Abgeordnetenhaus BERLIN

19. Wahlperiode

Plenar- und Ausschussdienst

# Wortprotokoll

Öffentliche Sitzung

**Ausschuss für Inneres, Sicherheit und Ordnung**

27. Sitzung
11. Dezember 2023

Beginn: 09.00 Uhr
Schluss: 12.26 Uhr
Vorsitz: Florian Dörstelmann (SPD)

Vor Eintritt in die Tagesordnung

Siehe Beschlussprotokoll.

Punkt 1 der Tagesordnung

**Besondere Vorkommnisse**

Siehe Inhaltsprotokoll.

Punkt 2 der Tagesordnung

Antrag der Fraktion Bündnis 90/Die Grünen — 0118
Drucksache 19/1054 — InnSichO
**Gerechte und rechtmäßige Entlohnung für Objektschützer*innen des Landes Berlin** — Haupt

Siehe Inhaltsprotokoll.

**Vorsitzender Florian Dörstelmann:** Ich rufe auf

Punkt 3 der Tagesordnung

Besprechung gemäß § 21 Abs. 3 GO Abghs 0113
**Schutz vor Cyberangriffen: Stand und Entwicklungen** InnSichO
(auf Antrag der Fraktion Bündnis 90/Die Grünen)

Hierzu erfolgt eine Anhörung, zu der ich ganz herzlich an dieser Stelle die drei Anzuhörenden begrüßen darf, Frau Caroline Krohn, Herrn Manuel Atug und Herrn Dr. Sven Herpig. – Herzlichen Dank, dass Sie uns heute hier als Anzuhörende mit Ihrer Expertise zur Verfügung stehen! Ich darf noch anmerken, zu welchen Einrichtungen Sie gehören: Herr Manuel Atug gehört zur Arbeitsgemeinschaft Kritische Infrastrukturen, AG KRITIS, Herr Dr. Sven Herpig ist Leiter der Abteilung Cybersicherheitspolitik und Resilienz der Stiftung Neue Verantwortung e. V. und Frau Caroline Krohn ist in der Arbeitsgemeinschaft Nachhaltige Digitalisierung, AGND, als Expertin tätig. – Vielen Dank, dass Sie heute hier sind!

Wir haben unsere Anzuhörenden heute aus verschiedenen Gründen digital zugeschaltet, einmal natürlich wegen der Gesundheitssituation, die allgemein bekannt ist, und zweitens war auch das Wetter in der vergangenen Woche nicht so ermunternd, dass wir gesagt hätten, es ist zwingend erforderlich und zumutbar, dass Sie hierherkommen. Es ist sehr schön, dass Sie uns auch auf diesem Wege zur Verfügung stehen.

Ich denke, an dieser Stelle darf ich auch Herrn Waniek ganz herzlich begrüßen, den Landesbevollmächtigten für die Informationssicherheit, der zwar nicht als Anzuhörender, sondern als Mitglied der Administrative zur Verfügung steht, aber voraussichtlich in ähnlicher Form hier befragt und Stellung nehmen wird.

Ich gehe davon aus, dass die Anfertigung eines Wortprotokolls nach § 26 Absatz 7 Satz 4 der Geschäftsordnung des Abgeordnetenhauses gewünscht wird. – Das ist der Fall. Dann verfahren wir so und kommen nun zur Begründung des Antrags, falls eine solche gewünscht wird. – Selbstverständlich ist das der Fall. – Herr Abgeordneter Franco für Bündnis 90/Die Grünen, Sie haben das Wort!

**Vasili Franco** (GRÜNE): Vielen Dank, Herr Vorsitzender! – Vielen Dank auch, dass wir hier die Möglichkeit bekommen, eine Anhörung zu diesem Thema durchzuführen. Wir diskutieren in diesem Ausschuss über sehr viele Straftaten, die in Berlin so passieren. Meistens geht es um Parks, Schwimmbäder, darum, was auf den Straßen so los ist. Was man nicht ganz so oft sieht, aber auch eine Realität ist, ist alles, was im Netz passiert, und das ist etwas, was auch stärker in den Fokus der Innenpolitik geraten muss. Die Cybersicherheit wird immer so abstrakt dargestellt, dabei kann man sie sehr konkret machen; allein dieses Jahr hatten wir beispielsweise im Oktober Angriffe auf das Berliner Naturkundemuseum; die Hunderte von Mitarbeitern konnten nicht mehr arbeiten, die Website war über längere Zeit nicht zugänglich. Ähnliche Angriffe mit anderen und langen Folgen gab es auch beim Helmholtz-Zentrum und der Technischen Universität. Dabei gab es auch Abgriffe von sensiblen Daten. Wir alle erinnern uns, glaube ich, auch noch an die Situation beim Berliner Kammergericht, das durch den Trojaner Emotet lahmgelegt wurde und wo man festgestellt hat, dass die IT-Infrastruktur dort komplett und hoffnungslos überaltert war. Auch Angriffe auf das Hauptstadtportal Berlin.de

sind inzwischen schon fast eine Alltäglichkeit, auch da gab es in letzter Zeit Vorfälle, bei denen Daten abgegriffen worden sind. Natürlich kann das noch viel gefährlicher werden, wenn es um kritische Infrastruktur geht, also um Energie- und Wasserversorgung.

