

Wortprotokoll

Öffentliche Sitzung

Ausschuss für Kommunikations- technologie und Datenschutz

5. Sitzung
13. November 2017

Beginn: 15.04 Uhr
Schluss: 17.04 Uhr
Vorsitz: Ronald Gläser (AfD)

Vor Eintritt in die Tagesordnung

Siehe Beschlussprotokoll.

Punkt 1 der Tagesordnung

Aktuelle Viertelstunde

Siehe Inhaltsprotokoll.

Punkt 2 der Tagesordnung

- | | | |
|----|---|-------------------------------|
| a) | Besprechung gemäß § 21 Abs. 3 GO Abghs
IT-Sicherheit in der Berliner Verwaltung
(auf Antrag der Fraktionen der SPD, Die Linke und Bündnis
90/Die Grünen) | 0020
KTDat |
| b) | Besprechung gemäß § 21 Abs. 3 GO Abghs
Stand der Umsetzung des Berliner E-Government-
Gesetzes: Umsetzung höherer IT-Sicherheit und Schutz
vor Cyberattacken
(auf Antrag der Fraktion der CDU) | 0033
KTDat |

- c) Antrag der Fraktion der FDP
Drucksache 18/0295
Kritische Infrastrukturen schützen. Jetzt!
- d) Antrag der Fraktion der FDP
Drucksache 18/0388
IT-Sicherheit durch Aus-, Fort- und Weiterbildung gewährleisten – Ein Cyber-Führerschein für die Berliner Verwaltung

[0019](#)

KTDat
InnSichO(f)
WiEnBe

[0027](#)

KTDat
InnSichO(f)

Hierzu: Anhörung

Vorsitzender Ronald Gläser: Hierzu haben wir drei Gäste, die wir jetzt anhören möchten. Ich begrüße in alphabetischer Reihenfolge zunächst Herrn Daniel Krupka, Geschäftsführer der Gesellschaft für Informatik. Herr Krupka hat dem Ausschuss zu den Anträgen unter Tagesordnungspunkt 2 c) und d) jeweils eine Stellungnahme sowie zu Tagesordnungspunkt 2 d) ein Positionspapier zur Verfügung gestellt, die Ihnen als Tischvorlage vorliegen. Dann begrüße ich Herrn Dr. Alexander Löw, Geschäftsführer Data-Warehouse GmbH, und Frau Professorin Dr. Margit Scholl von der TH Wildau, Fachbereich Wirtschaft, Informatik und Recht. Auch Frau Professor Dr. Scholl hat einige Unterlagen eingereicht, die Ihnen ebenfalls als Tischvorlage vorliegen, sowie eine Präsentation vorbereitet. – Ein herzliches Willkommen an die drei Anzuhörenden! – [Beifall] – Zu diesem Tagesordnungspunkt begrüße ich zudem vom IT-Dienstleistungszentrum Berlin Frau Ines Fiedler und Herrn Karsten Pirschel. – Herzlich willkommen!

Ich gehe davon aus, dass die Anfertigung eines Wortprotokolls gewünscht ist. – Gut, dann werden wir so verfahren. Ein Hinweis zum Vorgehen: Ich möchte vorschlagen, dass wir die Punkte 2 a) bis d) in der Aussprache verbinden und darum bitten, gegebenenfalls deutlich zu machen – das sage ich auch in Richtung der Anzuhörenden –, auf welchen Punkt sich eine konkrete Bemerkung bezieht. Sind Sie mit diesem Vorgehen einverstanden? – Das ist der Fall. Dann verfahren wir so.

Wir kommen nun zur Begründung des Besprechungsbedarfs zu Tagesordnungspunkt 2 a) durch die Regierungsfractionen. – Bitte, Herr Kohlmeier!

Sven Kohlmeier (SPD): Herzlichen Dank, Herr Vorsitzender! – Liebe Anzuhörende! Herzlichen Dank, dass Sie sich bereit erklärt haben, uns heute als Anzuhörende zur Verfügung zu stehen! – Wir haben schon ein kurzes Vorgespräch geführt. Als Politik sind wir ja, wie wir wissen, faktisch allzuständig und allwissend, gleichwohl ist es für uns immer interessant, auf manche Dinge auch einen Außenblick zu bekommen, damit man z. B. hier im Ausschuss nicht nur sozusagen in seiner eigenen Sauce etwas erzählt, sondern auch eine Fachexpertise-Sicht auf bestimmte Dinge bekommt – in diesem Fall auf die IT-Sicherheit.

Das Thema IT-Sicherheit ist eines der meist unterschätzten Themen in unserem Land, weil wir alle hoffen, dass der Kelch an uns vorbeigehen wird und es uns nicht betreffen wird, aber gleichwohl sehen wir ja, wie oft und wie stark Angriffe sowohl auf Verwaltungen wie auch auf öffentliche Institutionen oder Unternehmen allein im letzten halben Jahr passiert sind. Da

kann man den großen Hackerangriff oder den großen Virusbefall von Wanna-Cry beispielhaft herausgreifen, der Millionen von PC infiziert hat und wo in Großbritannien u. a. ein großer Krankenhauskonzern – auch so etwas muss man sich vorstellen, so etwas wäre durchaus auch in Deutschland möglich – angegriffen wurde. Man kann an den Hacker-Angriff auf die größte Reederei der Welt – Maersk – erinnern, die fünf oder sieben Tage lang faktisch lahmgelegt wurde. Da gab es gar keinen weiteren Hintergrund. Es war ein einfacher Hackerangriff, ohne Daten zu zerstören, aber die waren erst mal lahmgelegt und konnten dort nicht mehr arbeiten. Dann kann man in den USA Hackerangriffe auf die Atomindustrie als Beispiel nehmen, die angegriffen wurde oder wo zumindest versucht wurde, sie anzugreifen. Oder man kann das Beispiel nehmen, dass das Bundeskriminalamt festgestellt bzw. im Darknet gefunden hat, dass Millionen von personenbezogenen Daten, also Kontonummern, Benutzernamen und zugehörige Passwörter zu diversen Online-Marktplätzen, dort zu finden und zu kaufen sind.

Die Hauptschwachstelle, die bei allem immer wieder verifiziert wird und die sowohl vom BSI, dem Bundesamt für Sicherheit in der Informationstechnik, als auch von allen anderen Experten immer wieder genannt wird, ist ganz oft der End-User, und zwar derjenige, der in diesem Fall jetzt in der Berliner sitzt, eine E-Mail bekommt, auf einen infizierten Link klickt und dadurch letztlich diese Welle auslöst. In den seltensten Fällen, wenn man die Sicherheitsberichte des ITDZ und der Berliner Verwaltung liest, sind die Hackerangriffe wohl darauf zurückzuführen, dass es von ausländischen Geheimdiensten oder von anderen Staaten Angriffe gibt. Auch so etwas kann bei der Berliner Verwaltung nicht ausgeschlossen werden, aber das soll jedenfalls nicht der Hauptgrund der Angriffe sein.

Deshalb finde ich, dass das Thema IT-Sicherheit wichtig ist und dass wir gerade hier im Ausschuss für Kommunikationstechnologie und Datenschutz ein Bewusstsein dafür schaffen müssen – sowohl bei uns selber als auch bei den End-Nutzern und Anwendern, also der Berliner Verwaltung –, dass es dort ein Problem gibt. Es muss ein Problembewusstsein geschaffen werden, wie man heutzutage vernünftigerweise mit dieser Technik umgeht. Das war zu früheren Zeiten anders, als es die noch nicht gab. Da musste man auf andere Dinge achten. Heutzutage muss man halt achten, auf welche Anhänge man klickt.

Insofern bin ich dankbar, dass Sie uns als Anzuhörende heute zur Verfügung stehen und uns möglicherweise auch Eindrücke aus Ihrer täglichen Arbeit widerspiegeln und Hinweise geben können, was wir vielleicht besser machen können, und dass Sie dann gegebenenfalls auch Stellung zu den beiden Anträgen der FDP-Fraktion nehmen. Mein Vorschlag wäre, dass wir wie üblich die heutige Anhörung dann erst mal auswerten, also das Wortprotokoll abwarten und dann im Nachgang in der folgenden Sitzung mit den beiden Anträgen der FDP-Fraktion entsprechend umgehen.

Vorsitzender Ronald Gläser: Danke, Herr Kohlmeier! – Besteht Einvernehmen, was den Vorschlag von Herrn Kohlmeier angeht, dass wir die Abstimmung über die FDP-Anträge erst in der nächsten Sitzung machen, wenn das Wortprotokoll vorliegt und die Anhörung ausgewertet wurde? – Das ist so. Widerspruch höre ich nicht. – Nun bitte ich Herrn Lenz um die Begründung für den Besprechungspunkt der CDU-Fraktion. – Bitte!

Stephan Lenz (CDU): Ich kann mich ganz kurz fassen und mich dem Kollegen Kohlmeier anschließen. Es sind die gleichen Dinge, die uns umtreiben. Wir sind sehr gespannt auf die Anhörung und werden das weiter vertiefen durch Fragen. Wir sind sehr froh, heute die Mög-

lichkeit zu haben, hier zu lernen. Inhaltlich ist aber alles schon so weit vorgetragen worden, und ich kann mich darauf beschränken.

Vorsitzender Ronald Gläser: Vielen Dank, Herr Kollege Lenz! – Dann bitte ich jetzt Herrn Schlömer, die Anträge unter 2 c) und 2 d) zu begründen. – Herr Schlömer!

Bernd Schlömer (FDP): Die FDP-Fraktion hat in den vergangenen Wochen bzw. Monaten zwei Anträge in die parlamentarische Diskussion eingebracht, die unterschiedliche Regelungskreise betreffen. Das eine ist ein Antrag, der insgesamt die Sensibilisierung von Beschäftigten im Land Berlin verbessern helfen soll, indem die herkömmliche IT-Sicherheitsbelehrung durch eine neue Art von Awareness sinnvoll aufgewertet und erweitert werden soll.

Es geht darum, ein mehrstufiges, webgestütztes Verfahren für die Sensibilisierung in IT-Sicherheitsfragen auf den Weg zu bringen, welches mit einem Basismodul für alle Beschäftigten und weitergehenden Modulen für Professionals und Fachkräfte, die hohe Anforderungen in ihrem Arbeitsgebiet an die T-Sicherheit haben, das berücksichtigen soll. Nach wissenschaftlichen Erkenntnissen – vielleicht werden die Anzuhörenden dazu noch etwas sagen – trägt die regelmäßige und qualitativ hochwertige Sensibilisierung von IT-Beschäftigten signifikant dazu bei, das Niveau von IT-Sicherheit in Institutionen zu steigern. Ich halte daher diesen Antrag für sehr gut formuliert und bitte die anderen Fraktionen um Unterstützung.

Aber selbstverständlich bitte ich auch um eine Bewertung seitens der Anzuhörenden, die ich seitens der FDP-Fraktion ganz herzlich begrüße. Ich freue mich, dass wir eine Vertreterin der Wissenschaft, einen Vertreter eines Fachverbandes und einen Vertreter aus dem Unternehmensbereich hier haben. Das verspricht eine multiperspektivische Betrachtung. – Vielen Dank dass Sie da sind!

Der andere Antrag – „Kritische Infrastrukturen schützen. Jetzt!“ – ist formuliert worden vor dem Hintergrund des IT-Sicherheitsgesetzes. Sie wissen ja, dass in verschiedenen Sektoren das IT-Sicherheitsgesetz Betreiber besonders kritischer Infrastrukturen dazu verpflichtet, eine erhöhte, verbesserte Nachweispflicht und ein höheres Schutzniveau einzugehen. Diese Sektoren sind unter anderem Nahrungsmittel, Logistik, Abwasser, Energieversorgung, aber auch Rettungswesen, Informations- und Kommunikationstechnologie. Man kann sagen, dass diese Betreiber – das ist zumindest die Beobachtung der Fraktion der Freien Demokraten gewesen – sich schwertun, die ab Mai 2018 geltenden erhöhten Berichtspflichten und dazu bezogene Qualitätsrahmenbedingungen zu formulieren.

Der Antrag soll daher eines bezwecken: Er soll den Senat sensibilisieren, dass die in Berlin ansässigen Betreiber besonders kritischer Infrastrukturen – das sind Energieversorger, Krankenhäuser etc. – sich sehr aktiv dafür einsetzen, dass diese sektorspezifischen Regelungen formuliert werden, denn das Land Berlin mag nach dem IT-Sicherheitsgesetz nicht unmittelbarer Adressat dieser Sorgfaltsverantwortung sein, aber Senatoren und Staatssekretäre sind nichts anderes als Hauptverwaltungsbeamte, die mit den Kosten und Schäden, die durch Cyber-Angriffe entstehen, letztendlich umgehen müssen. Insofern haben wir diesen Antrag formuliert und bitten auch hierfür um Unterstützung seitens der anderen Fraktion.

Jetzt schon einmal mündlich angekündigt, schriftlich nachgereicht: Natürlich sind aufgrund der verzögerten Befassung mit den beiden Anträgen hier im Ausschuss die Daten für die Berichtspflichten anzupassen. Ich würde hierfür zur nächsten Sitzung eine schriftliche Formulierung einreichen, gebe aber erst einmal zur Kenntnis, dass das angepasst werden muss. – Vielen Dank!

Vorsitzender Ronald Gläser: Vielen Dank, Herr Kollege Schlömer! – Bevor wir zur Anhörung kommen, möchte ich noch einmal daran erinnern, dass Sie bei jeder konkreten Aussage bitte angeben, auf welchen Antrag oder Besprechungspunkt sich Ihre Aussage bezieht. – Ich bitte nun Herrn Krupka um seine Stellungnahme. – Bitte schön!

Daniel Krupka (Geschäftsführer der Gesellschaft für Informatik e. V.): Zunächst einmal vielen Dank, dass ich als Vertreter der Gesellschaft für Informatik heute hier zu Ihnen sprechen darf. Ich werde mich zuerst zu dem ersten Antrag der FDP-Fraktion äußern – „Kritische Infrastrukturen schützen. Jetzt!“ –, und im zweiten Teil zu dem zweiten Antrag bezüglich des Cyber-Führerscheins.

Wir haben es gerade schon gehört: Informatische und informationstechnische Systeme halten allerorten Einzug in unser Leben – in unser Alltagsleben, in unser Arbeitsleben – und eröffnen da enorme Chancen für die Beschäftigung, für die Art und Weise, wie wir arbeiten, und auch dafür, wie wir künftig zusammenleben. Aber diese neuen Möglichkeiten bringen eben auch eine ganze Menge an neuen Sicherheitsrisiken. Die zunehmende Vernetzung von IT-Komponenten und daraus erwachsende Abhängigkeiten führen zu einer erhöhten Verletzlichkeit der eingesetzten Systeme. Das betrifft natürlich insbesondere kritische Infrastrukturen und die Betreiber von kritischen Infrastrukturen, weil sie attraktive Angriffsziele sind. Sie haben ein besonders hohes Schadenspotenzial.

Letzte Woche hat das BSI seinen Bericht zur Sicherheitslage veröffentlicht, und da ist zum einen auch weiterhin die Rede von einem sehr hohen Risikopotenzial. Als zweiten zentralen Punkt hat das BSI festgehalten, dass praktisch die Mitarbeiter gewissermaßen ein zentrales Einfallstor für Angriffe sind.

