diese verpflichtende Versicherung aufrechtzuerhalten. Das ist ein Modell, in welche Richtung es gehen kann. Ob das perfekt ist, kann ich nicht sagen, aber es ist eine Idee, die ich zu diesem Thema beitragen kann.

Herr Bolte-Richte, Sie hatten dann noch eine Frage zum Offenhalten von Sicherheitslücken gestellt. Meine Position dazu ist, dass dieses Offenhalten von Sicherheitslücken ein Risiko für die gesamte Gesellschaft, für ganz NRW darstellt – um es kurz zu beantworten. Tatsächlich halte ich es auch für relativ unverantwortlich, dies zu tun.

Dr. Gerhard Schabhüser (Bundesamt für Sicherheit in der Informationstechnik): Die erste an mich adressierte Frage lautete, ob Hersteller derzeit verpflichtet sind, datenschutzfreundliche Technik herzustellen. Da bin ich nicht ganz der richtige Ansprechpartner. Ich weiß, dass man als Nutzer durch die Datenschutzgrundverordnung verpflichtet ist, datenschutzfreundliche Technik einzusetzen. Ob in der Datenschutzgrundverordnung ein entsprechender Passus enthalten ist – vorher war das nicht der Fall –, weiß ich nicht. Vielleicht kann Herr Schuldzinski dazu noch etwas ausführen.

Was ich aber ausführen kann, ist, dass es keine Verpflichtung gibt, so etwas wie Security by Design umzusetzen. Wie Herr Schuldzinski beschrieben hat, gibt es dort kaum Haftungsregeln. Genauer gesagt: Sie werden derzeit nicht so umgesetzt, weil die Rechtsauslegung eher fragwürdig ist.

Da sehe ich durchaus ein Problem, welches im Rahmen des IT-Sicherheitsgesetzes 2.0, welches derzeit in der Bundesregierung in Ressortabstimmung ist, aber schon öffentlich geworden ist, behandelt wird. Dort geht es darum, insbesondere für den Bereich der kritischen Infrastrukturen nicht nur den Betreiber von Anlagen in die Pflicht zu nehmen, sondern auch Anforderungen in der Zuliefererkette zu platzieren, sodass kritische Komponenten ein gewisses Sicherheitsniveau aufweisen müssen. Das ist neu, und ich bin der Meinung, da besteht Handlungsbedarf.

Weil es dazu passt, würde ich hier gerne Ausführungen zum Beipackzettel ergänzen. Es ist in der Koalitionsvereinbarung verankert, dass es so etwas wie ein IT-Sicherheitskennzeichen geben soll. „IT-Gütesiegel“ stand, glaube ich, darin, „IT-Sicherheitskennzeichen“ ist meiner Meinung nach der bessere Begriff.

Was soll damit erreicht werden? – Ein wesentliches Element ist das Erreichen von Transparenz der Sicherheitseigenschaften als Informationsquelle, um bei der Kaufentscheidung mit gewürdigt zu werden. Wenn man heute in einen großen Produktladen für IT-Konsumenten geht, dann erfährt man über ein Produkt wie ein Smartphone, eine Überwachungskamera für das eigene Haus, eine Schließanlage oder eine elektronisch gesteuerte Steckdose ganz viele technische Daten. Beim Smartphone erfährt man, wie viele Megapixel die Front- und die Rückkamera haben, was man als normaler Nutzer schon gar nicht mehr unterscheiden kann. Man erfährt, wie viele Kerne die CPU hat, wobei die meisten wahrscheinlich gar nicht wissen, was eine CPU darüber hinaus alles leistet, usw. Man erfährt alle möglichen Dinge, die für die Kaufentscheidung wichtig sind, aber über die Sicherheitseinstellungen und -eigenschaften des Produkts erfährt man nichts.

Da möchten wir Transparenz erzeugen im Sinne eines IT-Sicherheitskennzeichens. Man muss das in den Rahmen des europäischen Cybersecurity Acts einbetten, in dem ein europäisches Cybersecurity Certification Framework aufgesetzt wird, das genau den Aspekt vorantreiben soll, dass wir nicht nur im Hochsicherheitsbereich Zertifizierungen von Produkten und Dienstleistungen haben, sondern dass es mit geringerer Prüftiefe, aber hinreichender Aussagekraft auch auf Consumer-Bereiche ausgedehnt werden soll.

Um das IT-Sicherheitskennzeichen aufbringen zu können, braucht es eine Rechtsgrundlage. Die gibt es derzeit nicht. Aber ein solches Kennzeichen basiert natürlich auf Kriterien. Die Kriterien kann man jetzt schon erstellen, und auch die notwendigen Prüfmechanismen kann man schon heute erstellen. Wir haben das als BSI im Vorgriff und im Nachgang zum Telekom-Router-Vorfall, bei dem vor zweieinhalb Jahren 900.000 Telekomkunden zwischenzeitlich vom Netz getrennt waren, getan. Das war kein Angriff auf die Router im Sinne der Verfügbarkeit, sondern ein Kollateralschaden: Die Router sollten eigentlich in ein Botnetz übernommen werden. Wir haben also eigentlich Glück gehabt, dass der Angreifer den falschen Code hochgeladen hatte und die Router einfach nur ausgefallen sind.

Dennoch war das ein Vorfall auf den wir reagiert haben. Die Heimrouter sind sozusagen der Schutzwall für die vielen kleinen Helferlein, die man im Hause über WLAN und Ähnliches anbringt. Wir haben deshalb eine Technische Richtlinie für Breitband-Router erstellt, in der wir ein paar Grundprinzipien aufgestellt haben – nicht zu viele –, die ein solches Produkt leisten soll. Zweitens erstellen wir parallel eine Prüfmethodik, in der beschrieben wird, wie man dies auch im Herstellungsprozess abprüfen will. Schlussendlich: Wenn beide zusammen sind, kann man mit einer Herstellererklärung antreten und sagen, dass man die Prinzipien erfüllt und die Prüfmethodik angewandt hat. Momentan kann man das auch ohne Prüfmethodik behaupten, aber dann kann man schlecht rationalisieren, warum es wirklich so sein sollte. Dafür ist die Prüfmethodik angesetzt.