Meine Kollegin Frau Ahmadi hat das Thema schon im Ausschuss für Digitalisierung und Datenschutz aufgerufen. Vielleicht ist es gut, dass es hier noch mal ein bisschen mehr Aufmerksamkeit erlangt, denn der Schutz vor Cyberangriffen ist ein Zusammenspiel einmal aus Cybersicherheit, die auch durch staatliche Institutionen und die Sicherheitsbehörden sichergestellt werden muss und kann, und die Frage der IKT-Sicherheit, also: Wie sind eigentlich unsere Behörden, unsere staatlichen Institutionen und genauso unsere kritische Infrastruktur vorbereitet auf all das, was über das Netz passieren kann? Wie können wir uns hier so wappnen, dass Angriffe nicht nur jederzeit abgewehrt werden können, sondern man auch die angreifenden Strukturen dahinter ausmacht?

Hier geht es auch darum, dass wir sehen, dass wir sehr viele internationale Bezüge haben, das heißt, auch Nachrichtendienste nutzen explizit Cyberangriffe als Mittel der modernen Kriegsführung, durchaus auch, um in Krisenzeiten noch mehr Verunsicherung zu schaffen, staatliche Institutionen zu destabilisieren und diese natürlich unter Druck zu setzen. Denn wenn einmal die eigene Behörde nicht mehr läuft, weil man keine E-Mails mehr lesen kann, Homepages nicht mehr aufrufbar sind, dann liegt der komplette Staat an der Stelle flach. Das darf nicht passieren. Bisher hatten wir zum Glück noch keine so großen relevanten Vorfälle, dass man sagen musste: Berlin war völlig lahmgelegt –, aber wir hatten sie, wie gesagt, schon im Kleinen.

Das wollen wir uns heute näher ansehen. Wir freuen uns auf die Expertise der eingeladenen Anzuhörenden, die in diesem Bereich auch schon bekannt sind, unterschiedliche Perspektiven einbringen und vielleicht uns auch noch mitgeben können: Welche Möglichkeiten haben wir als Landespolitikerinnen und Landespolitiker, diesem Thema ausreichend Geltung zu geben und sowohl personell, finanziell, haushälterisch und technisch die notwendigen Voraussetzungen zu schaffen, damit das Land Berlin gut geschützt und sicher mit Cyberangriffen umgehen und diese bestenfalls auch da, wo möglich und nötig, entsprechend verfolgen kann. – Vielen Dank!

**Vorsitzender Florian Dörstelmann:** Vielen Dank, Herr Abgeordneter Franco! – Wir hören dann zunächst die Stellungnahmen der Anzuhörenden, und in der Folge besteht für alle Mitglieder des Ausschusses die Möglichkeit, Fragen zu stellen und entsprechende Erörterungsrunden zu eröffnen. Ich darf die Anzuhörenden in alphabetischer Reihenfolge aufrufen. Das wäre dann zunächst Herr Atug. – Herr Atug, bitte, Sie haben das Wort!

**Manuel Atug** (AG KRITIS) [zugeschaltet]: Vielen lieben Dank für die Einladung! – Mein Name ist Manuel Atug, ich bin in diesem Internet auch aktiv als HonkHase. Ich berate und prüfe kritische Infrastrukturen und bin seit weit über 23 Jahren in der Cybersicherheit tätig. Wer ist die AG KRITIS? – Kurz zur Einordnung: Unsere Arbeitsgruppe ist vollständig unabhängig von Staat oder Wirtschaft. Wir vertreten keine Interessen von Unternehmen oder Wirtschaftsverbänden. Unser Ziel ist einzig und allein, die Versorgungssicherheit der Bevölkerung zu erhöhen. Wir sind ungefähr 42 Fachleute, die sich täglich, durchaus auch beruflich, mit kritischen Infrastrukturen beschäftigen. Wie gesagt, unser Engagement ist getrieben von der Motivation, unabhängig von wirtschaftlichen Interessen eine nachhaltige Verbesserung der

IT-Sicherheit kooperativ mit allen Beteiligten herbeizuführen. Insofern eint unsere Gruppe, dass wir durch unsere Arbeit unabhängig voneinander zu dem Schluss gekommen sind, dass die Ressourcen der Bundesrepublik zur Reaktion auf Großschadenslagen beispielsweise durch Cybervorfälle im Bereich der kritischen Infrastruktur nicht ausreichen, um die Auswirkungen der dadurch verursachten Krisen und Katastrophen zu bewältigen.