Vor diesem Hintergrund begrüßen wir diesen Antrag der FDP-Fraktion – „Kritische Infrastrukturen schützen. Jetzt!“ – und erkennen gleichzeitig die Bemühungen des Senats an, in diesem Bereich tätig zu werden, also mit dieser Arbeitsgruppe Cybersicherheit, die als Koordinierungsstelle fungiert, mit der Benennung von konkreten Ansprechpartnern und auch damit, dass der Senat in diesem Bereich auch proaktiv unterwegs ist. Grundsätzlich würden wir uns natürlich wünschen, dass da noch mehr passiert. Zumindest sind das die verfügbaren Informationen aufgrund der Veranstaltung, die im Dezember stattgefunden hat. Eigentlich müsste der Senat an dieser Stelle noch viel aktiver werden, um auf diese Sicherheitsrisiken hinzuweisen und das Bewusstsein bei den Betreibern kritischer Infrastrukturen zu erhöhen.

Wir regen an, die eingeleiteten Maßnahmen des Senats zum Schutz kritischer Infrastrukturen und die Unterstützungsangebote für KRITIS-Unternehmen insbesondere in der Rolle des Senats als Aufsichtsbehörde auch transparent und nachvollziehbar darzustellen. Da hat sich für uns jetzt vorab in der Recherche eine gewisse Lücke gezeigt. Einige Sofortmaßnahmen, die aus unserer Sicht helfen könnten: Der Senat oder das Land sollte konkret Hilfestellungen für KRITIS-Unternehmen anbieten, beispielsweise bei der vollständigen Risikoanalyse aller Da-

ten und Anwendungen – idealerweise. Weisen Sie die KRITIS-Unternehmen auch darauf hin, dass das Sicherheitsniveau der Anwendungen und der genutzten Systeme in den Unternehmen von unabhängigen Dritten untersucht wird, und weisen Sie KRITIS-Unternehmen darauf hin, gleichermaßen auch die Sicherheitsprodukte selbst zu untersuchen auf zielführende Parametereinstellungen hin – also Firewalls, Verschlüsselung, Protection. Häufig genug ist z. B. die Firewall oder die Verschlüsselung zwar installiert, aber per Parameter abgeschaltet.

Letzter Punkt zu diesem ersten Antrag: Aus unserer Sicht wäre es sinnvoll, wenn der Senat darauf hinwirken würde, dass die KRITIS-Unternehmen im Berliner Raum das Thema IT-Sicherheit auch bei sich ganz oben auf die Agenda setzen – es idealerweise auch im Verantwortungsbereich der Geschäftsführung angesiedelt sein sollte, weil es ein ganz wichtiges Thema ist.

Ich will noch ein paar Sätze zum zweiten Antrag der FDP-Fraktion sagen, der aus unserer Sicht auch ein ganz wichtiger ist. Ich hatte es anfangs erwähnt: Die BSI-Erläuterungen haben das ganz zentral festgehalten, dass das Personal ein ganz entscheidender Faktor ist und deswegen auch das Know-how und die Sensibilisierung des Personals. Deswegen finden wir auch diesen Antrag sehr unterstützenswert. Wir sind überzeugt, dass das eine wirkungsvolle Maßnahme zur Sensibilisierung der Beschäftigten der Berliner Behörden hinsichtlich möglicher Cyber-Gefahren, der Informationssicherheit und des persönlichen Datenschutzes sein kann. Auch die webgestützte Variante – oder dass webgestützte Module angeboten werden – halten wir für ein gutes Instrument, vor allem auch, um relativ kurzfristig aktiv werden zu können.

Grundsätzlich finden wir auch diesen modularen Aufbau gut. Allerdings – und das ist wichtig festzuhalten – kann es aus unserer Sicht nicht dabei bleiben. Also es geht eigentlich darum, auch eine tiefere Weiterbildung der Mitarbeiter durchzuführen. Das ist mit einem reinen Webtool nicht getan. Das heißt, es muss – und das müsste der Kern des Ganzen sein – mit Schulungsmaßnahmen unterfüttert werden, insbesondere auch vor dem Hintergrund der EU-Datenschutz-Grundverordnung, die im Mai nächsten Jahres in Kraft tritt.

Das wären die mittel- bis langfristigen Baustellen, die angegangen werden müssten. Sie haben als Vorlage auch ein Positionspapier unserer Fachgruppe Verwaltungsinformatik bekommen. Darin geht es auch um die Frage, wie die Kompetenz in Behörden gesteigert werden kann, und da ist das auch ein ganz zentraler Punkt.

Einen letzten Punkt möchte ich noch ansprechen, und der betrifft auch das, was die Gesellschaft für Informatik unter anderem macht. Ich möchte darauf hinweisen, dass es Angebote in dem Bereich schon gibt. Es gibt beispielsweise den Europäischen Computerführerschein, der letztlich genau solche Themen adressiert. Also da gibt es auch ein Modul IT-Sicherheit und ein Modul Datenschutz. Also auch da der Appell: Man muss das Rad nicht neu erfinden, denn es gibt auf dem Markt schon eine Reihe von Dingen, die schon da sind und die Sie sich, sollten Sie sich entscheiden, dass es so etwas geben soll, natürlich auch einmal dezidiert anschauen sollten. – Wir als Gesellschaft für Informatik stehen auch gerne bereit in Bezug auf das, was grundsätzlich das Thema IT-Sicherheit angeht, und auch bei einer möglichen Entwicklung eines wie auch immer gearteten Cyber-Führerscheins. – Vielen Dank!

Vorsitzender Ronald Gläser: Vielen Dank, Herr Krupka! – Jetzt Herr Dr. Löw – bitte schön!

Dr. Alexander Löw (Geschäftsführer der Data-Warehouse GmbH): Sehr geehrte Damen und Herren! Vielen Dank für die Einladung und die Möglichkeit, vor ihnen zu sprechen! Herr Krupka! Vielen Dank für Ihre interessanten Ausführungen! – Ich möchte mich erst einmal mit dem Tagesordnungspunkt 2 a) beschäftigen, dem Thema „IT-Sicherheit in der Berliner Verwaltung“. Ein grundsätzliches Thema ist auch das Thema Awareness, worauf ich später noch eingehen werde.

Ich möchte erst einmal auf zwei Statements verweisen. Das eine ist vom Internet Security Forum 2016 verkündet worden: „No-one left to trust in cyberspace.“ – Das heißt, es ist sehr, sehr schwierig, im Bereich IT überhaupt noch Vertrauen und Vertrauensanker zu finden, und das ist eine der Herausforderungen, vor denen Sie als gesetzgebendes Organ entsprechend stehen und wo Sie auch entsprechende Vorbildwirkung haben können.

Das Zweite: Ich war 2016 in New York und hatte das Glück, mit dem Cyber-Leiter des New York Police Departments zu sprechen, und er hat mir gesagt, mit Stand heute ist die Cyberkriminalität einträglicher als Prostitution und Drogenhandel zusammen. Das heißt also, dass IT-Angriffe und IT-Kriminalität ein einträgliches Geschäftsmodell sind, und entsprechend sollte es auch innerhalb von Verwaltungen, Behörden und Unternehmen behandelt werden. Ich habe das Gefühl, dass wir in Deutschland noch nicht ganz so weit sind. Das heißt, wir stehen professionellen Angreifern gegenüber, die sich immer mehr spezialisieren und immer stärker werden, während wir in amateurhaften Gegenmaßnahmen versuchen, dem entgegenzuwirken, die sehr schwach koordiniert sind.

Das IT-Sicherheitsgesetz ist der Weg in die richtige Richtung. Es geht um Ransomware, Angriffe auf die Verwaltungen, wo zufällige Angriffe durch Verschlüsselung von Accounts stattfinden, und Datendiebstähle, die meistens nicht entdeckt werden. Datendiebstahl kann bedeuten, dass ein Angreifer bis zu 240 Tagen in Ihrem Netzwerk ist, aber niemand bemerkt das. Er kann Ihre E-Mails lesen und Ihre Informationen abziehen, er kann Passwörter mitbekommen, und die Amerikaner haben sehr schmerzhaft Erfahrung damit machen müssen. Ich verweise auf den berühmten OPM-Hack, in dem die gesamten Informationen aller Bundesbediensteten abgegriffen wurden inklusive Sozialversicherungsnummern. Das ist so etwas wie die eID des Personalausweises.

Entsprechend sind die Maßnahmen, die zu ergreifen sind, sehr wichtig. Ich habe im E-Government-Gesetz kurz mal nachgelesen. Wenn das stimmt, sind in Bezug auf die standardisierten PC 14 000 von 75 000 PC tatsächlich standardisiert. Das heißt, da ist noch ein großer Anteil an Arbeit, der entsprechend fortgeführt werden muss, damit die PC und die Infrastrukturen entsprechend abgesichert werden. Natürlich gibt es noch ein ganz wichtiges Thema – immer wieder ein Einfallstor auch in der Industrie –, und das ist das Thema von Identitäten und Vertrauensbeziehungen. Der Equifax-Hack war z. B. nur dadurch möglich, dass ein Administrator-Passwort nicht vergeben wurde und man über ein Standardadministrator-Passwort in das Computersystem eindringen konnte. Das heißt also, es geht auch um wirklich ganz triviale Fehler, die immer wieder passieren, und zwar nur dadurch, dass bestimmte Basismaßnahmen einfach nicht eingeleitet wurden.

Dementsprechend kommen wir immer wieder gerade auch bei Behörden und Verwaltungen auf das Thema Budget. Als IT-Sicherheitsunternehmen ist es für uns immer eins der Themen, dass wir meistens damit konfrontiert werden, dass die Verantwortlichen nicht genügend Budgets bekommen, um das Thema IT-Sicherheit in ihre Planungen mit aufzunehmen, und das ist eine der Herausforderungen, vor denen die IT-Verantwortlichen und die Dienstleistungsunternehmen immer wieder stehen: Sie versuchen, die Dienstleistung zu erbringen, haben aber nicht genügend Geld zur Verfügung.

Der Antrag unter Tagesordnungspunkt 2 c) – mit dem IT-Sicherheitsgesetz, Unterstützung von Firmen – betrifft genau das gleiche Thema. Auch in den Krankenhäusern, den öffentlichen Verwaltungen ist das Thema Budget für die IT immer ein ganz großes Thema. Budget für IT-Sicherheit: Das bedeutet manchmal, dass wir Kunden haben, bei denen es heißt, dass sie pro Mitarbeiter 17 Euro Budget pro Jahr zur Verfügung haben. Das heißt, das ist Virenschutz und eine Firewall. Das ist nichts heutzutage. Im Vergleich dazu werden bei Boeing oder im UK, wo wir gerade in entsprechenden Verhandlungen stehen, bis zu 1 000 Pfund pro Jahr pro Mitarbeiter in die IT-Sicherheit investiert. Das sage ich nur, damit man einmal ungefähr die Balance dazu sieht und ein Gefühl für die Zahlen bekommt.

Der dritte Punkt, zu dem ich Stellung nehmen möchte, ist der IT-Führerschein. Es ist ein sehr guter Ansatz für Erstausbildung oder für Awarenessbildung. In meinen Augen wäre vielleicht zielführender, so etwas wie Sicherheitsübungen zu machen, ganz einfache Sicherheitsübungen wie zum Beispiel: Man beglückt eine Behörde oder einen Behördenteil einfach mal mit ein bisschen Ransomware und schaut, wer auf die E-Mails reagiert, und wenn dann die ganzen E-Mails verschlüsselt sind, ist die Awareness beim Mitarbeiter ganz automatisch da.

Das ist auch der Psychologe in mir, was meine zweite Ausbildung ist, der sagt: Praxis ist viel besser, als über Theorie etwas zu machen. Ein IT-Führerschein ist etwas zum abhaken. Nach dem zweiten Jahr weiß man, wie er geht, und dann macht es vielleicht sogar noch ein Kollege, der sich damit besser auskennt. Also rein vom Gefühl her sind diese Sicherheitsübungen wesentlich zielführender. Das machen auch große Energieunternehmen. Die gehen davon aus, dass sie gehackt werden – es heißt nicht mehr „ob“, sondern „dass“. Und dann heißt es: Welche Maßnahmen werden getroffen, wenn wir angegriffen werden? – Immer in Zusammenarbeit mit der IT-Abteilung, mit dem Security Operation Center werden dann die Maßnahmen abgestimmt, und dann werden Übungen durchgeführt. Das kann zum Beispiel ein Cyber-Sicherheitstag sein. Dann weiß jeder Mitarbeiter: Okay, es kann passieren, dass wir angegriffen werden. – Dann kann er sich schon einmal entsprechend darauf vorbereiten, und damit ist die Awareness und die Befassung mit dem Thema viel leichter und viel zielführender als über theoretische, entsprechend abhakbare Maßnahmen. Das ist nur ein Vorschlag von meiner Seite. – Ich danke Ihnen für Ihre Aufmerksamkeit

Vorsitzender Ronald Gläser: Vielen Dank, Herr Dr. Löw! – Wir kommen zu Frau Prof. Dr. Scholl. – Bitte schön!

*Ausschuss für Kommunikationstechnologie und Datenschutz
des Abgeordnetenhauses*

*Anhörung zum Thema
Informationssicherheit in der Berliner Verwaltung*

Prof. Dr. rer. nat. Margit Scholl
13. November 2017

<p>Technische Hochschule Wildau (Wirtschafts- und Verwaltungsinformatik; Trainingszentrum für Informationssicherheit – „IT Security Arena“)</p>  <p>margit.scholl@th-wildau.de http://www.th-wildau.de/scholl</p>	<p>Wildau Institut für innovative Lehre, lebenslanges Lernen und gestaltende Evaluation</p>  <p>wille@twz-ev.de http://www.twz-ev.org/</p>
---	---

Prof. Dr. Margit Scholl (TH Wildau, Fachbereich Wirtschaft, Informatik und Recht): Vielen Dank für die Einladung! Ich bin gerne hier. Ich bin Qualifizierungsstelle der BAKöV, ich bilde also Informationssicherheitsbeauftragte aus – seit 2010 –, ich bin Qualifizierungsstelle der

BAköV für den Datenschutzbeauftragten nach EU-Datenschutz-Grundverordnung seit diesem Jahr, ich bin Prüfungszentrum des Europäischen Führerscheins mit den Modulen Informationssicherheit und Datenschutz, und ich bin seit diesem Jahr auch Prüfungsstelle des Datenschutzh Führerscheins und beschäftige mich, wie Sie sehen, als Hochschullehrerin in Forschung und Lehre mit dem Thema auch schon eine ganze Weile. Ich habe an unserer Hochschule und mit meinem Institut ein Trainingszentrum für Informationssicherheit aufgebaut und habe dort eine „IT Security Arena“ eingeführt, die das Ganze ein bisschen anders macht als nur mit digitalen Methoden, auch wenn digitale Methoden natürlich auch eine Rolle spielen.