Wir glauben, dass man mit der Kennzeichnung eben diesen angesprochenen Beipackzettel hat, sodass man im Geschäft beispielsweise über einen QR-Code zugreifen kann, um sich die Sicherheitseigenschaften anzusehen. Dann kann man entscheiden, ob man das Gerät mit seinen Sicherheitseigenschaften kaufen möchte oder ob man ein anderes Gerät kaufen möchte. Es wird also zunächst einmal der mündige Bürger adressiert, diese Informationen in seine Kaufentscheidung einzubeziehen.

Wenn das nicht greifen sollte – obwohl ich hoffe, dass es funktioniert –, kann man in Zukunft natürlich durch eine solche Kennzeichnung und die Kriterienerfüllung auch regulierend eingreifen. Bei elektronischen Geräten darf man zum Beispiel in Europa kein Gerät vermarkten bzw. in den Markt bringen, welches die Anforderungen hinsichtlich der elektromagnetischen Verträglichkeit nicht erfüllt. Ich erinnere zum Beispiel an das Knistern im Radio, wenn der Föhn an ist. Das ist die elektromagnetische Einstrahlung. Davon sollten Geräte nicht beeinflusst werden, und es ist verpflichtend, dass sie hinreichend robust sind. Da könnte man nachziehen, aber ich denke, es wird sukzessive durch eine Fortentwicklung der IT-Sicherheitsarchitektur und der IT-Sicheheits-Frameworks ausgestaltet werden.

Ich bin mir nicht sicher, ob sich die Frage danach, wofür man eine Zertifizierung des Grundschutzes brauchen würde, sich an mich oder an IT.NRW richtete. Ganz kurz: Für Profirechenzentren und Ähnliches ist die Zertifizierung nach IT-Grundschutz – also nach der ISO-27000-Reihe – meiner Meinung nach das richtige Mittel der Wahl. Wir haben den Grundschutz modernisiert und mit einem „Testat nach der Basis-Absicherung“ versehen, um für kleine Unternehmen den Einstieg ganz einfach zu machen. Wir haben das Ganze durch eine Profilierung unterstützt, sodass man für ausgewählte Zielgruppen den Grundschutz so profilieren kann, dass man nicht das volle Programm fahren muss, sondern genau das, was zielgruppenspezifisch zu tun ist.

Dafür haben wir zum Beispiel ein Profil für Kommunen aufgesetzt. Wir haben auch etwas für Handwerker und Handwerkskammern aufgesetzt – sogar mit Handreichungen von drei DIN-A5-Seiten. Dabei ist es wirklich einfach, den Einstieg zu gewähren, für größere Abhängigkeiten sollten wir aber in Richtung eines zertifizierten Grundschutzes gehen. Ansonsten kommen wir nicht zu einem angemessenen Schutzniveau.

Zu der Frage, was das BSI im Vergleich zum Schutz der Regierungsnetze und Ähnlichem im Kontext des Verbraucherschutzes tut: Hier muss man etwas differenzieren. Das BSI hat schon seit gefühlt 10 bis 15 Jahren „BSI für Bürger“ im Angebot – eine Webseite, auf der wir eine Menge Informationen zur Verfügung stellen. Ob diese Informationen immer zielgruppengerechte schön gemacht sind? – Da kann man sicherlich immer besser werden, es stehen aber eine Menge Informationen zur Verfügung.

Wir haben den Dienst „Bürger-CERT“, den man abonnieren kann, um nahezu tagesaktuell wichtige Schwachstelleninformationen und Handlungsempfehlungen direkt per Push-Nachricht nach Hause zu erhalten. Wir haben als unterstützende Kanäle den Facebook-Kanal, um andere Zielgruppen zu erreichen, und seit Kurzem haben wir auch einen YouTube-Kanal eröffnet, weil wir der Meinung sind, dass eine Visualisierung der Dinge besser ist, als alles nur aufzuschreiben und lesen zu müssen.

Das ist aber erst ein kleinerer Teil. Im Koalitionsvertrag wird dem BSI ja die Rolle „digitaler Verbraucherschutz“ zugewiesen. Da würden wir ein solches IT-Sicherheitskennzeichen mit einbauen, es stehen aber auch andere Aspekte im Vordergrund wie das Schaffen von Awareness, der Ausbau von Vernetzungen und digitaler Kompetenz sowie das Adressieren von Dialogen, bei denen wir sehr stark mit den Verbraucherschützern zusammenarbeiten. Wir haben das Konzept mit dem BMJV schon abgestimmt – mit dem BMI ohnehin.

Hinsichtlich der personellen Ressourcen – ohne den Ausbau mit dem IT-Sicherheitskennzeichen usw. – kann ich sehr schlecht eine genaue Aussage treffen, weil wir so etwas wie eine integrierte Wertschöpfungskette haben. Selbst die Leute aus dem Hochschutzbereich, wo wir intensivere Schwachstelleninformationen und Ähnliches erhalten, filtern aus ihrer Arbeit das heraus, was bürgerrelevant ist und schieben es dann in Richtung Bürger-CERT. Das wird dann eben mit einem Push-Verfahren gemacht.

Wenn ich nur die Organisationstrukturen zusammenzähle, die explizit für den Bürger und für KMU auftreten, dann komme ich auf ca. 40 Personen, die für diesen Bereich arbeiten. Wenn ich die mittelbare Zuarbeit berücksichtige, dann sind, würde ich sagen, etwa 80 % des BSI mitbeteiligt – natürlich nicht in Vollzeit. Momentan arbeiten bei uns etwa 900 Personen; viele von ihnen wenden Teile ihrer Arbeitszeit in dem Bereich rund um Bürger und KMU auf, andere im Bereich der Regierungsnetze, kritischer Infrastrukturen usw.

Zu den Hemmnissen, um kleine und mittlere Unternehmen zu erreichen, habe ich vorhin zum Grundschutz teilweise schon etwas ausgeführt. Ich meine, die Werkzeuge stehen zur Verfügung. Einfache Mechanismen, die eine Grundabsicherung bieten, bis hin zu hohen bis sehr hohen Reifegraden stehen auch in der Profilierung zur Verfügung.

Wir haben auch noch eine Menge an Kommunikation zu leisten. Erstens ist noch nicht überall angekommen, dass diese Mechanismen zur Verfügung stehen. Und zweitens – da möchte ich zwischen Land und Kommunen sowie zwischen kleinen, mittleren und großen Unternehmen fast nicht unterscheiden – haben wir erst bei 60 bis 70 % der betroffenen Organisationen den Effekt, dass Informations- und Cybersicherheit Chefsache sein müssen. Das ist noch nicht überall angekommen. Dort, wo es angekommen ist, haben wir typischerweise ganz schnell sehr viel höhere Reifegrade, als wenn es noch heißt: Das macht die IT-Abteilung; das sind ja sowieso so komische Nerds, die im Zweifelsfall auf die Frage, was man tun soll, antworten, man solle ausschalten und wieder anschalten.