Ich fange mit dem Koalitionsvertrag an. Da steht – Zitat –:

> Gerade die Hauptstadt Berlin benötigt einen erhöhten Sicherheitsstandard. Die Digitalisierung von Dienstleistungen erfordert ein hohes Niveau der digitalen Sicherheit durch eine ganzheitliche Umsetzung von Informationssicherheit und Cybersicherheit als Grundlage von Vertrauen in digitale Dienstleistungen für Bürgerinnen und Bürger sowie für die Wirtschaft.

Das klingt erst mal gut. Wenn man sich die Sicherheitslage im Land Berlin von außen betrachtet anschaut, gibt es allerdings durchaus Beispiele wie die Softwarekomponente Microsoft Windows: Anfang 2023 waren wohl noch Windows Server 2008 R2 im Einsatz, die am 10. Januar 2023 aus dem sogenannten ESU-Support herausgefallen sind. Der Landesbevollmächtigte für Informationssicherheit, Herr Waniek, hat wohl am 13. Januar ein Schreiben verschickt, in dem er auf das Supportende des Betriebssystems hinwies. Dort hat es dann geheißen, der Weiterbetrieb der Server „ist im Sinne einer Schwachstelle mit höchster Kritikalität zu bewerten“, ein Wechsel auf eine laut den geltenden Vorschriften des Landes zulässige Systemversion sei „unverzüglich erforderlich“. – Das kann ich nur begrüßen. Noch besser wäre gewesen, vorab rechtzeitig zu migrieren und solche Aussagen wie im Koalitionsvertrag ernst zu nehmen und zu sagen: Wir kümmern uns vorab um Sicherheit und nicht, wenn der Drops gelutscht ist.

Anmerkungen dazu: Anfang Januar sind circa 800 Geräte mit Windows Server 2012 vorhanden gewesen, die nur noch bis Oktober dieses Jahres Updates erhalten haben. Wie der Stand da ist, ist nach außen hin nicht transparent.

Wie steht es um kritische Infrastrukturen in Berlin? – Die AG Cybersicherheit befindet sich im Referat III A der Abteilung III, hat dazu eine Website aufgesetzt und listet alle relevanten Gesetzgebungen unter Berlin.de auf. Das sind allerdings die EU- und bundesdeutschen Vorgaben; nicht adressiert werden die beiden landeshoheitlichen Sektoren, nämlich der Sektor Staat und Verwaltung und der Sektor Medien und Kultur. Der Staat sollte stringenter und rigider sein, weil der Hebel des Bußgeldes nicht da ist. Aktuell macht der Staat – so, wie wir es fordern – weniger als die KRITIS-Betreiber, und das kann eigentlich nicht sein. Die Lösung der AG KRITIS wäre, eine KRITIS-Verordnung für das Land Berlin zu erlassen, so wie sie auch jedes andere Bundesland benötigt und umsetzen muss. Alternative konkrete Lösung, wenn man nicht anlassunbezogen eine KRITIS-Verordnung erlassen möchte: Die NIS2-EU-Gesetzgebung wird ab Oktober nächsten Jahres verbindlich. Auch da könnte man die Bundesländer einspannen und Kommunen und Landkreise und alles andere integrieren. Leider hat der IT-Planungsrat beispielsweise einen offiziellen Beschluss gefasst und gesagt: Wir raten dem Bund und den Bundesländern, lieber nicht Kommunen und Landkreise und dergleichen in die NIS2-Gesetzgebung aufzunehmen. Warum? – Das hat er nicht kundgetan, aber es geht um Kosten und Verantwortung; beides ist schwierig, und darunter leidet man.

Der Sektor Staat und Verwaltung, um es klarzumachen, enthält derzeit gemäß der Bundesdefinition, die man auf den Webseiten des BBK – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe – finden kann: Parlament, also Legislative, Regierung und Verwaltung, also Exekutive, Judikative und Justizeinrichtungen und das Notfall- und Rettungswesen einschließlich Katastrophenschutz. – Der Sektor Medien und Kultur enthält zusätzlich in der offiziellen Definition Archive, Bibliotheken und Museen – Museen wie das Landesmuseum.

Was wir also benötigen, ist diese KRITIS-Verordnung auf Landesebene. Wir benötigen darüber hinaus Weiterbildung. Wir brauchen administrative Arbeitsplätze und Stellen, und wir brauchen vernünftige Hardware, die das leisten kann, was die Software fordert.