Das heißt, mein Beitrag bezieht sich schwerpunktmäßig auf den Tagesordnungspunkt 2 d), aber eigentlich auf alle vier Punkte, weil natürlich letztendlich eine Erhöhung des Informationssicherheitsbewusstseins bei allen vier Punkten relevant ist und nicht nur bei dem letzten Punkt.

Ich habe Ihnen ein paar Folien ausdrucken lassen. Keine Angst, ich werde nicht alle zeigen. Ich habe das noch einmal eingeschränkt, aber ein paar Sachen zeige ich nun doch. Was bedeutet erfolgreiche Digitalisierung?

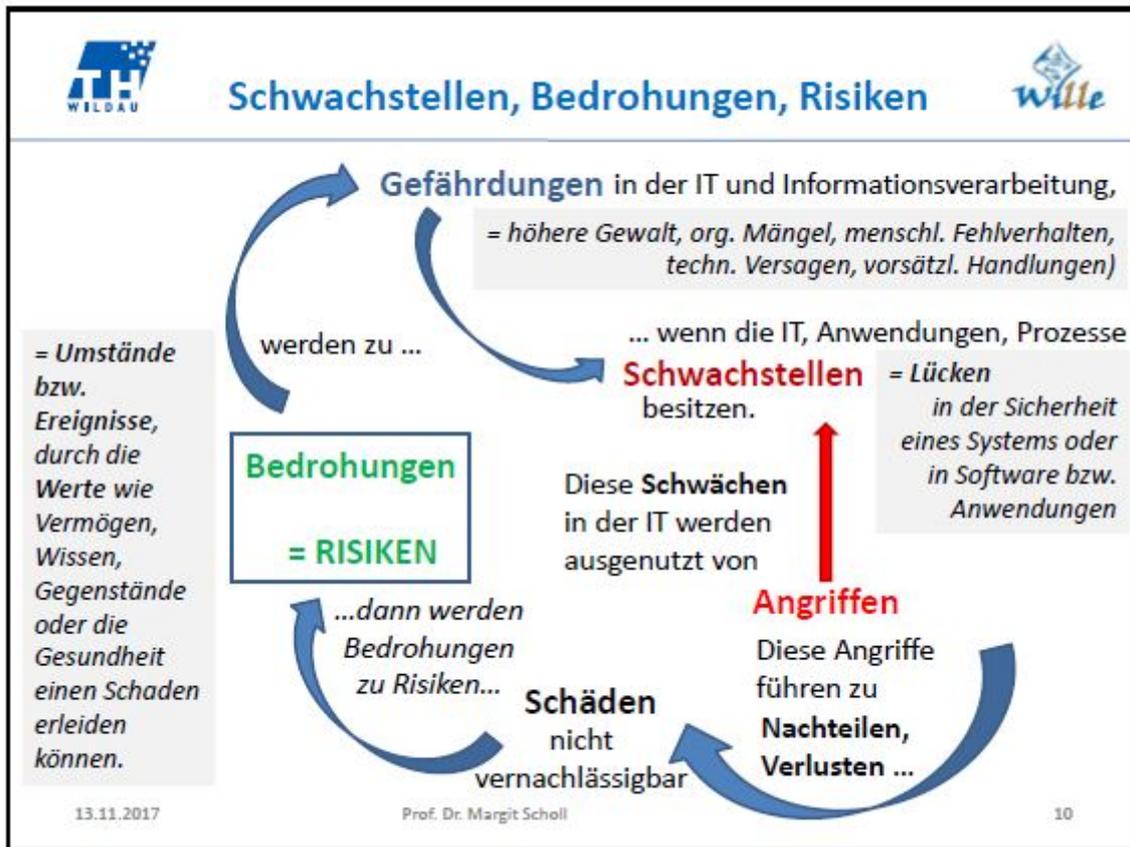
WILDAU **Erfolgreiche Digitalisierung...** **Wille**

- ...benötigt**
einen strategischen Blick sowie die Berücksichtigung von ablauf- und aufbauorganisatorischen Veränderungspotenzialen
- ...gewährleistet**
ein angemessenes IT-Sicherheitsniveau, Sicherheitsstandards und Datenschutz
- ...braucht**
ausreichend qualifiziertes Personal, das zudem Gestaltungsinteresse in komplexe Strukturen, interdisziplinäre Denk- und Arbeitsweisen, also **E-Government-Kompetenz** und **Informationssicherheitsbewusstsein** mitbringt
- ...erfordert**
einen Kulturwandel in der Organisation mit einer Neuausrichtung des Personals und mit spezifischen Kompetenzen in allen Arbeitsfeldern
- ...bedarf**
eines veränderten Personalmanagements mit kontinuierlicher, zielgruppenorientierter Fort- und Weiterbildung für **alle** Beschäftigten

13.11.2017 Prof. Dr. Margit Scholl 4

Sie benötigt einen strategischen Blick. Sie gewährleistet ein angemessenes IT-Sicherheitsniveau. Das ist auch die Grundeinstellung des BSI mit seinen entsprechenden Standards. Man braucht eine erfolgreiche Digitalisierung, ausreichend qualifiziertes Personal, und zwar eines, das auch Gestaltungsinteresse mitbringt, das interdisziplinär denkt, das neue E-Government-Kompetenz und natürlich auch Informationssicherheitsbewusstsein mitbringt. Das erfordert auch einen Kulturwandel in den Institutionen. Das heißt, es muss auch möglich sein, sich darüber auszutauschen, und es muss auch möglich sein, Fehler zu erkennen und aus

Fehlern lernen zu können. Es bedarf meines Erachtens eines veränderten Personalmanagements, und die Fort- und Weiterbildung, die zur Stärkung des Informationssicherheitsbewusstseins notwendig ist, betrifft alle Beschäftigten. Dazu will ich auch noch sagen: Informationssicherheit ist Chefsache. Es geht also von ganz oben bis ganz unten.



Lassen Sie mich noch einmal verdeutlichen, vor welchen Problemen wir stehen! Wir haben in unserem Leben überall Bedrohungen. Bedrohungen beziehen sich auf unsere Werte, auf unsere Gesundheit, und damit müssen wir umgehen. Das ist ganz natürlich. Diese Bedrohungen werden durchaus zu Gefährdungen, und zwar im Informationssicherheitssinne, wenn in der IT, also in der Informationssicherheit und in der Verarbeitung der Daten, Schwachstellen sind, und davon müssen wir ausgehen. Schwachstellen sind Lücken im System, Schwachstellen sind Lücken in der Organisation, Schwachstellen sind Lücken in der Software, und wir müssen davon ausgehen, dass solche Lücken existieren.

Diese Schwachstellen oder auch Schwächen der Informationsverarbeitung in Organisationen erleiden natürlich Angriffe. Das wissen wir, und das wurde von meinen Vorrednern auch schon ausgeführt. Diese Angriffe führen zu Nachteilen, zu Verlusten und zu Schäden. Das kann ein Imageschaden sein, das kann aber auch ein finanzieller Schaden sein. Wenn die Schäden nicht mehr vernachlässigbar sind, was bei den Beispielen, die hier schon genannt wurden, ganz offensichtlich ist, dann ist klar, dass sozusagen die Bedrohung inzwischen Risiken sind. Das heißt, alles, was wir in der Fort- und Weiterbildung unternehmen müssen, ist eben u. a. auch, diese Risiken zu reduzieren, indem wir das Bewusstsein und die Achtsamkeit für Informationssicherheit erhöhen.



Maßnahmen für höhere Sicherheit ...



- ... bedeuten Aufwand (persönlich und durch qualifiziertes Personal)
- ... benötigen Zeit
- ... kosten Geld ...



13.11.2017Prof. Dr. Margit Scholl11

Eine angemessene Sicherheit bedeutet immer, dass es aufwendig ist, dass man Zeit braucht und dass man natürlich auch Geld braucht. Also für null ouvert ist so etwas nicht zu bekommen. Die Frage ist nur, wie ich Geld, Zeit und Personal so einsetze, dass ich wirklich etwas nachhaltig hinbekomme. Da die Zusammenhänge einerseits komplex und andererseits nicht linear sind, ist das nicht ganz so einfach.



Sicherheitsgerechtes Verhalten



Technische Sicherheit
Angesichts der gewachsenen Gefährdungslage wird zwar verstärkt in technische Informationssicherheit investiert und über die Risiken informiert, doch reicht das nicht aus.

Mangelnde Sensibilität
Befragungen zu den Belangen der Informationssicherheit in Organisationen belegen nach wie vor eine mangelhafte Sensibilisierung.

Sicherheitsgerechtes Verhalten
ist bei **allen** Beschäftigten notwendig und erfordert das Wissen um und ein Gefühl für die Risiken, ebenso wie die Fähigkeit und das Wollen, sach- und sicherheitsgerecht mit Daten, Informationen und Informationstechnik (IT) umzugehen.

Vorgegebene Regelungen
sind eine Voraussetzung dafür, sich adäquat zu verhalten, und sollten eindeutig formuliert, allgemein bekannt und auf Einhaltung hin kontrolliert werden.
Regelungen allein langen jedoch nicht – sie müssen auch gelebt werden.

Vorschriften
können leichter eingehalten werden, je informierter die Beschäftigten über die Sachverhalte sind und je besser sie die Motive dafür verstehen.

13.11.2017Prof. Dr. Margit Scholl19

Sicherheitsgerechtes Verhalten heißt technische Sicherheit. Da wird investiert. In Technik wirst investiert, aber das reicht nicht aus. Es geht um die mangelnde Sensibilisierung, mangelnde Sensibilität für Informationssicherheit, das zeigen alle Untersuchungen immer wieder. Dann geht es alle Beschäftigten an. Es ist nicht nur der IT-Bereich. Informationssicherheit und Informationssicherheitsbewusstsein sind nicht nur IT-Bereich.

Dann müssen wir uns auch überlegen: Wir haben Regelungen. Es ist ja nicht so, dass es keine Regelungen gibt. Die Frage ist, ob diese Regelungen gelebt werden können. Denn hierbei ist die Frage: Werden sie gelebt werden? – Sie werden nicht zwingend gelebt, und da müssen wir überlegen: Warum werden sie nicht gelebt? – Die Vorschriften werden umso leichter einhaltbar – das zeigen unsere ganzen Forschungsergebnisse –, je besser die Akzeptanz ist, und die Akzeptanz ist umso besser, je informierter die Beschäftigten auch über die Motive – warum das so gemacht werden sollte – Bescheid wissen.

Die Spirale der transformativen Wechselwirkung: Ich will darauf gar nicht groß eingehen. Ich habe ein Exemplar von unserem Abschlussbericht hier dabei und, und den gebe ich gerne dem Vorsitzenden. Wir haben die Wechselwirkung zwischen Organisationsvorgaben und der Akzeptanz bei den Beschäftigten in unseren verschiedenen Projekten immer wieder untersucht, und eines ist ganz wichtig, und deshalb kann ein webbasierter Teil auch nur ein Teil sein. Wir müssen an die Emotionalität der Menschen heran. Wir müssen ihnen verdeutlichen: Ihr seid selbst betroffen, es geht euch an, ihr seid Teil davon. – Demzufolge müssen wir kreative, innovative Lernmethoden nutzen. Das bekommen wir nicht nur mit Websachen hin. Das ist ganz wichtig. Also wir brauchen Emotionalität, wir brauchen Austausch, wir brauchen Motivation, damit wir letztendlich eine Akzeptanz bekommen und ein Engagement, die Regelungen auch einzuhalten.



Unsere Erfahrung ist, dass wir einen integrativen Mix brauchen von analogen, haptischen, situationsbedingten Lernszenarien, wo wir wirklich vor etwas üben und wo klar werden muss, was man da tut, kombiniert mit digitalen Simulationen. Und wir brauchen einen Austausch, eine Kommunikation. Das heißt also, auch interaktive Methoden sollten da eingesetzt werden.

 **Erlebnisorientierte Sensibilisierung** 

 Sponsored by 
SecAware4job **HGS**
Hartmut Gierke
Berufshilfe

Forschungsprojekt SecAware4job:
Informationssicherheitsbewusstsein
für den Berufseinstieg, 2015-2017.



- Digitale Simulationen**
 - App- und Browser-Anwendungen
 - Wiederholung und Vertiefung
 - Selbststudium
- Analoge Simulationen**
 - Arena
 - Planspiele
 - Teamansatz
- Interaktive Methoden**
 - Diskussionen
 - Storytelling
 - Tiefenpsychologische Studien
 - Anwendung

Quelle: Scholl (Hrsg.), Abschlussbericht SecAware4job, 2017. Fuhrmann, Koppatz, Edich & Scholl, 2017.

13.11.2017 Prof. Dr. Margit Scholl 22

 **Mensch = „Kritischer Faktor?“** 

... wegen Mangel an Verständnis für Sicherheitsfragen
in Verbindung mit dem
allgegenwärtigen Gebrauch
von Computern ...



Aufmerksame und sachkundige Menschen
sind durchaus besser in der Lage
moderne Verletzungen der Informations-
Sicherheit zu verhindern...

Technologielösungen
reichen allein nicht aus,
um Gegenmaßnahmen
zu gewährleisten!

Menschen können auf Zwischenfälle effizient und effektiv reagieren, indem sie sie umgehend melden, Probleme unter Quarantäne stellen und diese Probleme richtig diagnostizieren und behandeln.

Dark, M.J., "Security Education, Training and Awareness from a Human Performance Technology Point of View", in M.E. Whitman, and H.J. Mattord (eds.), *Readings and Cases in Management of Information Security*, Course Technology, Mason, 2006, pp. 86-104.
Singh, A.N., A. Picot, J. Kranz, M.P. Gupta, and A. Ojha, "Information security management (ism) practices: Lessons from select cases from India and Germany", *Global Journal of Flexible Systems Management*, Vol. 14, No. 4, 2013, pp. 225-239.

2017/2018 Prof. Dr. Margit Scholl 30

Jetzt komme ich noch zu dem Menschen als kritischem Faktor. Das ist in allen Veröffentlichungen immer wieder drin und hängt damit zusammen, dass ihm dabei natürlich ein Mangel an Verständnis und auch ein nicht professioneller Umgang mit digitalen Medien und Computern nachgesagt wird. Aber ich bitte darum: Registrieren Sie, dass in der Forschung inzwischen ein Umdenken da ist, und zwar ein Umdenken insofern, dass uns Technologielösungen allein nicht die Informationssicherheit bringen, die wir brauchen.

Aufmerksame und sachkundige Menschen sind besser als Systeme in der Lage – es gibt dazu Tests –, Verletzungen zu erkennen und zu reagieren. Das heißt, wenn Menschen aufmerksam sind, also Awareness für Informationssicherheit haben, und wenn sie sachkundig sind – das heißt, wenn sie entsprechendes Wissen in Schulungen mitbekommen haben –, dann können sie Zwischenfälle effizient und effektiv bearbeiten. Da sind sie dann nicht der kritische Faktor, sondern im Gegenteil der stärkende Faktor.

Vorschlag: Landeskonzert Awareness

Ein Cyber-Führerschein für die Berliner Verwaltung ...

... ist ein guter Anfang, kann jedoch nur ein kleiner Baustein sein.

Benötigt wird ein
neues, strategisches

Landeskonzert
Awareness

(Sensibilisierung für
Informationssicherheit).