Das Thema „Informations- und Cybersicherheit“ als Erfolgsfaktor für das zu erledigende Geschäft durchsetzen zu wollen, ist noch nicht überall angekommen. Es wird uns bei der Digitalisierung auf die Füße fallen, wenn wir das nicht ganz schnell hinbekommen.

Prof. Dr. Thorsten Holz (Ruhr Universität Bochum; Institut für Elektrotechnik und Informationstechnik): Vielen Dank für die Einladung in den Ausschuss. Leider habe

ich es im Vorfeld nicht geschafft, eine schriftliche Stellungnahme einzureichen. Ich hoffe, dass ich die Fragen durch meine Ausführungen beantworten kann.

Ich möchte mit der Frage von Herrn Braun zur IT-Sicherheitslage beginnen. Dazu zunächst ein historischer Rückblick. Windows 95 wurde vor etwa 25 Jahren veröffentlicht; das erste iPhone vor 10 Jahren. Hinsichtlich der Sicherheit liegen zwischen diesen Produkten und dem aktuellen Windows 10 bzw. der aktuellen iPhone-Generation Welten.

In den letzten Jahren haben wir sowohl in der Forschung als auch in der Industrie sehr viele Schutzmechanismen entwickelt, und es wird sehr viel schwieriger, Sicherheitslücken auszunutzen. Wir verstehen mittlerweile relativ gut, wie man Sicherheitslücken findet und wie man diese effektiv verhindert. Wir haben mittlerweile auch einige generische Schutzmechanismen entwickelt, die auch nicht zu viel Leistungsverlust verursachen. Insofern ist das Grundniveau der IT-Sicherheit deutlich höher geworden.

Das sieht man auch an einigen Beispielen. Früher war es so, dass sogar Einzelpersonen relativ einfach gewisse Lücken finden konnten. Heute sind es häufig Teams aus mehreren Personen, die über Monate und teilweise noch längere Zeiträume hinweg Lücken erst einmal finden und dann einen sogenannten Exploit, also ein komplettes Tool-Kit entwickeln, mit dem man die Lücke verlässlich ausnutzen kann. Das erfordert sehr hohen Entwicklungsaufwand. Auf dem Markt sind Exploits dann für fünf-, sechs- und teilweise auch siebenstellige Beträge käuflich. Dass die Kosten für solche Exploits deutlich angestiegen sind, ist sicherlich ein guter Indikator dafür, dass das generelle Sicherheitsniveau sich in den letzten Jahren deutlich verbessert hat.

Dazu muss allerdings auch die Einschränkung gemacht werden, dass wir noch immer sehr weit davon entfernt sind, komplett sichere und vor allem beweisbar sichere Systeme zu entwickeln. Das zeigen all die Vorfälle aus der Praxis – Herr Dr. Schabhüser hat den Vorfall mit den Routern der Deutschen Telekom genannt. Falls Sie gestern die Nachrichten verfolgt haben: Da waren Lücken in den neuen Intel-Prozessoren ein großes Thema. Vor ein paar Tagen wurde bekannt, dass eine israelische Firma in der Lage ist, iPhones zu übernehmen, ohne dass man es mitbekommt, indem aus der Entfernung das Telefon angerufen wird. Es kann dann eine Schadsoftware auf dem Telefon installiert und dann das Telefon überwacht werden. Im Antrag der Grünen wird auch auf WannaCry eingegangen, wobei – aus Sicht der Angreifer – sehr eindrucksvoll demonstriert wurde, dass man es auch heute noch schafft, viele Hunderttausend Systeme zu kompromittieren. Durch diese immer noch sehr häufig auftretenden Sicherheitsvorfälle sehen wir, dass wir noch sehr weit davon entfernt sind, komplett sichere Systeme zu entwickeln.

In Bezug auf NRW muss man gar nicht so weit gehen wie zu WannaCry oder ähnlichen Vorfällen. Sie haben vermutlich auch die Vorfälle mit Ransomware im Lukaskrankenhaus in Neuss vor einiger Zeit mitbekommen. Es war noch etwa ein Dutzend weiterer Krankenhäuser in NRW betroffen. Auch hier gibt es also häufig Vorfälle.

In letzter Zeit haben wir uns Angriffe auf Bayer angesehen. Vermutlich haben Sie es auch in der Presse gelesen, und auch die ARD hat darüber berichtet, dass es chinesischen Angreifern über einen Zeitraum von mehreren Monaten hinweg gelungen ist,

knapp 20 Maschinen von Bayer zu übernehmen. Ähnliche Angriffe auf thyssenkrupp – vermutlich von derselben chinesischen Gruppe – wurden vor zwei Jahren bekannt.

Es gibt also einen deutlich höheren Grundschutz dank der vielen Maßnahmen, die entwickelt wurden, aber wir sind immer noch weit davon entfernt, wirklich absolute Sicherheit zu garantieren.

Ein Aspekt, der auch in der Frage genannt wurde, war der Zusammenhang zwischen IT-Sicherheit und künstlicher Intelligenz bzw. maschinellem Lernen. Dort besteht sehr viel Potenzial. Wir sehen gerade in den letzten Monaten und Jahren, dass gerade im Bereich des maschinellen Lernens sehr schnell Fortschritte gemacht werden. Heutzutage ist bei der Bildklassifizierung ein Algorithmus dem Menschen überlegen. Er kann viel schneller beispielsweise auf einem Briefumschlag die Zieladresse erkennen. Er kann Objekte erkennen, und er kann Personen in einem Videostream identifizieren – und das alles ermüdungsfrei und 24 Stunden am Tag. In eigentlich allen Spielen – angefangen bei Schach über Go bis hin zu Echtzeitstrategiespielen – sind uns die Maschinen mittlerweile überlegen, und Algorithmen übersetzen mittlerweile automatisch von einer Sprache in eine beliebige Zielsprache. Auch all die digitalen Assistenten wie Alexa usw. zeigen sehr eindrucksvoll, welche Fortschritte die künstliche Intelligenz in den letzten Jahren gemacht hat.