Die Onlineterminvergabe, also das Brot-und-Butter-Digitalisierungsgeschäft, sollte ohne Medienbrüche statt beispielsweise mit Glitzer und Hype wie KI- und Startup-Kruscht irgendwie umgesetzt werden. Dass wir inzwischen immerhin einen Capture eingeführt haben im Jahr 2023, begrüße ich sehr; das haben viele andere schon seit Jahrzehnten im Einsatz. Insofern kommen wir da vielleicht mal dazu, dass das Brot-und-Butter-Digitalisierungsgeschäft auch bewerkstelligt werden kann.

Das Cyber-Hilfswerk, ein Konzept der AG KRITIS auf Bundesebene, befindet sich derzeit als Machbarkeitsstudie im THW, wo ein Cyber-Hilfswerk bei Amtshilfeverfahren, wenn es digitale Katastrophen gibt, zu Hilfe kommt. Das würde auch dem Land Berlin sehr helfen, insofern können wir auch nur empfehlen, da dranzubleiben.

Noch mal etwas zum aktuellen Stand, wie Cybersicherheit in Berlin derzeit von außen wirkt: Es gibt eine Leitlinie des Landes Berlin zur Informationssicherheit, da steht unter „Informationssicherheitsstrategie“: „Die Informationssicherheit wird im Land Berlin unter Einsatz und auf Grundlage der IT-Grundschutzmethodik des BSI gewährleistet.“ – Okay, so weit so gut; darauf kommen wir nachher noch zurück. Unter anderem sieht sie „Datenminimierung“ als Leitziel vor. Wie ist das vereinbar mit KI- und Big-Data-Initiativen, die da alle angegangen werden sollen und wollen? Die „Einbindung aller Beschäftigten“ steht drin. Das geschieht unserer Meinung nach unzureichend, denn der Mangel an Digitalisierungs- und Medienkompetenz ist definitiv bemerkbar. Die „zentrale Rolle der Informationssicherheit“: Uns bleibt die leider unklar und ist nicht ausgeprägt sichtbar.

IT-Sicherheitskonzepte sollen anscheinend auf Basis veralteter BSI-Grundschutzstandards 100-1 bis -4 statt der aktuellen 200-1 bis -4 gemacht werden, denn so steht es in der Leitlinie drin. Diese Standards des BSI wurden übrigens vor sechs Jahren auf die 200-er Version angehoben. In der Schlussbestimmung steht allerdings:

> Diese Leitlinie zur Informationssicherheit tritt am 21.09.2017 in Kraft. Im Rahmen des Informationssicherheitsprozesses wird diese Leitlinie zur Informationssicherheit regelmäßig (bei wesentlichen Änderungen von in der Leitlinie benannten Referenzdokumenten

– zum Beispiel vor sechs Jahren –

> und mindestens alle zwei Jahre)

– also vor sechs, vier, zwei Jahren und jetzt –

> auf ihre Aktualität hin geprüft und ggf. aktualisiert.

Die Leitlinie im Land Berlin ist also von 2017 und soll alle zwei Jahre nach Bedarf aktualisiert und geprüft werden. Sie ist leider veraltet und basiert auf den Grundschutzstandards 100-

1 bis -4, statt 200-1 bis -4, die vor sechs Jahren erneuert wurden. Die AG KRITIS denkt, das spricht für sich.

Wir haben im Webportal im Bereich Moderne Verwaltung unter „Aktuelles aus der Informationssicherheit“ gerade zwei Einträge stehen: „In Zeiten von Viren – Keine IKT-Infekte riskieren!“ und den Eintrag „Emotet – oder wie Cyber-Kriminelle Computersysteme lahmlegen“. Das war es. Mehr gibt es da nicht an Informationen, und beides ist auch durchaus etwas älter.

Daher noch mal: Der Staat sollte stringenter und rigider sein, weil der Hebel des Bußgeldes nicht da ist. Aktuell macht der Staat aber weniger als die KRITIS-Betreiber. Das kann einfach so nicht sein. NIS2 sollte daher als Basis genutzt werden und auch für Bundesländer, Kommunen und Landkreise et cetera gelten. Staat und Verwaltung in die KRITIS-Verordnung aufnehmen, Medien und Kultur ebenfalls aufnehmen. – Vielen lieben Dank!

**Vorsitzender Florian Dörstelmann:** Vielen Dank, Herr Atug! – Dann hören wir als Nächsten Herrn Dr. Herpig. – Bitte, Herr Dr. Herpig, Sie haben das Wort!

**Dr. Sven Herpig** (Stiftung Neue Verantwortung e. V.) [zugeschaltet]: Vielen Dank! Vielen Dank für die Einladung! – Sehr geehrter Herr Ausschussvorsitzender! Sehr geehrte Abgeordnete! Sehr geehrte Sachverständige! Sehr geehrte Zuschauende! Die IT-Sicherheit ist eine der Grundlagen für eine funktionierende Digitalisierung der Verwaltung, damit verbunden natürlich auch das Vertrauen von Wirtschaft und Gesellschaft in den Staat. Gleichzeitig ist laut unseren Bundessicherheitsbehörden die Bedrohungslage in und aus dem Cyberraum so hoch wie nie zuvor.