Dazu müssen Haushaltsmittel
eingeplant werden.



13.11.2017Prof. Dr. Margit Scholl30

Ich schlage Ihnen vor, dass der Cyber-Führerschein nur ein kleiner Baustein ist. Sie brauchen meines Erachtens etwas anderes. Nicht nur Berlin, sondern alle Länder brauchen etwas anderes, nämlich ein strategisches Landeskonzert von Awareness, wo integrativ alles zusammengefasst wird, wo eine Strategie ist und wo innovative Konzepte zum Tragen kommen.

Auf der folgenden Folie habe ich mal einfach aus dem Handbuch der BAKÖV zusammengefasst, welche Themen insgesamt behandelt werden müssten, also von Grundlagen der Informationssicherheit über einen Arbeitsplatz, über einen operativen Bereich bis hin zur Informationssicherheit. Das ist also eine ganze Menge. Vor allen Dingen muss es zielorientiert sein im Sinne von: zielgruppenorientiert sein. Und es muss auch arbeitsplatzbezogen sein.



BAköV-Handbuch: Schulungsinhalte



1. Grundlagen der Informationssicherheit
2. Informationssicherheit am Arbeitsplatz
3. Gesetze und Regularien
4. Sicherheitskonzept der Organisation
5. Risikomanagement
6. Informationssicherheitsmanagement
7. IT-Systeme
8. Operativer Bereich
9. Technische Realisierung von Sicherheitsmaßnahmen
10. Notfallvorsorge/Notfallplanung
11. Neue Entwicklungen im IT-Bereich
12. Betriebswirtschaftliche Seite der Informationssicherheit
13. Infrastruktur-Sicherheit



13.11.2017

Prof. Dr. Margit Scholl



p. 121f

31

Hier sehen Sie: Man würde zu solchen Tabellen letztendlich kommen, wo gesagt wird: Wer muss welche Inhalte wissen, damit er gut in seiner Arbeitssituation damit umgehen kann?



BAköV-Handbuch



• Seite 123: **Table 4: Zielgruppen und Schulungsmodul**

Zielgruppe	Schulungsmodul Nr.												
	1	2	3	4	5	6	7	8	9	10	11	12	13
Vorgesetzte	X	X	X	X							O	X	
Sicherheitsmanagement	X	X	X	X	X	X	X	X	X	X	X	X	X
Datenschutzbeauftragte	X	X	X	X							X	O	
Infrastrukturbeauftragte	X	X	X	X	X	O				X			X
Benutzer	X	X											
Administratoren	X	X		X	X		X	X	X	X	X		O

Legende: X: Modul wird empfohlen, O: Modul ist optional

Und mit welchen Methoden?

13.11.2017

Prof. Dr. Margit Scholl

32



Nach unserem Kenntnisstand reicht Wissensvermittlung allein nicht aus. Wir brauchen Emotionalisierung, und darüber hinaus brauchen wir den wirklichen Austausch über die Probleme, über die Situationen und über das Herangehen. Das ist für uns ein systemischer Ansatz, und wir bezeichnen ihn mit 3.0. Ich weiß, die Verwaltung ist manchmal schon bei 4.0, aber wir sind da noch bei 3.0.

Zusammenfassung: Der Mensch ist der Stärkefaktor. Er muss nur entsprechend ausgebildet sein und sensibilisiert worden sein. Das heißt: Digitalisierung nicht ohne Informationssicherheit, Informationssicherheit nicht ohne Awareness, und Awareness muss durch nutzerzentrierte Sensibilisierung und Schulungen erreicht werden! – Das bedeutet: Sie ist zielgruppenorientiert. Es geht um spezifische Situationen am Arbeitsplatz. Es geht um den Einsatz von kreativen Techniken, um die Emotionalität zu bekommen, um Motivation zu bekommen und um auch auszutauschen – und letztendlich, um darüber das Informationssicherheitsbewusstsein zu erhöhen. – Das war mein Beitrag.

Vorsitzender Ronald Gläser: Vielen Dank, Frau Prof. Scholl für den wertvollen Beitrag! – Ich schlage vor, bevor wir die Aussprache machen, sammeln wir erst einmal Fragen an die Anzuhörenden. – Herr Kohlmeier, bitte!

Sven Kohlmeier (SPD): Herzlichen Dank für Ihre Ausführungen, die – wenn ich es vorsichtig formulieren darf – ja faktisch nur die Spitze des Eisberges oder des Diskussionsansatzes abbilden können, und zwar der Diskussion, die wir hier miteinander führen müssten, oder zumindest, wo Sie uns politisch informieren müssten und dann die Verwaltung entsprechend arbeiten müsste.

Ich fand ein paar Punkte interessant, die Sie uns mitgegeben haben, und dazu habe ich einige Fragen. Herr Krupka hat gesagt, dass man die Mitarbeiter motivieren muss. Nun möchte ich von den Mitarbeitern der Verwaltung nicht sagen, dass sie nicht motiviert wären, insbesondere nicht die der Berliner Verwaltung, denn die sind ja bekanntermaßen hervorragend motiviert. – Es wird sogar genickt seitens der Verwaltung. – Können Sie aus Ihrer Sicht darstellen, wie wir es eventuell besser schaffen, die Mitarbeiter noch mehr zu motivieren, an Fortbildungen teilzunehmen, sich über die Cyber-Security-Punkte zu informieren und solche Dinge ernst zu nehmen?

Nach meinem Informations- und Kenntnisstand ist es so, dass durchaus in der Berliner Verwaltung etwas angeboten wird. Es ist also nicht so, dass es an Angeboten mangelt. Aber die Mitarbeiter nehmen daran nicht teil, wo auch immer die Gründe dafür liegen. Vielleicht liegt es am Angebot selber, vielleicht liegt es auch daran, dass sie so viel zu tun haben, vielleicht liegt es auch daran, dass sie einfach keinen Bock haben. Auch das wäre ja eine typisch menschliche Reaktion, zu sagen, dass man sich damit nicht befassen will, solange man mit dem PC einfach nur so herummacht und im Zweifel ein IT-Typ irgendwo sitzt, den man anrufen kann, wenn etwas passiert. Die Sache selbst interessiert ja nicht. Deshalb würde mich interessieren, ob die Anzuhörenden Empfehlungen haben, wie man die Mitarbeiter der Berliner Verwaltung motivieren kann, an diesen Trainings und Fortbildungen teilzunehmen, dafür ein Bewusstsein schaffen zu wollen und sich dieses Bewusstsein auch aneignen zu wollen.

Einen zweiten Punkt hat Herr Dr. Löw angesprochen, und den fand ich äußerst spannend, nämlich die Sicherheitsübungen. Da würde mich interessieren, ob es seitens der Verwaltung oder des ITDZ entsprechende Überlegungen gibt, weil ich das durchaus für einen interessanten, spannenden und nachvollziehbaren Punkt halte. Die Feuerwehr macht entsprechende Übungen, die Polizei macht entsprechende Übungen, der Katastrophenschutz macht entsprechende Übungen und hat gerade erst vor einigen Wochen in Lichtenberg eine Übung gemacht. Gibt es da entsprechende Überlegungen, so etwas auch in der Berliner Verwaltung einzuführen? Vielleicht kann Herr Dr. Löw, wenn er gesagt hat, dass große Energieunternehmen das machen, uns etwas an die Hand geben, wie sie das machen. Ich habe eine Vorstellung davon, muss ich deutlich sagen, aber vielleicht können Sie uns das noch einmal genauer darstellen: Kaufen die sich jemand Externen ein, um das zu machen? Haben die eigenen Leute? Wie könnte man so etwas auf den Weg bringen und so etwas entsprechend regulieren?

Die dritte Frage richtet sich an Frau Prof. Scholl, und zwar bezüglich des Landeskonzpts Awareness, das sie vorgeschlagen hat. Können Sie mir kurz skizzieren, was nach Ihrer Auffassung dort entsprechend drinstehen müsste? Denn es mangelt meines Erachtens in der Berliner Politik nicht daran, dass es keine Konzepte gibt – davon haben wir viel zu viel –, sondern möglicherweise mangelt es daran, dass man die Konzepte nicht auch entsprechend umsetzt. Deshalb meine Frage: Was müsste da eigentlich drinstehen, und wie müsste es umgesetzt werden?

Vorsitzender Ronald Gläser: Vielen Dank, Herr Kohlmeier! – Weitere Fragen? – Herr Ziller, bitte!

Stefan Ziller (GRÜNE): Ich habe auch eine Reihe von Fragen, und mit meiner ersten kann ich an die Ausführungen von Herrn Kohlmeier anschließen. Sie betrifft die Themen Awareness und Mitarbeiterschulung: Freiwillig oder verpflichtend, in welchem Abstand? Was wür-

den Sie empfehlen? – Das sind die klassischen Fragen. Wir haben gehört, dass es Angebote gibt, dass es aber keiner freiwillig macht, und wenn es verpflichtend ist, mögen die Leute das auch nicht. Wie kommt man aus diesem – ich sage mal – Schlamassel heraus, damit zumindest das Ziel erreicht wird?

Den Vorschlag dieser Sicherheitsübungen finde ich total spannend, vielleicht auch in Zusammenarbeit mit den Berliner Unis. Da kann man ja eine ganze Menge machen. Eine Bitte habe ich: Bitte fangen Sie nicht bei uns hier im Abgeordnetenhaus an! – (Heiterkeit) – Die Berliner Verwaltung ist da wichtiger.

Dann habe ich eine Frage zu den KRITIS-Unternehmen. Was ist da zu tun ist, wie kann man da Awareness schaffen, und welche Rolle kann dabei die Politik spielen? Das Land versucht ja, da mit dem Aufbau der Digitalagentur, was kleine und mittlere Unternehmen angeht, in die Beratung hineinzugehen und etwas zu machen. Meine These ist aber, dass das bei den KRITIS-Unternehmen, die ja eher Großunternehmen sind, eher schlecht funktioniert, wenn da jemand vom Land kommt und sagt: Ich erkläre Ihnen das mal. – Welche Instrumente würden Sie uns an die Hand geben, um bei den großen Unternehmen beratend zur Seite zu stehen, oder hilft im Zweifel eine hohe Geldstrafe als Androhung, damit die aktiv werden? Was würden Sie uns da empfehlen?

Dann habe ich eine weitere Frage: Wir sind als Land gerade dabei, auch über das E-Government viele Prozesse zu digitalisieren, und an vielen Stellen – ich glaube, Sie hatten es am Anfang gesagt – ist die Frage von Vertrauen im Internet und gegenüber den Akteuren von Bedeutung. Welche Rolle sollte dabei für uns Open-Source spielen? Wo brauchen wir öffentliches Wissen? Bei der Sicherheitssoftware sind wir von ein paar Herstellern abhängig. Das Land Berlin ist ja ein kleiner Baustein in Deutschland, aber sollten wir als öffentliche Hand diesen Weg der Abhängigkeit weitergehen, oder würden Sie uns zu etwas anderem raten? Wie bewerten Sie den Aufbau von tatsächlich öffentlichem, frei verfügbarem Wissen in dem Bereich, und wie sehen Sie die Notwendigkeit dafür?

Eine weitere Frage betrifft das Geld. Alle sagen, dass man dafür Geld haben muss. Wie bemesse ich als Politiker, wie viel Geld dafür gebraucht wird? Die IT-Sicherheitsleute sagen: Wir brauchen sehr viel. – Und dann kommen die Haushälter und sagen: Bisher ist doch nichts passiert, das Geld scheint gereicht zu haben. – Gibt es da einen wissenschaftlich anerkannten, objektiven Betrag, den wir ansetzen müssten? Ich glaube, die CDU hat in den Haushaltsberatungen immer wieder die Frage aufgeworfen: Wie viel Geld für die IT-Sicherheit ist in dem Titel drin? – Insofern frage ich die Anzuhörenden: Was können Sie uns dazu an die Hand geben? – Danke!

Vorsitzender Ronald Gläser: Vielen Dank, Herr Ziller! – Dann hat Herr Kollege Schulze von der Linksfraktion das Wort. – Bitte!

Tobias Schulze (LINKE): Vielen Dank, Herr Vorsitzender! – Ich schließe mich mit drei Fragen an. Mich würde interessieren, wie Sie die Gewichtung einschätzen, und zwar zwischen personellen Maßnahmen – also Weiterbildung, Motivation, Awareness usw. – und technischen Maßnahmen. Was sollte das jeweils bei einem bestimmten Finanzvolumen ausmachen? Welche Schwerpunkte sollte man da setzen? Kann man dazu etwas sagen? – Es wurde schon von mehreren, auch vom Kollegen Kohlmeier gesagt, dass häufig nicht die Technik das Problem war, sondern häufig war der Endnutzer oder die Endnutzerin das Problem. Bei Wanna-

Cry war es auch noch eine Verkettung sehr unglücklicher Umstände im Zusammenhang mit Geheimdienstaktivitäten und Geheimdienstentwicklungen. Das kann man auch nicht als rein technisches Problem ansehen, sondern das ist eher ein strukturelles oder wie auch immer geartetes Problem. Können Sie einen Hinweis geben – wir haben ja jetzt größere Etats für die IT-Sicherheit eingeplant –, wie die verteilt werden sollten? Wir kennen nur eine Globalsumme, aber wissen noch nicht genau, was die Verwaltungen damit tun, und vielleicht können Sie uns da Hinweise geben.

Ein zweiter Punkt: Sie hatten vorhin – ich weiß nicht mehr, wer es gesagt hat – von Standardisierung gesprochen und davon, dass zu wenige PC in Berlin standardisiert ausgestattet sind. Dazu meine Frage: Wie hilfreich ist Standardisierung an der Stelle? Wir arbeiten gerade daran, diesen Flickenteppich im IT-Bereich in der Berliner Verwaltung zu überwinden, und wenn es um Sicherheit geht, ist auch immer die Frage, ob Standardisierung hilfreich ist oder ob es manchmal nicht hilft, denn wenn man einen PC auf Standard hat, hat man gegebenenfalls mit einem auch gleich 60 000 PC geknackt. Dazu wäre ein Hinweis von Ihnen interessant.

Letzter Punkt: Kollege Ziller hat es schon angedeutet. Die Frage der Offenheit und der Sicherheit – bedingt sich das? Ist das ein Widerspruch, oder ist das kein Widerspruch? – Ich war damals an der Aufklärung des Bundestag-Hacks beteiligt, und da gab es sehr unterschiedliche Auffassungen darüber, wie man mit diesem Hack umgehen sollte. Es gab Leute, die sagten: Wir sagen dazu gar nichts, wir halten das alles unter der Decke. Auch die Ermittlungsergebnisse und Ähnliches darf niemand erfahren. – Und es gab andere, die gesagt haben: Nein, es bringt doch gerade etwas, die weltweite Community mitarbeiten zu lassen und mal darauf schauen zu lassen, was da eigentlich passiert ist und welche Prozesse dort genau stattgefunden haben. – Dazu muss man auch sagen, dass die Ermittlungsbehörden lange Zeit im Dunkeln tappten. Meine Frage schließt dabei etwas an das Open-Source-Argument an: Ist im Bereich der IT-Sicherheit, gerade wenn es um die Verwaltung geht, nicht auch die Sichtbarkeit von Schwachstellen oder das gemeinsame Arbeiten an der Beseitigung von Schwachstellen möglicherweise ein Konzept, was nicht nur für Hacker und Nerds interessant ist, sondern auch für die Verwaltung? – Danke schön!