Gleichzeitig gibt es eine sehr starke Synergie zwischen der IT-Sicherheit und dem maschinellen Lernen. Einerseits betrifft dies die Robustheit von maschinellen Lernsystemen. Meine Forschungsgruppe und auch diverse andere Forschungsgruppen auf der Welt haben gezeigt, wie einfach maschinelle Lernsysteme heutzutage ausgetrickst werden können. Das typische Beispiel ist der Bereich der Bilderkennung. Ein autonom fahrendes Auto muss Straßenschilder erkennen, und diverse Forschungsgruppen haben gezeigt, dass eine einfache Manipulation des Schildes – typischerweise reicht ein Aufkleber auf dem Schild – ausreicht, dass das Auto plötzlich ein Stoppschild als Tempo-100-Schild identifiziert. Das kann natürlich katastrophale Auswirkungen haben.

Ähnliches haben wir bei Spracherkennungssystemen auf Basis von Alexa gezeigt. Wir haben demonstriert, dass man ein Audiosignal erzeugen kann, welches wir als Menschen als Satz A verstehen, die Maschine versteht es allerdings als Satz B. Wir konnten also gewissermaßen etwas vergleichbar mit einer optischen Illusion erzeugen. Wir hören immer noch den Satz, den wir hören sollen, wir können die Maschine aber so austricksen, dass sie einen beliebigen Zielsatz erkennt, was entsprechend für Manipulationen genutzt werden kann. Wie man maschinelle Lernsysteme robust machen kann, ist also noch eine sehr offene Forschungsfrage.

Gleichzeitig gibt es aber auch eine Synergie in eine andere Richtung. Wir können maschinelle Lernsysteme benutzen, um diverse Probleme aus dem Bereich der IT-Sicherheit zu lösen. Wenn man beispielsweise sehr große Datenmengen hat – zum Beispiel Informationen über den Netzwerkverkehr oder Videoaufnahmen – kann man in diesen Datenmengen nach Anomalien suchen und so zum Beispiel neue Angriffe identifizieren oder auch viel schneller und effizienter identifizieren, dass etwas falsch läuft. Es gibt dort also sicherlich diverse Querschnittsthemen, bei denen KI – gerade KI.NRW als KI-Strategie der Landesregierung – und die Strategie zur Förderung der IT-Sicherheit in NRW zusammengebracht werden können.

Eine weitere Frage betraf den Kontext der Sicherheitslücken. Das ist sicherlich eine sehr spannende Frage. Ich möchte etwas weiter ausholen als Herr Professor Dr. Meier und auch hier auf das Beispiel WannaCry verweisen. Es dokumentiert sehr eindrücklich, welche Auswirkungen so etwas haben kann.

Die Sicherheitslücke hinter WannaCry ist von der NSA entwickelt worden. Sie können es sich so vorstellen, dass die NSA diverse Programme hat, um gezielt Sicherheitslücken zu suchen, die dann zur Aufklärung genutzt werden. Vor einiger Zeit war eine andere Angreifergruppe, bei der ein bisschen unklar ist, um wen es sich handelte, in der Lage, solche Exploits von der NSA zu stehlen. Diese Exploits wurden dann veröffentlicht. Auf einmal war also bekannt, welche Art von Angriffstools die NSA teilweise benutzt. Eines dieser Tools wurde im Kontext von WannaCry benutzt, um Angriffe durchzuführen.

Vermutlich hat also eine staatliche Stelle einen Exploit entwickelt, dieser Exploit wurde gestohlen und veröffentlicht, und im Endeffekt hat das dazu geführt, dass sehr viele Unternehmen und Privatbürger erfolgreich angegriffen werden konnten. Das demonstriert, dass diese von Herrn Professor Dr. Meier angesprochene Problematik nicht nur ein theoretisches Problem ist, sondern in der Praxis tatsächlich auftreten kann. Wir können also nicht garantieren, dass die staatlichen Stellen, die über Sicherheitslücken verfügen, diese auch wirklich für sich behalten und sie nicht irgendwie verloren gehen. Und da die Hersteller nicht über die Lücken Bescheid wissen, können sie sie auch nicht schließen und den Schutz der Firmen und Privatbürger garantieren.

Gleichzeitig hat diese Frage allerdings noch die andere Seite, dass wir natürlich auch staatliche Stellen haben – typischerweise Geheimdienste, die den gesetzlichen Auftrag verfolgen, gewisse Aufklärung zu betreiben –, für welche Sicherheitslücken häufig ein essenzieller Bestandteil sind, um in diversen Situationen Informationen überhaupt sammeln zu können. Wir haben hier also auf jeden Fall das Spannungsspiel, dass auf der einen Seite natürlich ein staatliches Interesse besteht, die Sicherheit der Bürger und der Firmen zu garantieren, andererseits benötigen gewisse staatliche Stellen Informationen über Sicherheitslücken, um ihren gesetzlichen Auftrag zu erfüllen.

Es handelt sich also um eine Frage mit sehr vielen Facetten, die man im Rahmen einer solchen Ausschusssitzung nicht abschließend klären kann. Ich wollte nur darauf hinweisen, dass es diese Facetten gibt. Mir persönlich ist auch gar nicht bekannt, welche staatlichen Stellen in NRW überhaupt über Sicherheitslücken verfügen. Es wäre vielleicht mal interessant, herauszufinden, wer in NRW über solche Informationen verfügt und wie diese Stellen mit den Informationen umgehen.

In diesem Feld sind uns andere Länder sicherlich voraus. In den USA hat die NSA diverse Programme, in denen gezielt Sicherheitslücken gesucht werden. Immer dann, wenn eine neue Lücke gefunden wird, wird eine Risikoabschätzung durchgeführt. Es gibt ein Gremium, welches sich jede Lücke ansieht und für jede Lücke entscheidet, wie wichtig sie für die eigene Aufklärung ist, ob man sie nutzen kann und wie wahrscheinlich es ist, dass ein anderer Geheimdienst bzw. ein anderes Land über dieselben Informationen verfügt und sie gegen US-Bürger nutzen kann. Es fließen noch diverse

andere Faktoren ein, und dann wird entschieden, ob die Lücke an die Hersteller gemeldet werden soll oder ob sie privat gehalten wird, um die Interessen der NSA voranzubringen.