Die Lage in Berlin wird kaum anders sein als die Lage in Gesamtdeutschland, aber so richtig mit Genauigkeit wissen wir das nicht. Während jede und jeder hier von den Vorfällen um Berlin.de und das KaDeWe, das Kammergericht und das Museum weiß, fehlt es an einem umfassenden Lagebericht für das Land Berlin. Ein solcher Lagebericht zur Cybersicherheit, der Kriminalität, Spionage und andere böswillige Aktivitäten aus dem und im Cyberraum zusammenfasst und analysiert, wäre jedoch notwendig, um entsprechende Handlungsoptionen abzuleiten. Kurzum: Ohne zu wissen, was gerade wirklich passiert, kann man nicht zielführend reagieren und noch viel weniger strategisch planen.

Für einen solchen Lagebericht braucht es jedoch weitere Voraussetzungen. Ein Lagebericht ist nur dann gut, wenn die Datengrundlage solide ist. Um eine bessere Datengrundlage zu bekommen, müssten Unternehmen – über die KRITIS-Unternehmen hinaus – verpflichtet werden, IT-Sicherheitsvorfälle zu melden. Ausnahmen für Kleinstunternehmen muss es dann genauso geben wie niedrigschwellige Meldemöglichkeiten mit ausreichenden Fristen für Unternehmen, die keine kritischen Dienstleistungen erbringen. Meldungen können zum Beispiel über die Digitalagentur erfolgen, damit nicht jedes Mal zwingend das Legalitätsprinzip zum Zuge kommen muss, was bei Meldungen an die Polizeien der Fall wäre. Wenn die Vergangenheit ein Anhaltspunkt ist, wird es nicht zu viel führen, hier auf Freiwilligkeit zu setzen.

Eine weitere Voraussetzung für einen sinnvollen Lagebericht ist eine zentrale staatliche Stelle, bei der Informationen zusammenlaufen und wo sie ausgewertet werden können, eine operative Stelle also. In Berlin würde sich hierfür vor allem das Landeskriminalamt mit seiner

Zentralen Ansprechstelle Cybercrime oder das Cyber Defence Center in der Landesverwaltung Berlin mit seinem Security Operations Center und dem Computer Emergency Response Team anbieten.

**Vorsitzender Florian Dörstelmann:** Herr Dr. Herpig! Darf ich Sie ganz kurz unterbrechen? Wir müssen das hier technisch noch etwas besser aussteuern, weil Sie nicht so gut zu verstehen sind. Erlauben Sie bitte, dass wir eine kurze Sekunde der Anpassung einfügen, damit Ihr Beitrag hier noch besser zu verstehen ist. – Vielen Dank, Herr Dr. Herpig!

**Dr. Sven Herpig** (Stiftung Neue Verantwortung e. V.) [zugeschaltet]: Gut, dann mache ich weiter! – Das Cyber Defence Center wäre dann eine gute Wahl, wenn man breiter als nur über Cyberkriminalität nachdenken möchte, was definitiv anzuraten wäre. Zweifelsohne müssten an dieser Stelle noch weitere Befugnisse geschaffen werden, vor allem, wenn man zum Beispiel zukünftig ein mobiles Vorfallbearbeitungsteam, ein Mobile Incident Response Team schaffen möchte. Die zentrale staatliche Stelle für Cybersicherheit in Berlin könnte dann auch über andere staatliche Stellen auf Bundes- und Länderebene hinaus mit Akteuren aus Wirtschaft, Wissenschaft und Zivilgesellschaft Sicherheitspartnerschaften bilden, um zum Beispiel gemeinsam Cybersicherheitsübungen durchzuführen.

Sowohl die Vorfallmeldepflicht für Unternehmen und weitere Organisationen als auch die Benennung einer zentralen Stelle für Cybersicherheit in Berlin mit gegebenenfalls weiteren Befugnissen wird einen Rechtsakt erfordern. Dieser wird gegebenenfalls auch deswegen unumgänglich werden, weil sich der IT-Planungsrat dagegen entschieden hat, Kommunen über die Umsetzung der Europäischen Richtlinie über Maßnahmen für ein hohes gemeinsames Sicherheitsniveau mit einer rechtlichen Basisabsicherung zu versehen; das hat der Sachverständige Manuel Atug gerade bereits angemerkt. Ob die Berliner Bezirke unter diese Regulierung fallen oder nicht, ist meines Erachtens noch nicht ganz final geklärt. Unabhängig davon sind die Bezirke aber neben der Wirtschaft diejenigen Akteure, die am meisten unter der aktuellen Bedrohungslage leiden. Gleichzeit ist das Funktionieren der Bezirke im Rahmen der Digitalisierung der Verwaltung elementar. Da die Bezirke vernetzt sind, braucht es ein einheitliches IT-Sicherheitsniveau für alle Bezirke in Berlin, oder kurzum: Berlin braucht zeitnah ein IT-Sicherheitsgesetz oder Ähnliches.