Vorsitzender Ronald Gläser: Vielen Dank, Herr Kollege Schulze! – Nun hat Herr Kollege Schlömer das Wort. – Bitte schön!

Bernd Schlömer (FDP): Vielen Dank erst einmal für ihre Ausführungen! – Viele Fragen sind schon gestellt worden. Ich möchte noch zwei konkrete Fragen nachschieben. Wir haben in den zurückliegenden Sitzungen zum Handlungsfeld Charité von der Datenschutzbeauftragten gehört, dass es mit dem IT-Sicherheitskonzept an der Charité nicht zum Besten bestellt ist. Diesen Punkt werden wir irgendwann noch mal aufgreifen, und darauf freue ich mich auch schon. Aber vor diesem Hintergrund würde ich um Ihre Einschätzung bitten: Wie bewerten Sie die Bestellung von hauptamtlichen IT-Sicherheitsbeauftragten versus nebenamtlichen IT-Sicherheitsbeauftragten durch Privatunternehmen? Was ist Ihrer Ansicht nach der bessere Weg – eine hauptamtliche Person mit einer behörden- oder institutionsinternen Organisations- und Durchgriffsmöglichkeit oder ein Unternehmensberater, der zu hohen Tagessätzen zeitweise in großen Institutionen aufläuft? Das würde mich im Spannungsfeld zwischen Unternehmen und Wissenschaft interessieren.

Die andere Frage, die ich habe, richtet sich an Herrn Krupka. Es geht um den von Ihnen angesprochenen Europäischen Cyber-Führerschein. Haben Sie Kenntnis darüber, wie hoch der Aufwand ist, um einen solchen zu beschaffen und einzuführen? Was kostet so etwas? Ist das entgeltlos, oder ist das mit hohen Aufwendungen verbunden? Vielleicht können Sie dazu noch etwas sagen. – Vielen Dank!

Vorsitzender Ronald Gläser: Vielen Dank, Herr Schlömer! – Es ist sonst niemand mehr auf der Redeliste. Ich habe auch noch eine Frage an Sie: Herr Dr. Löw! Sie hatten das Beispiel mit den 17 Euro pro Mitarbeiter gebracht, die für IT-Sicherheit ausgegeben werden. Kennen Sie die entsprechenden Zahlen für Berlin? Könnten Sie die bundesweit einordnen, wo das Land Berlin dabei liegt? Ist die Ausgabe in Berlin eher hoch oder niedrig im Vergleich zu den anderen Bundesländern? – Weitere Fragen liegen nicht vor. Dann würde ich die Anzuhörenden bitten, auf die einzelnen Fragen zu antworten. – Bitte schön, Herr Krupka!

Daniel Krupka (Geschäftsführer der Gesellschaft für Informatik e.V.): Zu allen Fragen werde ich sicherlich nicht etwas sagen können. Herrn Kohlmeier fragte, wie die Mitarbeiter der Berliner Behörden dazu gebracht werden können, doch noch stärker an Schulungsmaßnahmen teilzunehmen. Ich bin kein Organisationsentwickler, und ich kenne auch die Berliner Behörden nicht gut genug, aber aus meiner Erfahrung kann ich zu der Frage, was hilft – neben Pflichtanteilen, die den Mitarbeitern gegebenenfalls in den Arbeitsvertrag mit hineingeschrieben oder in Vereinbarungen oder Personalgesprächen festgelegt werden –, sagen, dass es schon wichtig ist, ein entsprechendes Angebot zu schnüren, das so spannend ist, dass die Leute da einfach Lust drauf haben.

Die Idee mit den Sicherheitsübungen, die ich gerade gehört habe – ich kannte das in dem Kontext noch nicht –, fand ich eigentlich ganz gut. Bei diesem Europäischen Computerführerschein haben wir so eine Art Spiel gemacht – ich weiß nicht, ob Sie „Quizduell“ kennen –, und man kann sich dann so vorarbeiten – über einen Gaming-Faktor –, und das ist mittlerweile mit den Smartphones, die jeder in der Tasche hat, durchaus auch denkbar. Das könnte aus meiner Sicht ein Weg sein, die Leute über eine spielerische Komponente dorthin zu bekommen, sich stärker mit dem Thema auseinanderzusetzen. Man könnte auch über neue Wege nachdenken, dass sich die Berliner Verwaltung beispielsweise an Hackathons beteiligt oder versucht, die Mitarbeiter dafür zu gewinnen. Aber das ist sicherlich noch mal ein Stückchen weiter weg.

Die zweite Frage: Es gibt die Berliner Digitalagentur, aber es ist wohl schwierig, an große Unternehmen heranzukommen. Aus meiner Sicht ist da nichts besser als der Dialog, also einfach immer wieder Angebote zu machen und die Unternehmen auf die Sensibilität hinzuweisen. Die Berliner Landesverwaltung ist da so ein bisschen auf einer Zwischenebene. Es gibt das IT-Sicherheitsgesetz, und an das müssen sich die Unternehmen eigentlich halten. Von daher wäre aus unserer Sicht zielführend, eine Art Kampagne oder Gesprächsangebote zu machen, um nicht an den Punkt zu kommen, dass die Unternehmen sagen: Mit den Berlinern will ich nicht reden. – Wenn es die passenden Angebote gibt, dann werden die auch wahrgenommen.

Eine weitere Frage betraf das Thema Open-Source – also sollte dieses Wissen frei verfügbar sein. Dazu würde ich aus unserer Expertise sagen: Ja, wo es möglich ist, Transparenz walten zu lassen, wäre es gut. Bei den Diskussionen um die Hackerangriffe hat man es letztlich gesehen. Wenn Behörden da Wissen horten, kann das sehr schnell nach hinten losgehen. Das ist in den Bereich natürlich auch nicht ganz so einfach, aber da, wo es möglich ist, würden wir es durchaus begrüßen.

Zur Frage des Geldes will ich mich, offen gesagt, nicht äußern. Das kann ich einfach nicht, dazu habe ich keinen Kenntnisstand. Ich glaube, auf die Frage „Personal versus Technik“ wird es wahrscheinlich auch keine pauschale Antwort geben. Es ist wahrscheinlich von Behörde zu Behörde unterschiedlich und auch von Fragestellung zu Fragestellung. Ich glaube, die Technik ist die Hausaufgabe, die einfach auf dem neuesten Stand sein muss, und alles, was dann an Mitteln noch drin ist, müsste praktisch für das Personal ausgegeben werden. Ich glaube, da kann man nicht genug tun. Da wird es auch nie den Stand geben, dass man an einem Level angekommen ist, wo man sagt: Jetzt haben wir einen Kenntnisstand erreicht, der ausreichend ist. – Das wird es nie geben. Das ist einfach ein kontinuierlicher, dauerhafter Prozess, da mit den Mitarbeitern im Austausch zu stehen.

Zum IT-Sicherheitskonzept der Charité kann ich jetzt auch nicht so viel sagen, aber zu der Frage, was die Kosten des ECDL angeht – Sie korrigieren mich bitte –: Grundsätzlich ist das ja erst einmal nur ein Test, der letztlich ein Leistungsniveau gewissermaßen abfragt, und der kostet zwischen 50 und 80 Euro pro Zertifikat bzw. Führerschein, der dann ausgegeben wird. Wichtiger ist aber der Weg, um dorthin zu kommen, dass die Leute diesen Test positiv gestalten. Das ist wiederum mit Schulungsmaßnahmen verbunden. Das könnte auch über so eine App oder über so eine Art Spiel erreicht werden, wobei ich sagen muss, dass das wahrscheinlich erst mal das unterste Level ist, denn es ist dann wahrscheinlich so, dass die Leute die Fragen lernen, aber vielleicht nicht das Verständnis dahinter. – Aber dazu können Sie vielleicht auch noch etwas sagen.

Prof. Dr. Margit Scholl (TH Wildau, Fachbereich Wirtschaft, Informatik und Recht): Als Prüfungszentrum für den ECDL – den Europäischen Computerführerschein – kann ich dazu natürlich etwas sagen. Es gibt verschiedenste Prüfungszentren, das heißt, man bewirbt sich als Prüfungszentrum, erfüllt bestimmte Bedingungen und wird das dann. Für den Computerführerschein werden Tests am PC gemacht – unterschiedlicher Art. Wir nehmen jetzt mal dieses IT-Sicherheitsmodul. Wenn man sich da als Prüfling anmeldet, hat man online Unterlagen zur Verfügung, mit denen man sich einarbeiten kann, und dann kann man den Test nach einer gewissen Zeit am PC – bei uns z. B. im PC-Labor – absolvieren. Ein Test dauert ungefähr 20 bis 40 Minuten. Das kommt ein bisschen darauf an – sagen wir mal: eine halbe Stunde. Die Fragen müssen mit einem Anteil von mehr als 75 Prozent richtig beantwortet werden.

Die Vorbereitungsunterlagen, die Online-Unterlagen, sind sehr gut. Das heißt, man kann sich gut vorbereiten. Wir selbst bieten allerdings auch noch Vorbereitungskurse an. Insofern existiert so etwas, das kann man einführen, und das ist eine Frage letztlich des Marktvergleichs: Wer bietet was zu welchem Preis an? – Für die einzelnen Teilnehmer gibt es noch den Vorteil, dass man eine sogenannte ID bekommt, und mit dieser ID, die man ein Leben lang hat, kann man weitere Module entsprechend absolvieren. Die werden dann immer auf diese ID geschrieben, und dann hat man irgendwann möglicherweise viele Module des Europäischen Computerführerscheins zusammen – nicht nur die Informationssicherheit.

Der Punkt ist: Das ist ein kleiner Baustein. So etwas kann man machen. Es ist beispielsweise so, dass die BAKöV – also die Bundesakademie für öffentliche Verwaltung im BMI – einen BISS-Test entwickelt hat, den sie schon lange hat und wo jetzt seit einiger Zeit alle Beschäftigten bei der Bundesverwaltung verpflichtet werden, diesen BISS-Test zu machen. Der BISS-Test – also Bundesinformationssicherheitsschein-Test – dauert 15 Minuten lang, und am Ende hat man ein kleines Zertifikat. Das ist jetzt bei der Bundesverwaltung verpflichtend.

Darüber hinaus hat die Bundesverwaltung auch eine „Lernwelt“, einen Online-Lernkurs, „Lernwelt“ genannt. Der dauert, wenn man ihn von vorne bis hinten durcharbeiten würde, drei Stunden lang. Er hat verschiedenste Aspekte, die sich auf den Arbeitsplatz beziehen, aber natürlich auch allgemeingültig sind. Er behandelt dann auch sämtliche Probleme, die letztendlich da auftreten können. Fakt ist, dass die wenigsten die intrinsische Motivation haben, dieses drei Stunden lang von vorne bis hinten durchzugehen. Das macht so gut wie kein Mensch. Darüber hinaus ist es so, dass man so einen Kurs natürlich auch nutzen kann, um dann punktuell etwas nachzuarbeiten.

Jetzt komme ich noch mal zu dem, was unsere Erfahrung ist: Solche elektronischen Tools oder ein elektronischer Test oder eine elektronische Stütze sind wertvoll, aber das ist etwas, was wir danach einsetzen können. Wir brauchen vorher einen ersten Schritt, und der erste Schritt wird sein, dass Sie – und jetzt komme ich zu dem Awareness-Konzept – unterscheiden müssen zwischen Sensibilisierung auf der einen Seite und Schulung auf der anderen Seite. Bei Sensibilisierung geht es darum, die Leute abzuholen, und darum, die Wahrnehmung zu stärken. Da brauchen wir Emotionalität. Das geht nur analog. Das bekommen wir nicht digital hin. So einfach ist das.

Ich habe einen IT-Security-Park aufgebaut, wo wir genau das versuchen. Den möchte ich ganz kurz erklären. Das geht in Richtung Übung. Es sind verschiedenste Themen relevant, vielleicht 20 Themen, die immer wieder auftreten, wo ein Bewusstsein für dieses Problemfeld da sein sollte. Jede einzelne Lernstationen – so nennen wir das – dieser „IT Security Arena“ hat von der Idee her das Konzept: Fünf Minuten Einweisung in die Problematik – also z. B. Social Media, Phishing, Social Engineering oder welches Thema auch immer Sie da haben. Zunächst also fünf Minuten Einweisung, Abfragen, was bekannt ist, und dann gibt es ein spielbasiertes Lernszenario: Fünf Minuten – ich sage das mal in Anführungszeichen – spielen, gemeinsam diskutieren: Was würde ich machen, wenn? – Und dann kommen fünf Minuten Auswertung. Das heißt, eine Lernstation in diesem Sinne hat insgesamt 15 Minuten. Das ist Sensibilisierung, aber das muss passieren, um dann weiterzugehen.

Wenn wir also verschiedenste Themen haben – sagen wir mal: 20 Themen –, die wirklich relevant sind für die Beschäftigten an ihren Arbeitsplätzen, und wenn wir dann noch Vorfälle einbauen können – das sehe ich übrigens auch so, dass man das kombinieren können sollte –, dann wissen wir ja die Defizite, und dann beginnen die eigentlichen Schulungen. Die eigentlichen Schulungen müssen zielgruppenorientiert aufgebaut werden. Es muss nicht jeder alles wissen. Ganz spezifisch für das jeweilige Tätigkeitsfeld sollen die Schulungen aufgebaut werden. Das ist entscheidend. Wie gesagt, meine Vorstellung ist wie folgt: Erst einmal eine Sensibilisierung, um zu emotionalisieren und abzuholen – kurz, aber gezielt! Dann Defizite erkennen und intensivere Schulungen zu den einzelnen Punkten durchführen, die aber nicht zu allgemein sein dürfen, sondern sie müssen zielgruppenorientiert und spezifisch für den

Arbeitsplatz sein! Wenn man das hat, dann kommt die Geschichte mit den Tests, dann kann ich einen solchen Penetrationstest, wie es heißt, machen. Dann kann ich mal eine Phishing-Mail durchschieben und kann mal sagen: Okay, wie ist denn das jetzt, nachdem wir sensibilisiert und geschult haben? Nehmen sie diese Mails immer noch an? – Das wäre dann sozusagen die Evaluation des Ganzen. Ich denke, dass in einem solchen Landeskonzept eben genau dieses enthalten sein müsste. Wir brauchen eine integrierte Kombination verschiedenster Methoden, um die Menschen abzuholen.