Im Bereich der Quellen-TKÜ sind Sicherheitslücken natürlich ein Faktor, allerdings gibt es in der Praxis auch diverse andere Methoden, die genutzt werden können. Da geht es dann häufig darum, dass ein physischer Zugriff auf das Gerät genutzt wird, um Schadsoftware zu installieren. Ein bekanntes Beispiel dafür ist der Bundestrojaner. Das Vorgehen war vermutlich so, dass während einer Sicherheitskontrolle am Flughafen in München das elektronische Gerät des Verdächtigten eingezogen wurde, und dann wurde dort am Flughafen München von den Polizeibehörden der Bundestrojaner auf dem System installiert. Das wurde also durch einen physischen Zugriff möglich.

Zuletzt möchte ich auf die Awareness-Maßnahmen eingehen. Meine Vorredner haben bereits diverse Mechanismen beschrieben, die ich nur unterstützen kann. Ich möchte mich noch zu dem Gütesiegel äußern, welches ich etwas kritisch sehe.

Aus Forschungssicht wird der IT-Sicherheitsmarkt häufig als sogenannter Market for Lemons angesehen – also nicht im Sinne von Zitronen, sondern vergleichbar mit dem Markt für Gebrauchtwagen. Wenn ich ein gebrauchtes Auto kaufe, gibt es eine gewisse Asymmetrie: Der Händler weiß viel mehr über das Auto als ich, und ich kann als Laie gar nicht einschätzen, ob es sich um ein Auto handelt, das nur aufpoliert wurde und bei dem innerhalb der nächsten 5.000 km der Zahnriemen kaputtgeht oder andere grundlegende Probleme auftreten. Ich kann also gar nicht einschätzen, ob es sich um ein gutes Produkt handelt. Ein schmieriger Autohändler kann mich daher sehr einfach über den Tisch ziehen.

Im Bereich der IT-Sicherheit ist die Situation leider ähnlich. Dort gibt es dieselbe Asymmetrie, dass der Käufer gar nicht einschätzen kann, welche Sicherheitsfeatures ein Produkt bietet und ob es das, was es verspricht, überhaupt kann. Technisch kann der Käufer gar nicht einschätzen, ob die versprochenen Mechanismen überhaupt umgesetzt werden und wie verlässlich dies funktioniert. So ist beispielsweise in fast allen Produkten, auf denen momentan etwas von „KI“ steht, gar keine künstliche Intelligenz enthalten. Im Bereich der KI-Tools gibt es also ein ähnliches Problem wie bei der IT-Sicherheit.

Aus Forschungssicht ist das Problem vor allem, dass wir Sicherheit nicht gut messen können. Wir können keine Metriken angeben, um zwei Lösungen effektiv zu vergleichen. Es handelt sich also um ein schwieriges Thema, wenn es darum geht, wie man verlässlich bzw. vertrauenswürdig IT-Lösungen einschätzen kann.

Amt. Vorsitzender Marc Herter: Herr Fischer und Herr Vieweg, bevor wir zu Ihnen bzw. zu IT.NRW kommen, würde ich vorschlagen, dass Sie sich entscheiden, wer von Ihnen antwortet, sodass wir auch noch Zeit für eine zweite Fragerunde haben. Ich würde Sie zumindest bitten, es sich so aufzuteilen, dass zeitlich Gelegenheit bleibt, pro Fraktion noch eine Nachfrage zu stellen.

Hans-Josef Fischer (IT.NRW): Das kriegen wir hin; wir werden uns beeilen. Erlauben Sie mir zunächst dennoch, mich dafür zu bedanken, an dieser Anhörung beteiligt zu werden und auf Ihre Fragen eingehen zu können.

Zur Frage des Abgeordneten Tritschler zu Zertifizierungen: Was ist eigentlich Gegenstand einer Zertifizierung? – Es werden nicht Behörden oder Landeseinrichtungen zertifiziert, sondern Informationsverbünde. So ist auch unsere Antwort zu verstehen. Wir haben einen Zertifizierungsverbund, einen Gegenstand, und das ist bei uns das Herz unseres Rechenzentrums. Diesen Gegenstand zu erweitern, halten wir nicht für sinnvoll.

Durchaus überlegenswert ist es, andere Informationsverbünde zu zertifizieren. Ich bin mir nicht ganz sicher – ich habe es nicht überprüft –, meine aber zu wissen, dass zum Beispiel die Scanstelle bei der Bezirksregierung Detmold zertifiziert ist. Unsere Zertifizierungsstrategie ist genau darauf eingerichtet, auf unserer Betriebsplattform aufbauende Verfahren einer Zertifizierung zugänglich zu machen bzw. diesen Prozess zu erleichtern. Man kann es sich vorstellen wie bei Legoplatten: Die Grundplatte wurde bereits einmal durchleuchtet.

Herr Tritschler, Ihre zweite Frage habe ich leider nicht ganz erfasst.

(Sven Werner Tritschler [AfD]: Da muss ich selbst nachschauen!)

– Vielleicht machen wir dann erst einmal mit der Frage von Herrn Bolte-Richter weiter.

Die Zuständigkeit von IT.NRW im Zuge der Informationssicherheit ist natürlich zunächst fokussiert auf unseren Auftrag, der nach unserer Betriebssatzung definiert ist: die Informationstechnik für die Landesverwaltung bereitzustellen. Wir tun dies im Referat 24, dem Herr Vieweg angehört, heutzutage in zwei Sachgebieten: zum einen für das Haus und zum anderen für das CERT – das ist die Aufgabe, die Herr Vieweg verantwortet. Wir sind aktuell dabei, ein drittes Sachgebiet aufzubauen, in dem wir Kunden wie das Finanz-, Justiz- oder Innenministerium in den vielfältigen Aufgaben der Informationssicherheit beraten können.

Vor dem Hintergrund, dass der Arbeitsmarkt in der Informationssicherheit heiß umkämpft ist, bin ich der Meinung, dass wir schlecht beraten wären, uns strategisch zu zerfasern. Wir wollen unsere Ressourcen schonend einbringen. Ich gehe davon aus, dass der private Bereich heutzutage – so habe ich auch die Stellungnahme von Herrn Schuldzinski verstanden – von den Verbraucherzentralen beraten wird. Auch das BSI bietet seit Jahren einen Bürgerservice an. Hier würde ich nicht einen Schwerpunkt von IT.NRW sehen.