Der Entwurf eines IT-Sicherheitsgesetzes für Berlin, die Überführung des Lagebilds und konkrete Handlungen zur Verbesserung der IT-Sicherheit, die klare Benennung und der Ausbau einer zentralen staatlichen Stelle für Cybersicherheit in Berlin sowie die Anbindung an andere Länder und den Bund mit seiner möglichen Zentralstellenfunktion beim Bundesamt für Sicherheit in der Informationstechnik obliegt der Senatsverwaltung für Inneres und Sport, dort vermutlich der Arbeitsgruppe Cybersicherheit.

Ich möchte mit einem Appell für die Fachkräfteausbildung schließen, denn all die genannten Maßnahmen können nur dann vom Reißbrett in die Realität transportiert werden, wenn Wirtschaft und Staat ausreichend qualifizierte Menschen haben, die operativ tätig werden können. Während maschinelles Lernen hierbei unterstützen kann, wird uns künstliche Intelligenz nicht retten. Laut der Cybersecurity-Workforce-Studie fehlen in Deutschland derzeit 100 000 Fachkräfte in diesem Bereich der IT- und Cybersicherheit. Hinzu kommen Qualifikationslücken zum Beispiel bei digitaler Forensik. Berlin sollte die Aus-, Um- und Weiterbildung bei IT-

Sicherheit zu einer Priorität machen. Die Grundlagen dafür hat Berlin als starker Wissenschafts- und Industriestandort für Informationstechnologien allemal. – Vielen Dank!

**Vorsitzender Florian Dörstelmann:** Vielen Dank, Herr Dr. Herpig! – Dann kommen wir zu Frau Krohn. – Bitte, Frau Krohn, Sie haben das Wort!

**Caroline Krohn** (AGND) [zugeschaltet]: Einen ganz herzlichen Dank! – Sehr geehrter Herr Ausschussvorsitzender! Sehr geehrte Abgeordnete! Ich bedanke mich sehr für die Einladung und fürs Hören der AG Nachhaltige Digitalisierung. Die AG Nachhaltige Digitalisierung beschäftigt sich nicht, wie so oft bei Nachhaltigkeit suggeriert, mit Abwärme von Rechenzentren und der Kreislaufwirtschaft, die auch ins Digitale greifen soll. Bei aller Wichtigkeit dieser Themen haben wir einen deutlich breiteren Nachhaltigkeitsbegriff, der vor allen Dingen den Kern in der IT-Sicherheit findet, weil uns das Hauptanliegen treibt, Menschen zu schützen, wenn wir digitalisieren. Das bedeutet, dass wir über den Anspruch einer guten Digitalisierung hinaus versuchen, eine Qualitätsebene in die Digitalisierung zu bringen, und die besteht aus unserer Sicht vor allen Dingen darin, dass Menschen, die digitalisieren, oder Projekte, die zur Digitalisierung all unserer Lebensbereiche führen, auch einem bestimmten Qualitätsstandard genügen. Wir haben uns mit der AG Nachhaltige Digitalisierung sehr darum bemüht zu schauen, dass wir uns zu frühen Zeiten Gedanken über die soziotechnische Folgenabschätzungen jedweder digitalen Maßnahmen machen, und da haben wir schon unterschiedliche Kriterien ausgemacht, nach denen wir die Nachhaltigkeit von Digitalprojekten ausmachen und erarbeiten wollen.

In diesem Kontext werden wir zu vielen Dingen befragt – von inwieweit der Nachhaltigkeitsaspekt, den wir meinen, bei autonom fahrenden Staubsaugern in Wohnungen gewährleistet ist bis hin zu Digitalprojekten der öffentlichen Hand und der öffentlichen Verwaltung. Das ist auch der Grund, warum wir hier schon direkt ansetzen können. Wir haben zur Anhörung keine sehr spezifische Frage erhalten als Sachverständige; ich glaube, das trifft auf uns alle zu. In den Punkten, die vorhin von den beiden anderen sehr geschätzten Sachverständigen schon geäußert wurden, gehen wir als AG Nachhaltige Digitalisierung übrigens komplett mit. Damit für Sie, die uns hier online zuhören, vielleicht noch mal eine Brücke gebaut wird, habe ich mich entschlossen zu versuchen, Ihnen ein gewisses Sicherheitsmindset nahezubringen. Wir haben es hier mit einer nicht nur rechtlichen und schon gar nicht mit einer nur technischen Aufgabe zu tun, sondern es ist im Prinzip eine Frage, wie wir Digitalisierung in Zukunft gestalten wollen und welche Kultur wir dieser Digitalisierung mitgeben wollen. Deswegen ist es wahrscheinlich kein Zufall, dass wir vom Ausschuss für Inneres eingeladen wurden. Ich hoffe, dass die Kollegen vom Ausschuss für Digitales und Datenschutz inzwischen auch eingetroffen sind. Wir begrüßen natürlich sehr, dass es für diesen Tagesordnungspunkt eine Zusammenlegung gegeben hat.