Zum Geld kann ich insofern etwas sagen, als es bei dem vom BSI anvisierten IT-Grundschutz erst einmal um ein angemessenes Sicherheitsniveau geht. Dieses angemessene Sicherheitsniveau wird dann noch darüber hinaus betrachtet, wenn ich höheren Schutz oder sehr hohen Schutzbedarf habe. Unabhängig davon ist die Geldfrage auch eine Frage der Risikobelastung. Risiken haben zwei Seiten. Ein Risiko hat eine Ursache, und ein Risiko hat einen hat ein Schadensausmaß. Die Ursache hängt mit der Frage der Eintrittswahrscheinlichkeit zusammen. Wie wahrscheinlich ist es, dass das passiert? Wenn ich nicht schule und wenn ich nicht sensibilisiere, ist die Eintrittswahrscheinlichkeit höher, als wenn ich es tue. Auf der anderen Seite habe ich das Schadensausmaß, und darin bewege ich mich. Diese Risiken muss ich als Unternehmen, als Verwaltung oder als Institution eben tatsächlich spezifisch entwickeln und abfragen, und ich muss mir Gedanken dazu machen. Dann können Sie Risiken entweder akzeptieren und sagen: Gut, warten wir mal ab! –, oder Sie sagen: Diese Risiken sind mir eindeutig zu hoch. – Wenn man eine hohe Eintrittswahrscheinlichkeit und ein hohes Schadensausmaß hat, dann muss man die Risiken reduzieren – das ist überhaupt keine Frage –, und das wird gemacht durch Maßnahmen. Und das kostet wiederum Zeit und Geld. – So würde ich das beantworten.

Zu der Frage eines hauptamtlichen Informationssicherheitsbeauftragten oder zum Thema „Herausgeben an Private“: Da ich selbst in der Verwaltung gearbeitet habe – in der Berliner Verwaltung vor langer Zeit –, kenne ich auch die Verwaltung und weiß, dass es dort eine andere Kultur gibt. In den Verwaltungen gibt es eine andere Kultur als in Unternehmen. Ich denke, dass die Verwaltung ihr Know-how nicht vollständig nach außen geben darf. Das bedeutet für mich, dass meine Position so ist: Die Institutionen, die Verwaltungen, brauchen einen eigenen IT-Sicherheitsbeauftragten, und zwar genau so, wie sie einen Datenschutzbeauftragten brauchen. Die beiden blicken auf die gleiche Sache aus unterschiedlichen Blickwinkeln, und die müssen sich ergänzen. Das würde ich nicht aus der Hand geben. – Ich glaube, jetzt habe ich erst einmal die Fragen so weit beantwortet.

Vorsitzender Ronald Gläser: Vielen Dank, Frau Prof. Scholz, für diese vielen beantworteten Fragen! Das gilt auch für Herrn Krupka. – Jetzt hat Herr Dr. Löw das Wort. – Bitte schön!

Dr. Alexander Löw (Geschäftsführer der Data-Warehouse GmbH): Vielen Dank! – Ich hoffe, ich habe jetzt auch sehr viele Antworten für Sie. Die erste Frage bezog sich auf das Berliner Budget: Nein, dazu habe ich keine Aussagen. Das habe ich auch nicht untersucht, und ich habe auch keine Zeit gefunden, mich darum genauer zu kümmern. Das müsste noch erhoben werden, kann gern gemacht werden.

Zur Fortbildung und Steigerung der Teilnehmerzahlen: Das ist immer ein sehr spannendes Thema. Wir waren vor zwei Wochen in Washington D.C., wo wir den Chief Information Security Officer von Facebook getroffen haben. Facebook hat z. B. einen Cyber-Security-

Monat. Die nennen den „Hacktober“. Das ist insofern eine gute Idee, weil das ganze Unternehmen auf Cyber-Security ausgerichtet wird. Es werden ständig irgendwelche Gamifications und entsprechende Awareness-Mails herumgeschickt. Also einen ganzen Monat lang im Jahr werden die Leute damit richtig genervt.

Rein prinzipiell ist es so, wenn ich mir das so vorstelle mit den Cyber-Führerscheinen: Ich selbst werde immer wieder von Schulungsveranstaltungen entsprechend angesprochen. Wenn ich alles, was ich wüsste, testifizieren müsste, dann müsste ich bei 35 bis 50 Schulungen und Zertifikaten teilnehmen. Das kann ich nicht machen, dazu habe ich keine Zeit, und vor allem ist mir das Geld dafür zu schade – und meine Zeit sowieso. Das ist ein ganz persönliches Statement, und ich glaube, vielen Ihrer Beamten geht es genauso. Durch die Elektronifizierung und Optimierung der Arbeitsplätze werden Sie angesichts der Freizeiten oder der Zeiten, in denen man noch zusätzlich Zeit für irgendetwas Lästiges wie Sicherheit hat – und dann auch noch IT-Sicherheit; das ist ja ganz weit weg von dem, was sich sonst noch täglich an Arbeitslast zu erledigen habe –, sicherlich begeisterten Zuspruch dafür erhalten. Das ist mein persönliches Gefühl.

Aber Sie haben ja z. B. die Strategie, einen Standard-PC auszurollen. Warum wird da Sicherheit nicht mit implementiert? Sie müssen sowieso Schulungen für die neue Software, die da drauf ist, durchführen. Warum wird da nicht gleich die Schulung für IT-Sicherheit mit eingepackt – im Rahmen der Schulung für die Betriebssysteme, für die Officesysteme? Irgendetwas so in dieser Richtung! Das wäre ein integrierter Ansatz, würde den Workload ein bisschen herunternehmen, und das würde die Leute vielleicht sogar ein bisschen bei ihrer täglichen Arbeit unterstützen.

Dann das Thema Sicherheitsübungen: Das sind grundsätzlich von der Spitze oder von dem strategischen Beauftragten geplante Übungen für bestimmte Bereiche, je nachdem, wo Sicherheitsmaßnahmen als nötig angesehen werden oder wo man Schwachstellen befürchtet. Man kann also nicht genau sagen, wo eine Cyber-Sicherheitsübung stattfindet. Das ist im Grunde wie bei einer Feuerwehübung. Wenn der Feuerwehralarm losgeht, dann muss man halt gemeinsam rausgehen. Dann gibt es bestimmte Leute, die bestimmte Tätigkeiten haben. Genauso wird das auch geplant, und genau das Gleiche passiert mit einem PC. Kann man die Back-ups wieder einspielen? Das ist ein klassisches Thema bei Ransomware. Das ist bei vielen Krankenhäusern schiefgegangen. Was passiert, wenn das Internet weg ist? Wie können die Leute ohne elektronische Kommunikation überleben? Kann das Krankenhaus ohne elektronische Kommunikation noch arbeiten?

Das sind so klassische einfache Übungen, die man durchführen kann. Das hat sich sehr bewährt. Bei entsprechenden Energiebetreibern wird das dann halt so gemacht: Was passiert, wenn unsere Kommunikation mit dem Kraftwerk ausfällt? Wie können wir damit umgehen? – Und die IT-Mannschaft und die Administratoren werden damit genauso überrascht, denn sonst ist es keine richtige Übung. Entsprechend sieht man dann, was ist. Man lernt sehr viel daraus, und dann kann man die entsprechenden Maßnahmen treffen. Und dann kann man sagen: Okay, wir müssen noch mal nachschulen. Wir müssen noch ein bisschen Awareness-Schulung machen oder etwas Ähnliches.

In die Richtung geht auch die Frage, wie man, wenn man an größere Gesellschaften herangeht, diese unterstützen kann oder wie man sie beraten kann. Da muss man sagen, dass das

auch ein strategisches Thema ist. Mein Vorschlag wäre: Vertragsgestaltung! Sie haben Verträge mit Ihren Vorständen, mit Ihren Vertretern, mit Ihren Aufsichtsräten in den großen Einrichtungen, die teilprivat sind. Entsprechend können Sie in Verträgen entsprechende Klauseln oder entsprechende Motivationen verankern. Das gilt außerdem auch für Mitarbeiter. Wenn die Sicherheitsrisiken finden, nicht bestrafen, sondern belohnen! Das ist ein ganz klassisches Thema, das fast überall in Deutschland falsch gemacht wird. Da sind wir Spezialisten in Deutschland. Man sollte Mitarbeiter belohnen, wenn sie Sicherheitslücken finden. Das ist ein ganz wichtiges Thema. Und das betrifft das Führungskonzept: Wie führe ich mein Unternehmen bzw. wie führe ich meine Behörde? – Das ist nämlich eins zu eins das Gleiche. Das Risiko ist genau das gleiche. Da gibt es keinen Unterschied, ob es eine Behörde ist oder ein Privatunternehmen.

Das Gleiche gilt für die Sicherheitssoftware. Hier fängt es an, philosophisch zu werden. Grundsätzlich, um es ganz einfach zu machen, von der Softwareentwicklungstheorie her: Jede Software enthält Fehler. Eine kritische Sicherheitssoftware darf maximal 0,5 Fehler pro 1 000 Zeilen Code enthalten. Kommerzielle Software hat ungefähr sechs Fehler pro 1 000 Zeilen Code. Damit man ein Gefühl dafür bekommt: MS-Windows hat ungefähr 350 Millionen Zeilen Code. Also da sind ein paar Fehler drin. SAP hat ungefähr die gleiche Größenordnung. Nur, damit man mal weiß, was so ein Hacker als Angriffsszenario zur Verfügung hat! Also da ist einiges zu tun.

Open-Source-Software: Dadurch, dass bekannt ist, wie der Code geschrieben ist, sind viele Schwachstellen herausgenommen, aber wie man immer wieder sieht, gerade in der Open-Source-Software: Es sind grundsätzliche Fehler durch eine Community da, die eben nicht gesteuert entwickelt. Da sind Basisfehler genauso möglich. Das heißt also, je nach Kritikalität muss man hier entsprechend entscheiden, welche Art hier günstiger ist. Bei uns war es z. B. so: Wir sind selber aus China angegriffen worden, und bei uns wurde durch die kommerzielle Software – – Das sind zwei Sicherheitsstufen. Die sind durchmarschiert ohne Probleme, und erst in der dritten – das war eine ganz proprietäre Firewall von einem meiner Administratoren, ganz unüblich aufgesetzt – haben sie einen Fehler gemacht, und unsere Internetverbindung ist weggefallen, und deshalb haben wir es entdeckt. Aber das ist sozusagen so, je nachdem, welche Kritikalität Ihr Bereich dann entsprechend hat, und entsprechend geht es auch um die Budgetfrage.

Sie müssen das je nach Kritikalität, je nach Risiko entsprechend abschätzen: Was ist der Schaden, der entstehen kann, wenn Daten verlorengehen? Wenn wir gehackt werden, wenn es publik wird, welchen Schaden haben wir dann? – Denken Sie an meine Eingangsworte: „No-one left to trust in cyberspace.“ Es führt dazu, dass eben das Vertrauen in die öffentliche Hand nicht besser wird, denn wir haben ja unsere Vorratsdatenspeicherung, Trojaner, Staatstrojaner, Datenhehlerei usw. auch noch als Themen haben, die auch immer wieder das Vertrauen nicht deutlich vertiefen.

Zuletzt zum Sicherheitskonzept: Das ist ein ganz heikles Thema. Ich selbst bin externer Datenschutzbeauftragter für den Paritätischen Wohlfahrtsverband in Bayern. Ich bin zuständig für knapp 200 Mitgliedsorganisationen, 20 000 Leute, und ich mache nebenbei das Sicherheitskonzept mit. Es hat beides ein für und Wider. Da muss man sich bei der Auswahl derjenigen, die man mit einer solchen Stelle betrauen würde, diese sehr genau ansehen. Rein prin-

zipiell bin ich eher auch dafür, dass man sagt: Erst mal einen Internen, falls Sie eine Expertise bekommen, die diese Aufgabe ausfüllen kann!

Das ist nämlich eines der größten Probleme, die heutzutage existieren: der Fight for Talents. Wo bekommen Sie die Expertise mit Ihren BAT-Besoldungsgehältern her – also für jemanden, der mit einem Hacker, der teilweise bis zu 10 000 US-Dollar am Tag bekommt, konkurrieren kann. Das ist dann auch eine Frage, ob die Gehälter in der richtigen Dimension sind, dass Sie die entsprechenden Experten für diese herausfordernde Aufgabe bekommen. Denn nur zu verwalten und eine ISO-27 000 oder einen BSI-Grundschutz entsprechend abzuhacken, ist nicht die Lösung. Das ist keine IT-Sicherheit. Man bekommt sein ISO-27 001-Zertifikat, aber deswegen haben Sie noch lange keine Sicherheit. Das stellen wir bei sehr vielen Unternehmen fest, wenn wir Audits machen. – Jetzt bin ich, glaube ich, mit meinen Antworten schon durch. – Vielen Dank für Ihre Aufmerksamkeit!

Vorsitzender Ronald Gläser: Vielen Dank für Ihren Vortrag, Herr Dr. Löw! – Jetzt haben wir eine Fragerunde gehabt. Gibt es noch den zusätzlichen Wunsch nach einer Aussprache? – Wenn das nicht der Fall ist, würde ich den Senat um eine Stellungnahme bitten. – Bitte, Frau Smentek!

Staatssekretärin Sabine Smentek (SenInnDS): Ich würde vorschlagen, dass Frau Fiedler die konkrete Frage beantwortet, und dann würde ich gern noch ein paar grundsätzliche Bemerkungen machen.

Ines Fiedler (ITDZ; Vorständin): Es ging um die Frage der Übungen. Ich kann den Gutachtern nur zustimmen, weil auch wir sehr gute Erfahrungen mit Übungen gemacht haben. Wir machen einmal im Jahr – das gehört tatsächlich für uns zum Prozedere – eine Notfallübung. Die läuft genau so. Im letzten Jahr haben wir sogar simuliert – mit dem LKA –, wo bei uns die Leute angerufen wurden: Es gibt ein Sicherheitsfall. – Und dann war die Frage: Sind die Administratoren in der Lage, das, was in unseren Konzepten steht, wirklich praktisch anzuwenden, nämlich das Netz dicht zu machen und die Eskalationsszenarien, die beschrieben sind – also bestimmte Leute anzurufen, bestimmte Sachen im Haus aufzunehmen –, auszuführen.

Genauso haben wir im letzten Jahr noch zusätzlich aufgrund der Ransomsituation auch mal Mails verschickt. Ich sage das mal so offen. Da ging es dann um ein Gewinnspiel, und tatsächlich war es so – unsere Leute sollen ja sehr affin sein –, dass auch tatsächlich zwei das angeklickt haben. Das hilft uns aber, denn wenn bei uns solche Fehler begangen werden, dann ist das gesamte IT-Landesnetz betroffen. Deswegen nehme ich diese Anregung mit und würde gern darüber nachdenken – zusammen mit der IKT-Steuerung –, dass wir vielleicht weitere Behörden mit dazu nehmen, um das basierend auf den Erfahrungen noch auszuweiten.

Ich kann das nur unterstützen. Es ist immer wieder spannend, zu sehen, wie all das, was aufgeschrieben ist, in der Übung umgesetzt wird. Also das ist schon ein Effekt, aber ganz wichtig. Denn alles, was man nicht übt – Genauso ist es mit dem Restore. Das ist auch ganz klassisch. Wir haben sehr viele Back-up-Dateien, und wenn es dann wirklich zum Restore kommt, also dass die Daten wieder eingepielt werden, ist das der Klassiker in der IT. Auch das versuchen wir wirklich immer wieder mal zu üben. Ich glaube, unsere Verantwortlichen hatten sogar zweimal im Jahr die Übung, aber ich bin da offen. Das ist auch ein Aufwand, denn das

wird alles separat geplant, keiner darf es wissen. Das muss auch Hand und Fuß haben. Aber ich kann nur dafür werben – wir haben da auch gute Erfahrungen –, das eine oder andere auszuweiten. Vielleicht schaffen wir es auch noch mal, über unser Haus hinaus z. B. eine Behörde mit einzubeziehen. – So viel als Antwort auf diese Frage.