Was die Sicherheit und Qualität auch von uns genutzter privater Software angeht, ist das Dilemma meines Erachtens bereits beschrieben worden. Ich kann hier insbesondere auf die Ausführungen von Herrn Dr. Schabhüser verweisen. Wir setzen als IT.NRW in hohem Maße private Software ein. Wie wir uns und unsere Kunden schützen, wird Herr Vieweg unter dem Stichwort „White-Box-Test“ noch erläutern. Das ist aber ein reaktives Tun. Was wir brauchen, ist mehr Proaktivität. Da halte ich das Vorgehen, über IT-Sicherheitskennzeichnungen nachzudenken und die Verbraucher über

Sicherheitsfeatures zu informieren, für einen richtigen Weg. Ob er ausreichen wird oder ob wir einen TÜV brauchen, ist eine andere Frage.

Wie schützen wir also sowohl öffentliche als auch private Nutzer vor nicht hinreichend sicher produzierten Produkten? – Security by Design ist ein Programmiergrundsatz bei IT.NRW, aber leider müssen wir feststellen, dass dies nicht bei allen Lieferanten, deren Produkte wir einsetzen, auch der Fall ist.

Herr Tritschler, was war nun Ihre zweite Frage?

> (Sven Werner Tritschler [AfD]: Hat sich mit Ihrer Antwort schon erübrigt!)

– Prima, dann gebe ich weiter an Herrn Vieweg.

Jens Vieweg (IT.NRW): Das Thema „White-Box-Test“ ist relativ leicht erklärt, wenn man ein Techniker ist, aber relativ schwer zu erklären, wenn man kein Techniker ist. Ich versuche jetzt den Spagat.

Ein Hacker, wie man ihn aus Filmen kennt, der von außen ein System angreift, eine Sicherheitslücke benötigt und sich dann in dem System befindet, wäre eher ein Black-Box-Test. Ganz grob gesagt: Der Hacker kennt das System nicht, sondern er muss sich von außen Eingabefelder usw. ansehen und prüfen, ob er dort irgendetwas findet – per Zufall oder durch Ausprobieren –, was er ausnutzen kann, um in das System hineinzukommen. Das heißt bildlich: Er steht vor einem Gebäude, rüttelt an der Tür und probiert an der Tür alle möglichen Dinge, um sie zu öffnen. Das ist die Black Box – er weiß nichts. Man nennt es auch „Zero-Knowledge-Test“.

Der White-Box-Test hingegen bedeutet: Man versucht, sich auf möglichst legalem Wege möglichst viele Informationen über das Programm zu beschaffen. Idealerweise erhält man vom Hersteller der Software – in vielen Fällen ist das bei uns das eigene Haus IT.NRW – den Quellcode. Übertragen auf die Analogie von vorhin bedeutet dies: Ich besitze den Bauplan des Gebäudes und weiß dann zum Beispiel, dass die Wand rechts neben der Tür so dünn ist, dass ich mich nur dagegen lehnen muss, um hineinzukommen.

Wir untersuchen also den Quellcode von Anwendungen. Wenn wir Anwendungen von Firmen bekommen, versuchen wir im Dialog mit den Firmen an den Quellcode zu kommen. Wenn sie es richtig verstanden haben, haben die Firmen auch ein Interesse daran, uns den Quellcode zur Verfügung zu stellen; denn sie erhalten kostenlos eine sehr intensive Überprüfung und letztendlich quasi eine Anleitung vom CERT Nordrhein-Westfalen, was sie an ihren Anwendungen umbauen müssen, damit sie sicherer werden. Es gewinnen also beide Seiten.

Der White-Box-Test ist also immer derjenige, bei dem wesentlich mehr Informationen zur Verfügung stehen. Bei keinem der beiden Tests steht das Gütesiegel am Ende, dass eine Anwendung sicher ist, aber beim White-Box-Test bleibt letztlich das gute Gefühl, dass das CERT NRW sagt: Wir haben trotz intensiver Suche nichts gefunden. – Wenn bei einem Black-Box-Test jemand sagt, er habe nichts gefunden, heißt das meiner Ansicht nach gar nichts. Man kann zwei Wochen lang von außen an einem

System herumgedoktert haben, ohne etwas zu finden, das bedeutet aber wirklich gar nichts.

Zur Kooperation im Verwaltungs-CERT-Verbund: Das ist eine sehr operative Kommunikation, die damit beginnt, dass der Operator vom Dienst im CERT Nordrhein-Westfalen – wie auch diejenigen der anderen Länder – morgens in einem speziell abgesicherten Instant Messenger mit den anderen CERTs in Echtzeit kommuniziert. Wir stehen den ganzen Tag über – während der Tagesdienstzeit von 7 bis 17 Uhr – mit dem CERT-Bund und allen CERTs der Länder im operativen Austausch.

Wir haben eine gemeinsame Zusammenarbeitsplattform, in der wir viele Grundlagendokumente gemeinsam bearbeiten. Dabei geht es um Passwortrichtlinien – Wie lang muss ein Passwort sein? –, organisatorische Dokumente zur Aufstellung eines CERT, Ausarbeitungen, darum, welche Rollen besetzt werden müssen usw. All diese Dinge bearbeiten wir nicht mehr alleine, sondern gemeinsam.

Wir teilen Erkenntnisse über Schwachstellen in Software, und zwar auch im Rahmen unserer Responsible Disclosure Policy, die vor einigen Jahren schon einmal Gegenstand hier im Landtag war. Wenn wir in einem Penetrationstest eine Schwachstelle in einer Software finden und nicht ausschließen können, dass andere Bundesländer diese Software auch nutzen, informieren wir die Länder über diese Schwachstelle – ebenso wie den Hersteller. So kann in allen Bundesländern sichergestellt werden, dass zusätzliche Maßnahmen zum Schutz vor dem Ausnutzen dieser Sicherheitslücke ergriffen werden können.

Es handelt sich also um eine sehr operative Zusammenarbeit mit relativ wenig Bürokratie. Deshalb funktioniert sie sehr gut.

Amt. Vorsitzender Marc Herter: Herzlichen Dank. – Ich bitte die Fraktionen, sich bei ihren Nachfragen in der zweiten Runde auf eine Frage zu beschränken. Bitte verknüpfen Sie auch nicht mehrere Fragen durch ein „und“, sondern stellen Sie tatsächlich nur eine Frage.