Uns ist vor allen Dingen wichtig, Ihnen mitzugeben, dass Digitalisierungen, wie im Koalitionsvertrag und auch auf den Webseiten Ihrer Landesregierung schon sehr deutlich gemacht wurde, große Chancen bergen, sowohl für die öffentliche Verwaltung als auch für die wirtschaftlichen Projekte, die Sie vor sich haben. Entscheidend ist vor allen Dingen, dass wir hier darauf schauen, dass wir sehr frühzeitig gucken, dass möglichst viele Rechtslagen eingebunden sind, die im Verlauf sind. Wir bemühen uns natürlich sehr um ein IT-Sicherheitsgesetz – das ist vollkommen richtig, ich begrüße auch diese Ambition –, allerdings muss man dazu natürlich auch sagen, wie Herr Atug und Herr Herpig auch schon darauf hingewiesen haben,

es gibt natürlich viele Standards, deren Ausführungen einen gewissen Raum für Sicherheit bringen, auch für das Land Berlin. Das ist einerseits deutlich bei den Berichten, die uns auch in der Community für IT-Sicherheit immer erreichen, aber es erreichen uns nebenbei auch die Vorhaben, bei denen sehr deutlich ist, dass, wenn Sicherheit überhaupt Erwähnung findet, diese Erwähnung nicht in den Gesamtkontext eingebettet ist, und das erfüllt uns natürlich mit Sorge. Es gibt verschiedene Stellen, bei denen bereits Security by Design gefordert worden ist; das ist allerdings ein hehrer Wunsch, wenn im Koalitionsvertrag allenfalls nach Dutzenden von Seiten zur Verwaltungsdigitalisierung und Dutzenden von Seiten zur Start-up- und Wirtschaftsförderung ein einziger Satz zum Thema Sicherheit vorkommt und gleichzeitig aber in den innenpolitischen Absätzen ganz viel über Menschenschutz geredet wird. Das passt nicht zusammen. Deswegen plädieren wir dafür, dass wir eine integrierte Sicht in die IT-Sicherheit bringen zum Zwecke des Menschenschutzes.

An der Stelle habe ich noch ein weiteres Beispiel für Sie. Wir haben uns natürlich die polizeikriminologischen Statistiken und Berichte angeschaut und haben festgestellt, dass dort unter Cybercrime sehr viele Betrugsfälle im Bereich E-Commerce zu verzeichnen sind und allenfalls noch in einigen Erläuterungen Identitätsdiebstähle. Damit erschöpft sich aber das Risikoprofil für Cybersicherheit keineswegs. Wir müssen uns nicht nur fragen, wann und wie man betrogen werden kann, wenn man sich in einem kommerziellen Akt befindet, sondern das, worum es aus unserer Sicht eigentlich geht, ist eine Bedrohung der persönlichen Unversehrtheit, der psychischen und physischen Unversehrtheit auch für vulnerable Gruppen, die immer betroffen sind. Das sind ärmere Menschen, die sich häufig nicht mal Privatsphäre leisten können, weil Privatsphäre auch immer mit einem finanziellen Aufwand verbunden ist; das sind auch Gruppen, die an bestimmten Stellen verfolgt werden von bestimmten Gruppen, die derzeit auch unsere Demokratie angreifen. Das ist der Grund, warum wir uns eben nicht nur fragen sollten, inwieweit Cybersicherheit ein Problem darstellt, das entweder von organisierter Kriminalität ausgeht oder, wie Sie eben auch schreiben, zu 76 Prozent aus dem Ausland generiert wird, sondern wir müssen uns leider auch immer Fragen, inwieweit Übergriffe des Staates oder die Gesetzgebung in der Innenpolitik, die vermeintlich zum Schutz von Bürgerinnen und Bürgern gedacht sind, tatsächlich aber die Gefährdung im Cyberraum erhöhen, hier auch Eingang finden in Ihre Gesetzgebung, in Ihre Sichtweisen des Menschenschutzes.