Vorsitzender Ronald Gläser: Vielen Dank, Frau Fiedler! – Herr Kohlmeier – bitte!

Sven Kohlmeier (SPD): Ich habe eine Nachfrage. Ich finde die Idee oder die Vorstellung einer Sicherheitsübung interessant. Da können wir uns jetzt als Regierungskoalition und als Opposition sofort nach der Sitzung daran machen, einen entsprechenden Antrag zu formulieren. Möglicherweise kann der Senat in Verbindung mit dem ITDZ uns dazu zumindest zu Protokoll geben und sagen: Wir werden so etwas prüfen und werden dem Ausschuss vielleicht in drei Monaten eine Überlegung vorstellen, ob man so etwas machen kann.

Ich finde die Idee auch spannend, so wie Herr Dr. Löw gesagt hat, dass man mal bei einer Verwaltung oder einer Teilverwaltung den Stecker für das Internet herauszieht und schaut, wie dort die Mitarbeiter reagieren. Das kann man ja mal ausprobieren. Es könnte ja mal passieren, dass das Internet ausfällt, und dann wäre es spannend zu sehen, wie die Abteilung damit umgeht – ob man sich dort entspannt hinsetzt und bis zum Nachmittag Kaffee trinkt und abwartet, was passiert, oder ob da die Alarmketten und die Informationsketten tatsächlich funktionieren. Das halte ich für eine durchaus spannende Geschichte, und wenn man so etwas ein paar Mal macht, dann sensibilisiert man vielleicht doch die Verwaltung, weil die natürlich nicht wissen, ob der Ausfall des Internets nun ein tatsächlicher Ausfall oder nur die Folge einer Idee ist, die an einem Montagabend nach einer Ausschusssitzung geboren wurde. Insofern finde ich es als Vorschlag tatsächlich äußerst spannend, und ich würde mich freuen, wenn Sie die Zusage machen könnten, dass man in drei Monaten so etwas noch mal aufruft und sagt: Wir haben da ein paar Ideen, um so etwas mal umzusetzen.

Vorsitzender Ronald Gläser: Vielen Dank! – Frau Smentek, bitte!

Staatssekretärin Sabine Smentek (SenInnDS): Ich würde gern die Gelegenheit nutzen, mich erst einmal zu bedanken, denn in den Vorträgen der Expertin und der Experten waren viele Anregungen praktischer Art, wie wir unser System noch verbessern können. Wir haben hier die ganze Zeit nicht etwa deshalb getuschelt, weil wir das so langweilig fanden, was Sie erzählt haben, sondern weil wir gleich überlegt haben, an welcher Stelle wir den einen oder anderen Ihrer Vorschläge bei dem, was bei uns zum Thema IT-Sicherheit gerade im Werden ist, mit einbeziehen. – Herzlichen Dank dafür!

Mein Einstieg zeigt auch, dass wir genau wie in allen anderen Bereichen des E-Government-Gesetzes dabei sind, jetzt die Leitplanken zu setzen und uns jetzt in die richtige Richtung zu bewegen. Das soll nicht heißen, dass wir hier in Berlin beim Thema IT-Sicherheit bei null anfangen. Das Thema BSI-Grundschutz gibt es natürlich schon eine Weile, und es gibt durchaus einige Verwaltungen, die auch bei der dezentralen Verantwortung – das hat etwas mit den 13 000 Arbeitsplätzen zu tun, die derzeit beim ITDZ betrieben werden – einiges gemacht haben. Es gibt auch andere Verwaltungen, die bisher im Bereich IT-Sicherheit schon einiges gemacht haben. Das hängt aber in der Tat von der Frage ab, mit welcher Priorität – ich glaube, das war auch so ein Thema – das von der jeweiligen Leitung der Behörden befördert wurde oder eben nicht.

Und man muss dazu auch sagen – das haben wir in dem Ausschuss schon öfter thematisiert –: Die Situation im Bereich der IT-Technik bzw. der IKT des Landes Berlin sortiert sich natürlich nach den Prioritäten der Vorjahre. Das ist die Situation, die wir hier im Augenblick vorfinden, und da haben wir noch einiges zu tun.

Wir haben natürlich versucht, einiges in Sachen IT-Sicherheit durch die Planungen der Migration zum ITDZ und die Einführung des flächendeckenden IKT-Arbeitsplatzes zu tun. Deswegen sind wir auch nicht unbedingt in der Lage, unsere Ausgaben für IT-Sicherheit pro Arbeitsplatz auszuweisen, denn bei den Investitionsvorhaben, die wir jetzt planen und hoffentlich dann nach der Beschlussfassung über den Haushalt auch umsetzen können, sind immer auch Anteile für das Thema IT-Sicherheit enthalten. Das hatten wir hier im Ausschuss auch so dargelegt. Das fängt an bei der Frage, wie gut das Landesnetz ist, wie gut die Ausstattung des IKT-Arbeitsplatzes ist und wie gut die Fortbildung der Mitarbeiterinnen und Mitarbeiter ist, damit sie die Möglichkeiten, die diese neue Ausstattung ihnen bietet, auch tatsächlich nutzen können. Das ist der Weg, den wir im Augenblick gehen.

Heute habe ich gelernt – und nur so viel würde ich an der Stelle sagen –, dass wir gut daran getan haben, in der neu aufgebauten Abteilung V der Senatsverwaltung für Inneres – IKT-Steuerung – eine extra Arbeitsgruppe für IT-Sicherheit einzurichten, die nicht nur die formalen Fragen abarbeiten wird, die ja schon genug wären, sondern sich auch mit den Themen Fortbildung und Awareness und den Fragen befasst, wie man das eigentlich kontrollt und wie wir die Verwaltungsakademie dazu bringen können, bestimmte neuere Methoden mit einzu beziehen. Das wird auch Teil der Arbeit dieser Arbeitsgruppe sein. Insofern sind wir im Augenblick ganz gut unterwegs, die einzelnen Teile des E-Government-Gesetzes, wo wir ja an verschiedenen Stellen Themen der IT-Sicherheit haben, auch umzusetzen. – Deswegen auch herzlichen Dank für das, was Sie uns heute dazu mitgegeben haben!

Lassen Sie mich an der Stelle vielleicht noch einen Punkt anführen. Bevor man die Mitarbeiterinnen und Mitarbeiter hinter die Fichte führt und ihnen mal das Internet abstellt und hinterher sagt: April, April, war nur eine Übung! –, würde ich eigentlich lieber so anfangen, wie Frau Prof. Dr. Scholl uns das vorgestellt hat. Ich glaube, wir müssen die Mitarbeitenden auch erst in die Lage versetzen, dass sie richtig damit umgehen, und dann können wir auch mit solchen Übungen vorangehen. Deswegen nehme ich gern diese Anregung auf, dass wir uns in einer der nächsten Sitzungen hier im Ausschuss mit einem solchen Schulungs- und Awareness-Konzept auseinandersetzen. Geben Sie uns die Chance, zu gucken, was wir Ihnen an der Stelle vorstellen können. Auch das ist etwas, was man nicht auf Knopfdruck einfach mal irgendwo her kopiert – so nach dem Motto: Die BAKöV hat es doch, macht das doch eins zu eins für die Berliner Verwaltung! – Dadurch, dass im Land Berlin sowohl Landesverwaltungen – und damit Ministerialverwaltungen – als auch Sicherheitsbehörden und Kommunalverwaltungen angesiedelt sind, haben wir eine besonders komplexe Herausforderung bei dem ganzen Thema rund um die IT-Sicherheit.

Ich glaube allerdings eines – und das ist die letzte Bemerkung, die ich machen möchte –: Wir haben es durch die Vorfälle der letzten Jahre und auch durch das, was in den letzten Monaten passiert ist – mit Lücken in Systemen, die dann auch zu erheblichen Beeinträchtigungen und auch zu Schäden geführt haben –, bei den Mitarbeitenden aller Hierarchiestufen im Land Berlin durchaus geschafft, ein gewisses Interesse für IT-Sicherheit zu wecken. Ich glaube, es hat sich auch in der Berliner Verwaltung herumgesprochen, dass IT-Sicherheit etwas mit Nutzerinnen und Nutzern zu tun hat und nicht nur die Frage einer guten Hardware-Ausstattung und einer Firewall ist. Insofern haben wir jetzt die Chance, da auch tatsächlich sinnvolle Schritte nach vorn zu tun.

Vorsitzender Ronald Gläser: Herr Lenz – bitte!

Stephan Lenz (CDU): Ich habe eine Frage direkt an den Senat, aber auch an die Sachverständigen, wenn es dazu von deren Seite etwas zu sagen gibt. Ich möchte vorab sagen, dass ich ein bisschen das Gefühl habe, dass das hierbei Thema Sicherheitspolitik noch nicht so richtig vorkommt. Ich meine, wir alle müssen stärker verinnerlichen, dass das ein erheblicher Teil der Debatte sein muss und dass man wahrscheinlich auch diejenigen, die diese Angriffe betreiben, stärker in den Blick nehmen muss. Man muss also auch die Täterperspektive stärker in den Blick nehmen. Das muss man erst mal lernen, und man muss sich dort hineinfinden, aber es steckt eben auch immer jemand dahinter, der diese Angriffe betreibt. Insofern fand ich auch gut, was Frau Fiedler gesagt hat, dass nämlich das ITDZ selbstverständlich im Rahmen seiner Notfallübung das LKA mit im Boot hatte. Das gehört auch dahin, und wahrscheinlich würde auch beim nächsten Mal hier bei einer solchen Anhörung jemand vom LKA mit dazugehören. Wenn man eine Anhörung zum Thema Einbruchssicherheit macht, ist ja auch klar, dass neben den Präventionsexperten jemand von der Polizei da säße, und ich denke, so sollte man auch hier stärker in diese Richtung umdenken.

Zu dem, was Kollege Kohlmeier gesagt hat: Ich habe auch eine große Sympathie dafür, dass man diese Notfallübung beim ITDZ, die hier von Frau Fiedler dargestellt wurde, erweitert – auf möglichst viele. Es sind ja nicht alle Arbeitsplätze so weit, aber wie ich es verstanden habe, sind schon einige auf diesem Standard. Das sind über 10 000, und mit denen könnte man ja schon mal eine Übung machen. Sie werden ja im Blick haben, welche das sind, und mit diesen kann man ja schon einmal eine Übung machen. Auch wenn sie noch nicht den Berlin-PC eingeführt haben, so sind sie doch auf einem Standard, der eine Übung möglich macht. Um diese Überforderungssituation, die Frau Smentek angesprochen hat, zu vermeiden, müsste man sich natürlich auf die beschränken. Aber das könnte man auch tun. Das heißt, wir müssen es nicht auf den Sankt-Nimmerleins-Tag verschieben, sondern wir können vielleicht schon im nächsten Jahr schauen, ob wir da etwas hinbekommen. Und im übernächsten Jahr sind es ja nicht nur 10 000 oder 14 000, sondern sicherlich über 20 000, und so kann man sich sukzessive, bis man dann die Gesamtzahl erreicht hat, voranarbeiten.

Dann noch eine Sache: Wir haben jetzt noch einmal gehört, dass das in Abteilung V zentral angesiedelt ist. Das ist eine Abteilung der Innenverwaltung. Da bietet es sich ja an – es greift ja ineinander –, stärker mitzudenken, dass es letztlich auch Sicherheitspolitik ist. Es ist nicht nur Sicherheitspolitik, aber eben auch. Das müssen wir in Zukunft stärker in den Blick nehmen.

Vorsitzender Ronald Gläser: Vielen Dank, Herr Kollege Lenz! – Frau Fiedler, bitte!

Ines Fiedler (ITDZ; Vorständin): Ich würde gern die Gelegenheit nutzen, um das eine oder andere, was die Experten und Gutachter gesagt haben, noch einmal auf unsere Situation herunterzubrechen. Die Frage ist dann: Wo stehen wir als Landesdienstleister heute, was die IT-Sicherheit betrifft? – Erst mal kann ich genau das bestätigen, was Sie sagen: Für uns hat das immer eine organisatorische und technische Dimension. Organisatorisch ist vieles schon im E-Government-Gesetz etabliert. Das betrifft z. B. die Einführung eines IT-Sicherheitsmanagementsystems. Das heißt zwar „System“, es hat aber nicht so viel mit Technik zu tun. Da geht es vor allem auch um Regelungen, die zu definieren sind, bezüglich der Frage: Wie gehe ich mit IT-Sicherheit um? – Ich finde, da kommen wir wirklich gut voran. Da sind erste Regelungen auch durch die Staatssekretärin sozusagen festgesetzt. Ich glaube,

gerade heute ging ein Vorschlag zur Gestaltung der Anforderungen an einen Mail-Server heraus, also wo man genau hinschaut, welche Regelungen und welche konkreten Vorgaben es braucht, damit wir dort wirklich sauber unterwegs sind.

Und dann ist da natürlich die technische Dimension. All das, was Sie zur organisatorischen Dimension gesagt haben, will ich gar nicht wiederholen, denn ich glaube, dass wir Awareness brauchen und dass wir in unserer gesamten Verwaltung tatsächlich auch noch viel mehr die Aufmerksamkeit brauchen: Was bedeutet das für mein konkretes Handeln? – Aber viel wichtiger sind dann die technischen Dimensionen, und dazu will ich auch gar nicht so viel sagen, denn ich glaube, dass wir als ITDZ in allen Bereichen mit Systemen ausgestattet sind – ob das die Server sind, ob es unser Datacenter ist, ob es die Endgeräte und die Kommunikationsnetze sind oder ob es natürlich auch die regelmäßige Beobachtung ist, was gerade auf dem Markt passiert. Denn das ist genau das, was Sie sagen: Wir haben eine Lösung, und schon ist die kriminelle Seite – ich würde das mal so schwarz malen – mit der Entwicklung ein Stück weiter, und wir müssen nachrüsten, was natürlich am Ende auch etwas mit Budget und Kompetenz zu tun hat. – Das will ich nur unterstreichen.

Um auch ein paar Zahlen zu nennen: Wir beobachten, dass sich das bei uns im ITDZ entwickelt. Wir haben das CERT, das Berlin-CERT, in Betrieb, und wenn man sich das anguckt, so werden dort täglich die Warnmeldungen des BSI gecheckt. Das ist sehr wichtig. Wir hatten davon in 2015 1 430, und in 2016 waren es schon 2 087. Das zeigt einfach, wie das anwächst, und hier wird mit dem CERT für das Land Berlin wirklich geguckt: Was sind das für Empfehlungen, und was machen wir damit – im ITDZ, aber auch landesweit? – Das Berlin-CERT ist ja nicht nur für das ITDZ da, sondern es gehen dann Informationen an alle Behörden raus: Was bedeutet das für Patch-Prozesse? Was bedeutet das für Schwachstellen? Ist vielleicht auch einmal ein System abzustellen, bis die Schwachstelle behoben ist? – Ich kann mich daran erinnern, dass es dann schon mal abendliche Telefonate gibt. Das hatten wir mit der Senatskanzlei, weil tatsächlich eine Schwachstelle dazu geführt hat, Systeme abzustellen. Also das ist bei uns im CERT etabliert.