Christina Kampmann (SPD): Herr Fischer, Sie haben in Ihren Ausführungen den Vorschlag eines TÜV eingebracht, ohne Zeit zu haben, den Gedanken näher auszuführen. Könnten Sie dazu noch etwas konkretere Angaben machen?

Florian Braun (CDU): Ich habe eine Nachfrage an Herrn Professor Dr. Holz. Es ist in Planung, bei Ihnen in unmittelbarer Nachbarschaft ein Max-Planck-Institut für Cyber Security einzurichten, was seitens des Landes unterstützt wurde und wird. Was versprechen Sie sich von der Zusammenarbeit mit diesem Institut? Was ist der Mehrwert für Nordrhein-Westfalen, um auch die Forschung weiter zu stärken?

Rainer Matheisen (FDP): Ich habe eine Frage an Herrn Professor Dr. Meier. Sie hatten eine Versicherungslösung ins Spiel gebracht. Da wäre die Frage, wie es sich derzeit am Markt darstellt und inwiefern Sie eine Art Kontrahierungszwang vorsehen. –

Wenn es eine Pflicht ist, müsste es ja auch sozusagen wie bei einer Haftpflichtversicherung eine Art Kontrahierungszwang geben. Wie würden Sie das umsetzen?

Sven Werner Tritschler (AfD): Ich habe eine Frage an Herrn Schuldzinski und Herrn Dr. Schabhüser. Sie haben vorhin angesprochen, dass Sie Ihre Erkenntnisse aus dem Phishing-Radar mit dem BSI teilen. Teilen Sie – beide Institutionen – solche Erkenntnisse auch mit privaten Anbietern, also zum Beispiel mit kommerziellen Anbietern von Virenschutzsoftware bzw. Sicherheitssoftware oder mit Mail-Providern?

Amt. Vorsitzender Marc Herter: Herr Bolte-Richter, von Ihnen liegt mir keine Wortmeldung mehr vor.

> (Matthi Bolte-Richter [GRÜNE]: Ich habe schon viele Fragen in der ersten Runde gestellt!)

– In Ordnung, dann beginnen wir nun in der zweiten Antwortrunde bei IT.NRW.

Hans-Josef Fischer (IT.NRW): Die Idee eines TÜV ist sicherlich noch nicht ganz durchdacht. Aber so, wie der TÜV bei Kraftfahrzeugen oder anderen gefährlichen Anlagen eine Vorabüberprüfung der Gefahrensituation ermöglicht, muss man meiner Meinung nach darüber nachdenken, ob nicht auch das In-Verkehr-Bringen jedenfalls einiger Soft- und Hardwareprodukte geeignet ist, ähnliche Schadensquellen zu eröffnen, wie es laut Gefährdungshaftung im BGB bei der Pferdekutsche oder beim Auto der Fall ist.

Es ist meines Erachtens darüber nachzudenken, ob es ausreicht, über Haftungsmöglichkeiten – gegebenenfalls auch über eine Beweislastumkehr – Haftungsrisiken auf die Produkthersteller zu übertragen, oder ob es nicht zumindest für gewissen Produktgruppen angezeigt ist, eine Vorabkontrolle durchzuführen. Wer das machen soll? – Ich denke, solche Technischen Überwachungsvereine, die auch zertifizieren, sehen sich durchaus in der Lage, so etwas durchzuführen.

Bei alldem ist aber wohl unbestritten, dass dies nicht ohne eine gesetzliche Grundlage möglich ist. Zurzeit sind wir, wie Herr Dr. Schabhüser dargestellt hat, in dieser Hinsicht niedrigschwelliger unterwegs.

Prof. Dr. Thorsten Holz (Ruhr Universität Bochum; Institut für Elektrotechnik und Informationstechnik): Bei der Frage von Herrn Braun ging es um das Max-Planck-Institut für Cyber Security und Privacy. Es wurde in der vorletzten Woche von der GWK final genehmigt. Aktuell sind wir also an dem Punkt, das Max-Planck-Institut aufzubauen.

Operativ wird das Ganze schon im Juni starten. Die beiden ersten Gründungsdirektoren sind bereits bekannt, und wir sind auch dabei, weitere Personen dafür zu suchen.

Mein Dank gilt da auch der Politik, die die Ansiedlung in Bochum überhaupt ermöglicht hat. Ohne die politische Unterstützung wäre es sehr schwierig geworden. Wir sind sehr froh, dass Bochum aktuell sehr stark ausgebaut wird. Uns wurde von der Deutschen

Forschungsgemeinschaft die Förderung für ein Exzellenzcluster zugesagt, wodurch für die nächsten sieben Jahre eine Förderung in Höhe von etwa 35 Millionen Euro gegeben ist. Das Max-Planck-Institut hat ein jährliches Volumen von 15 bis 20 Millionen Euro.

Das wird dazu führen, dass wir Bochum, wo momentan etwa 1.000 Studierende im Bereich der IT-Sicherheit studieren, deutlich ausbauen können. Im Endeffekt werden wir in dem ganzen Bereich 30 bis 40 Professuren haben. Es wird dazu führen, dass sich der Standort auch in den nächsten Jahren immer weiter entwickelt – von der Forschung, über Start-ups, von denen es momentan etwa ein Dutzend gibt, bis zu den etablierteren Endanwendern.

Insofern geht die Forschung in diesem Bereich sehr gut weiter. In NRW gibt es natürlich mit Bonn, Paderborn und Gelsenkirchen noch weitere Standorte. Gerade im Forschungsbereich sind wir in NRW im Bundesvergleich und auch im europäischen Vergleich gut aufgestellt.

Dr. Gerhard Schabhüser (Bundesamt für Sicherheit in der Informationstechnik): Zur Frage dazu, was wir mit dem Phishing-Radar machen: Daten, die wir monatlich erhalten, verarbeiten wir – soweit ich weiß; eventuell müsste ich es nachliefern – erstens im Kontext unseres Jahresberichts und zweitens als Input für Bürger-CERT und CERT NRW.

Dazu, ob wir die Daten eins zu eins an andere Stellen weiterreichen, bin ich überfragt. Wenn Dinge für den Verwaltungs-CERT-Verbund relevant sind, dann werden sie aber genau dort eingestreut werden.