Noch eine andere Zahl: Hinsichtlich der abgewehrten Angriffe – was man auf den Firewalls auslesen kann – sind wir bei ca. 7 Millionen. Also das ist etwas, das ansteigt, und das zeigt uns, dass heute – früher war es so, dass die Behörde vielleicht nicht immer im Fokus stand, das war eher die Wirtschaft – die Behörde interessant ist und dass wir uns deswegen an der Stelle weiter gut aufstellen müssen.

Wichtig ist auch noch die Zahl der von uns erkannten Viren – egal, ob sie auf den Endgeräten oder auf den Servern sind. Wir hatten 2016 16 700. Das Land Berlin ist groß, und da ist eine ganze Menge täglich zu tun. Was für uns aber häufig die größte Sicherheitsherausforderung darstellt, ist tatsächlich die veraltete Technik. Da sind wir genau bei dem, was auch Herr Dr. Löw gesagt hat. Für uns verursacht den größten Aufwand, um sicher zu sein, die veraltete Technik. Ich sage das immer wieder: Wir betreiben auch noch Winword-95-Verfahren, und wenn es darum geht, das dann sicher in einer Infrastruktur zu etablieren, sind wir echt gefordert. Deshalb helfen uns das E-Government-Gesetz und die Standardisierung an der Stelle enorm, auch wenn jetzt noch die Frage im Raum steht, ob ich dann 60 000 PC habe, die ich auf einmal angreifen kann. Da brauche ich dann andere Sicherheitsmechanismen. Aber dieses Individuelle und Veraltete ist auf alle Fälle hochgradig gefährlicher und auch für uns vom Sicherheitsaspekt her schwierig zu managen.

Zum Schluss: Nach welchen Rahmenbedingungen arbeiten wir? Woran orientieren wir uns? – Das ist ganz klar: Am BSI-Standard – das sind die Standards 100-1, 100-3, neu sind es dann 200-1 bis 200-3 – und natürlich am Grundschutzkatalog! Also so wird unsere Infrastruktur ausgerichtet. Wir sind auch BSI-zertifiziert, weil wir glauben, dass wir nur so den Sicherheitserfordernissen der Zukunft gerecht werden können. Das vielleicht als kleiner Exkurs dazu, wo wir stehen. Nichtsdestotrotz gestatten Sie mir noch abschließend zu sagen: Sicherheit bleibt für uns trotzdem eine große Herausforderung – sowohl, was Kompetenz betrifft, als auch, was Geld betrifft –, denn ich glaube, dass das sehr, sehr schnell wächst und dass wir als ITDZ da ständig mithalten müssen. Es ist eine Herausforderung, dem standzuhalten. – Vielen Dank!

Vorsitzender Ronald Gläser: Vielen Dank, Frau Fiedler! – Frau Smolczyk, bitte!

Maja Smolczyk (Berliner Beauftragte für Datenschutz und Informationsfreiheit): Vielen Dank, Herr Vorsitzender! – Nur eine kleine Ergänzung aus Sicht des Datenschutzes: Ich werbe natürlich dafür, dass die IT-Sicherheit immer gemeinsam mit dem Datenschutz gesehen wird. Es gibt ja riesige, sich überschneidende Felder. Auch die Datenschutz-Grundverordnung, die erwähnt worden ist, setzt neue Kriterien fest, die sich nicht nur auf den Datenschutz beziehen, sondern auch auf die IT-Sicherheit. Also Sicherheit durch Technikgestaltung ist da ein Stichwort, das relevant ist.

Was die Schulung und die Sensibilisierung angeht, so stimme ich dem voll zu, was die Anzuhörenden gesagt haben. Ich möchte nur noch einen Punkt ergänzen. Es gibt ja heutzutage auch neue Methoden mit webbasierten Angeboten am Arbeitscomputer, wo man also spielerische Angebote nutzt. Die gibt es teilweise auch schon zu kaufen. Man sollte dabei aber darauf achten, dass sie möglichst an die Arbeitsumgebung der Betroffenen angepasst werden, weil man Lust haben muss, das auch zu nutzen, denn nur dann funktioniert es. Wenn man das Gefühl hat, dass man nichts damit zu tun hat, wird das nicht aufgehen. Einfach etwas kaufen und zur Verfügung stellen, das reicht, glaube ich, nicht aus, sondern man muss es auch anpassen.

Dann möchte ich aber auch noch einen Punkt erwähnen, der heute noch nicht benannt worden ist, und das ist die Kontrolle. Bei unseren Prüftätigkeiten stellen wir immer wieder fest, dass Sicherheitskonzepte entweder gar nicht da sind oder da sind, aber nicht umgesetzt werden. Das ist ein großes Thema. Da muss der Senat noch mehr kontrollierend eingreifen, damit auch dafür gesorgt wird, dass die Sicherheitskonzepte zum einen angemessen erstellt und zum anderen auch umgesetzt und gelebt werden. Das ist eine riesige Herausforderung, die man bei der wichtigen Schulung und Sensibilisierung nicht vergessen darf. Sensibilisierung muss bei den einzelnen Nutzern ansetzen, sie muss aber auch auf den Leitungsebenen durchgeführt werden, eben im Hinblick auf Kontrolle. – Vielen Dank!

Vorsitzender Ronald Gläser: Vielen Dank, Frau Smolczyk! – Herr Kollege Ziller, bitte!

Stefan Ziller (GRÜNE): Meine erste Frage greift den von der CDU vorgebrachten Punkt mit auf: Wie weit sollte sich das Land auch im Kontext der Ebenen tatsächlich engagieren und Täter verfolgen? Welche der Fälle müssen an die Staatsanwaltschaft gehen, und wie soll das Land aktiv in den internationalen Prozess der Verfolgung von bösen Hackern einsteigen? Wie ist dazu Ihre Einschätzung? Wie viele Ressourcen sollte man da hineingeben, oder ist das das,

was die EU mit ihren Cyber-Agenturen macht oder machen sollte? Welche Aufgabe hat da aus Ihrer Sicht das Land Berlin?

Mein zweite Frage – um vielleicht auch wieder etwas zum Anfang zurückzukommen –: Wie soll das Land mit Sicherheitslücken und dem Ankauf für eigene Ermittlungsbehörden umgehen? – Jetzt ist der Innensenator selbst nicht da, und ich weiß nicht, inwieweit Sie da Auskunft geben können. Mich würde interessieren, wie Sie das einschätzen. Erhöht es die Sicherheit, wenn die öffentliche Hand selbst sozusagen Sicherheitslücken vorhält, oder ist es besser, die Sicherheitslücken dann zu melden und zu schließen? Wie sieht der Senat das? Wird in Berlin aktiv in Bezug auf Sicherheitslücken gehandelt?

Vorsitzender Ronald Gläser: Vielen Dank, Herr Ziller! – Bitte, Herr Krupka!

Daniel Krupka (Geschäftsführer der Gesellschaft für Informatik e. V.): Ich würde gern auf den letzten Punkt eingehen. Wir haben eine relativ klare Meinung dazu, und die besagt, dass der Staat sich das nicht zu eigen machen sollte, sondern die Sachen melden sollte, damit die Sicherheitslücken behoben werden können. Ich meine, wir haben bei Wanna-Cry gesehen, was passiert, wenn es der Staat nicht macht.

Vorsitzender Ronald Gläser: Vielen Dank, Herr Krupka! – Herr Dr. Löw, bitte!

Dr. Alexander Löw (Geschäftsführer der Data-Warehouse GmbH): Da kann ich eigentlich nur zustimmen. Auch als Softwarehersteller im Cybersicherheitsbereich sind wir eher der Meinung, dass es der falsche Weg ist, Sicherheitslücken einzukaufen, denn wenn Sicherheitslücken bekannt sind, dann wissen es die Hacker normalerweise auch schon, und die haben schon Geld dafür gezahlt. Das heißt, den Zeitvorsprung zum Schließen der Lücken zu nutzen – flächendeckend –, wäre wesentlich sinnvoller, als sich diese Sicherheitslücken zunutze zu machen. Das ist ein rein persönliches Gefühl aus jahrzehntelanger Erfahrung in der Softwareentwicklung und im IT-Sicherheitsbereich.

Zum zweiten Thema – Täterverfolgung –: Sie haben ja Strafverfolgungsorgane mit dem Landesamt für Verfassungsschutz und dem Bundesamt für Verfassungsschutz, die über sehr gut ausgebildete Experten verfügen, die auch das Thema Täterverfolgung durchaus durchführen können. Gerade aus Bayern heraus kann ich sagen, dass wir mit Herrn Geier öfters auch als Firma schon gute Erfahrungen gemacht. Man hat sich immer wieder ausgetauscht, und die haben auch sehr gute Experten, die auch gegenüber israelischen Experten durchaus bemerkenswerte Ergebnisse geliefert haben.

Vorsitzender Ronald Gläser: Vielen Dank! – Frau Smentek, bitte!

Staatssekretärin Sabine Smentek (SenInnDS): Ich bin natürlich nicht die Innensenatorin, und ich bin noch nicht einmal die Staatssekretärin für innere Sicherheit, aber da wir gerade beim Thema IT-Sicherheit in unseren Diskussionsrunden überhaupt nicht in Silos denken, kann ich natürlich zu den Themen etwas sagen. Es ist keineswegs so – das war vielleicht ein Missverständnis, weil wir hier heute im Ausschuss für Kommunikationstechnologie und Datenschutz sitzen –, dass das Thema „Verfolgung von Cybercrime“ irgendwie eine nachrangige Bedeutung hätte. Es ist auch nicht so, dass die Federführung dafür bei mir in der Abteilung V liegt, sondern es ist selbstverständlich so, dass es für alles, was den Bereich rund um die

Strafverfolgung von Cybercrime angeht, die Strafverfolgungsbehörden gibt. Dort gibt es extra spezielle Bereiche – auch bei der Polizei, beim Landeskriminalamt –, und ich weiß auch sehr genau, dass es einen intensiven Austausch gerade mit den Israelis an der Stelle gibt. Es gibt auch einen bundesweiten Austausch. Das heißt, das ist eine Dimension der Strafverfolgung von Cyberkriminalität, die selbstverständlich von den Berliner Sicherheitsbehörden und den Strafverfolgungsorganen ganz genauso wie überall anders auch, vielleicht sogar einen Tick besser, organisiert wird. Das würde ich jetzt mal fast behaupten. Genauer müsste dann in der Tat Herr Akmann dazu sagen. Ich weiß aber, dass es ein wirklicher Schwerpunkt seiner Arbeit ist, sich um diese Thematik zu kümmern.

Wir haben auch eine intensive Zusammenarbeit, soweit es das Thema Cyber-Sicherheit in der Berliner Verwaltung einerseits angeht – wie auch mit der zentralen Arbeitsgruppe Cyberkriminalität in der Abteilung Innere Sicherheit. Also es ist nicht so, dass da jeder aneinander vorbei agieren. Da haben wir aus vergangenen Zeiten gelernt und organisieren das jetzt tatsächlich abteilungsübergreifend und auch verwaltungsübergreifend. Den Austausch auf Bundes- und Länderebene bespielt das Land Berlin an dieser Stelle sehr aktiv.

Wir haben uns aber heute über die Fragen unterhalten, was wir jetzt noch besser machen können und welche Möglichkeiten uns das E-Government-Gesetz gibt, um nicht nur Inseln der Glückseligen – in Klammern: der Sicherer – zu schaffen, sondern möglichst die Flächendeckung hinzubekommen. Dazu hatte Frau Fiedler eben auch noch mal gesagt, dass wir tatsächlich noch das Risiko der veralteten Technik haben, was wir aber durch die notwendigen Investitionen und den zentralen Betrieb beim ITDZ abmildern wollen.

Ich würde aber gern noch mal an einem Punkt ansetzen, den Frau Smolczyk angeführt hat – das Thema Kontrolle. Sie haben, glaube ich, dieser Tage den IT-Sicherheitsbericht erhalten. Mich haben schon erste Rückfragen dazu erreicht, wie es denn sein kann, dass der so aussieht. Wir haben in diesem Sicherheitsbericht – ich nehme an, den werden wir hier auch noch diskutieren – ein Symptom zu bemerken, dass wir nämlich in der Tat, bevor wird das E-Government Gesetz mit all seinen Kontrollmöglichkeiten hatten, nicht die Möglichkeit hatten, in allen Behörden das Thema IT-Sicherheit in der Tiefe zu verankern, wie wir es gerne hätten. Mit den Möglichkeiten des E-Government-Gesetzes, die mir wirklich so etwas wie die Richtlinienkompetenz und auch die Kontrollkompetenz an der Stelle geben, ist verbunden, dass der nächste IT-Sicherheitsbericht, den wir Ihnen vorlegen, völlig anders aussehen wird, und zwar nicht nur formal vom Aufbau her, sondern auch von den Inhalten her.

Ich habe gehört, dass sich das in den Behörden schon herumspricht, was ich sehr gut finde. Mir geht es in dem Bericht doch nicht darum, jemand mit irgendwelchen Schwachstellen vorzuführen, sondern viel lieber wäre es mir doch, wenn wir im nächsten IT-Sicherheitsbericht bessere Ergebnisse für die IT-Sicherheit hätten. Deswegen reden Sie darüber, dass wir den IT-Sicherheitsbericht völlig ändern und unsere Kontrollmöglichkeiten ausschöpfen werden, und vielleicht führt das auch dazu, dass im Vorwege die eine oder andere Verwaltung ihre Schwerpunkte noch ein wenig überdenkt. Das würde mich sehr freuen, denn mir geht es nicht um das Bloßstellen, sondern um die Verbesserung der IT-Sicherheit im Land Berlin. Ich glaube, das eint uns alle.

Vorsitzender Ronald Gläser: Vielen Dank, Frau Smentek! – Damit können wir die Aussprache beenden, und ich möchte mich bei den Experten noch einmal ganz herzlich bedanken!

– Der Tagesordnungspunkt wird jetzt vertagt. Zum Thema der IT-Sicherheitsschulung werden wir möglicherweise in der Sitzung am 9. Februar 2018 von Ihnen, Frau Smentek, mehr erfahren – hinsichtlich einer möglichen Kontrolle, so wie Herr Kollege Kohlmeier das vorgeschlagen hat. – Vielen Dank!

Punkt 3 der Tagesordnung

Vorlage – zur Beschlussfassung –
Drucksache 18/0365

**Gesetz zum Zweiten Staatsvertrag zur Änderung des
Staatsvertrages über das Gemeinsame Krebsregister
der Länder Berlin, Brandenburg, Mecklenburg-
Vorpommern, Sachsen-Anhalt und der Freistaaten
Sachsen und Thüringen**

[0025](#)
KTDat
GesPflGleich(f)
Haupt

Siehe Inhaltsprotokoll.

Punkt 4 der Tagesordnung

Verschiedenes

Siehe Beschlussprotokoll.