Prof. Dr. Michael Meier (Rheinische Friedrich-Wilhelms-Universität Bonn; Institut für Informatik): Herr Matheisen, Sie hatten noch eine Nachfrage zu meiner Idee bzw. Vision gestellt, Cyberversicherer zur Regulierung einen Anreiz hinsichtlich kontinuierlicher Weiterbildung von IT-Nutzern generieren zu lassen – insbesondere im unternehmerischen Kontext.

Ich muss dazu einleitend sagen: Ich bewege mich da auf dünnem Eis bzw. ich bin als Informatiker die Versicherungswirtschaft betreffend absoluter Laie. Deshalb ist es wirklich nur eine Idee – ich finde sie aber nicht schlecht.

Meiner Wahrnehmung nach ist es so, dass sich der gesamte Versicherungsbereich im Kontext von Cybersicherheit erst noch entwickelt. Es ist sicherlich auch eine schwierige Materie; es ist deutlich einfacher, gegen Feuer und Wasser zu versichern. Das sind Risiken, die sich erst einmal gegenseitig ausschließen, aber solche sich gegenseitig ausschließenden Risiken zu finden, ist im Cyberbereich nicht so leicht. Von daher muss man schauen, inwieweit es sich entwickelt und wie es funktionieren kann. Eine Verpflichtung ist aus meiner Sicht aber erforderlich. Ohne eine solche verpflichtende Versicherung macht meine Idee keinen Sinn.

Ich würde so argumentieren: Die Unternehmer arbeiten mit Kundendaten, Mitarbeiterdaten usw. Sie haben Verantwortung für viel verschiedene Stellen und sind Risiken ausgesetzt, denen man nur begrenzt begegnen kann. Das Restrisiko muss dann durch

eine Versicherung aufgefangen werden. So würde ich die Verpflichtung, eine solche Versicherung abzuschließen, ableiten.

Den Rest übernehmen dann hoffentlich die Versicherungen, indem sie kontrollieren, wie hoch das konkrete Risiko beim Unternehmer ist, und entscheiden, ob er eine hohe Prämie erhält oder eine geringe, wenn er sich Mühe gibt.

Wolfgang Schuldzinski (Verbraucherzentrale NRW): Zur Frage von Herrn Tritschler: In der Tat ist es eine spannende Idee, zu überlegen, was man noch alles mit den Daten des Phishing-Radars machen könnte.

Zufällig war ich noch am letzten Freitag in Bochum bei einem dort ansässigen großen mittelständischen Unternehmen, das sich mit Datensicherheit befasst. Da haben wir auch philosophiert, was man alles machen könnte. Es gab viele Ideen. Wir müssen natürlich sehen: Wenn wir als öffentlich geförderte Organisation Daten zur Verfügung stellen, können wir sie nicht einer Firma zur Verfügung stellen, die damit Geld verdient, sondern dann muss man es auf Plattformen machen. Dann geht es eher darum, Tools zu entwickeln, die andere anwenden können oder so etwas. In Verbindung mit der Forschung ist da einiges denkbar, weil es sich um ein interessantes Datenmaterial handelt.

Die Ressourcen, die dort zum Einsatz gebracht werden können, sind allerdings sehr begrenzt. Das Datenmaterial ist vorhanden und spannend, und damit könnte man einiges machen.

Ich würde gerne anschließend an Herrn Professor Dr. Meier noch eine Idee ergänzen, wie das Land NRW gerade für KMU oder sogar noch eine Ebene darunter etwas tun könnte. Erfreulicherweise werden in erheblichem Maße Start-ups gefördert. Alles, was man zum Thema Privacy by Design tun kann, könnte man Start-ups vielleicht nicht als Bedingung, aber zumindest als Beratungsunterstützung ans Herz legen. Mit anderen Worten: Man gibt nur da öffentliches Geld aus, wo es von Anfang an mitgedacht wird und wo es nicht nur um die tolle Idee geht, die immer hinter dem Start-up steht, sondern auch um Datensicherheit und idealerweise auch um Datenschutz – darüber haben wir heute gar nicht gesprochen.

Ansonsten haben wir hier sehr viele schöne Ideen, aber was man bräuchte, wären meiner Meinung Plattformen – zum einen für Nutzer und zum anderen für KMU und Gewerbliche –, auf denen diese Ideen gebündelt und abgerufen werden können, damit man einen schnellen Zugang hat. Am Ende stehen dann gesetzliche Forderungen.

Ich will abschließend noch ein Beispiel nennen: Bei uns wird 1.500-mal pro Woche die Internetseite „Instagram-Account gehackt – wie erreiche ich den Support?“ aufgerufen. – Das zum Abschluss.

Amt. Vorsitzender Marc Herter: Ich danke den Herren Sachverständigen herzlich. Wir haben die Anhörungen sicherlich mit einem Erkenntnisgewinn verfolgt.

Das Protokoll der heutigen Veranstaltung ist nach seiner Fertigstellung auf der Internetseite des Ausschusses einsehbar.

Wir sind damit am Ende der heutigen Anhörung angelangt. Ich wünsche den Sachverständigen eine gute Heimreise und den Kolleginnen und Kollegen gleich noch eine gute Ausschusssitzung.

gez. Marc Herter
amt. Vorsitzender

Anlage
06.06.2019/14.06.2019
73

Stand: 14.06.2019

Anhörung von Sachverständigen
Sitzung des Ausschusses für Digitalisierung und Innovation
"**Lehren aus Hackerangriff ziehen – IT-Sicherheit in NRW verbessern"**
Antrag der Fraktion der AfD, Drucksache 17/4803
In Verbindung mit
„IT-Sicherheit in Nordrhein-Westfalen stärken – Freiheit sichern“
Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN, Drucksache 17/5056

am Donnerstag, dem 16.05.2019
14.00 bis 15.30 Uhr, E 3 D 01

Tableau

eingeladen	Teilnehmer/innen	Stellungnahme
Verbraucherzentrale Nordrhein-Westfalen, Düsseldorf	Wolfgang Schuldzinski	**17/1448**
Universität Bonn, Institut für Informatik, Bonn	Professor Dr. Michael Meier	**17/1455**
Bundesamt für Sicherheit in der Informationstechnik; Bonn	Dr. Gerhard Schabhüser	**17/1454**
Ruhr-Universität Bochum, Bochum	Professor Dr. Thorsten Holz	**---**
Information und Technik Nordrhein-Westfalen, Düsseldorf	Hans-Josef Fischer Jens Vieweg	**17/1453**
Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Düsseldorf	keine Teilnahme	**17/1447**

***