Ein Beispiel dafür ist das ganze Thema Vorratsdatenspeicherung, das das Bundesinnenministerium infolge der Innenministerkonferenz gestern wieder zur Sprache gebracht hat, die natürlich per se verneint ist, aber doch wieder zur Sprache gekommen ist, weil es da vermeintlich nur um die Sicherung der IP-Adressen geht, wobei der EuGH auch schon längst bemängelt hat, dass IP-Adressen selbst personenbezogene Daten sind. Beispielsweise – das habe ich aus Berlin noch nicht gehört, ich weiß nicht, ob Sie das erwägen, aber aus Hessen, wo ich herkomme oder Hamburg, Bayern oder Nordrhein-Westfalen – ist Palantir ein bereits getestetes Unternehmen, das für die Polizeiarbeit installiert wird, das ganz deutlich den Menschenschutz gefährdet. Auch hier appelliere ich an den Ausschuss für Inneres, die Gesetzgebung einer Technologiefolgeabschätzung zu überprüfen, denn digitale Rasterfahndung ist keinen Deut besser als die Rasterfahndung, die wir aus den Sechzigerjahren schon kennen. Das hat das Bundesverfassungsgericht auch schon beschlossen und Hessen das Gesetz zur Überprüfung zurückgegeben. Ich rechne damit, dass das noch mal passieren wird und auch in Bayern nicht ohne Folgen bleiben wird, dass die Testverfahren schon mit Realdaten passieren.

Wie gesagt, das haben wir bisher aus Berlin noch nicht verlauten hören, aber wenn es um die Modernisierung der Polizeiarbeit geht, dann ist auch ganz häufig künstliche Intelligenz mit in den Schriftstücken, die das Land herausgibt, und davor möchten wir eindringlich warnen; das aber nicht, weil wir eine grundsätzliche Skepsis der staatlichen Hand gegenüber haben. Im Gegenteil: Die AG Nachhaltige Digitalisierung hat sich ganz deutlich zur rechtskonformen Umsetzung von Digitalisierung ausgesprochen, und die Rechtskonformität ist nicht nur einer der Leitsprüche unserer Arbeit, die sich ganz häufig beispielsweise in der DSGVO, in Zukunft sicherlich auch bei NIS2 und dem AI-Act niederschlagen wird, sondern wir sind auch für eine sehr starke Rechtsdurchsetzung der Bestandsgesetze, die wir hier haben. Auch hier appelliere ich an das Land Berlin und an den Innenausschuss und den Digitalisierungsausschuss, einmal sehr deutlich zu gucken, wie auch in den eigenen Ambitionen der Digitalisierung und Digitalisierungsförderung die bereits bestehenden IT-Sicherheits- und Datenschutzgesetze zum Zwecke des Menschenschutzes schon Berücksichtigung gefunden haben. – Soweit vielleicht zur Einführung. Für Fragen stehe ich selbstverständlich gern zur Verfügung.

Eine Antwort noch ganz kurz auf die Frage des Abgeordneten Franco von Bündnis 90/Die Grünen. Sie haben gefragt, welche Möglichkeiten wir personell, finanziell, technisch und haushälterisch sehen. – Wir sind sicher als Sachverständige nicht in der Position, Ihre haushaltspolitischen Fragestellungen zu beantworten, aber so viel sei gesagt: IT-Sicherheit ist eine Investition. Es ist eine sehr lohnende Investition, aber Sie müssen berücksichtigen, dass es hier eben nicht nur Fachkräftemangel gibt und wir diesen Fachkräftemangel mitnichten nur mit Technologie abfangen können, sondern wir müssen uns darüber klar werden, dass es hier eine sehr ausgefeilte Organisationsstruktur braucht, die Sicherheit by Design konzipiert, die Privatheit by Design konzipiert, die ganz stark menschenschutzorientiert personenbezogene Daten prüft und schaut, ob es Möglichkeiten gibt, dass das, was digital angestoßen wird vom Land, möglicherweise auch Kollateralschäden erzeugt. Es muss gelingen, mit einer sehr durchgreifenden Organisation in die Bereiche, beispielsweise Vergaberecht, reinzuschauen, damit das Land sich nicht abhängig macht von Systeminfrastruktur, die einen möglicherweise auch durch Fahrlässigkeiten aller Art, technische oder personelle Fahrlässigkeiten, noch weiter gefährdet. – So viel dazu, einmal kurz den Rahmen gezogen. Ich hoffe und gehe davon aus, dass sich noch eine Diskussion anschließen wird. Vielen Dank!

**Vorsitzender Florian Dörstelmann:** Vielen Dank, Frau Krohn! – Bevor ich das Wort an den Senat zur einleitenden Stellungnahme weiterleite, möchte ich kurz Herrn Waniek als Landesbevollmächtigten für Informationssicherheit fragen, ob Sie vielleicht auch direkt schon eine Stellungnahme anschließen möchten. Dazu wäre jetzt die Gelegenheit; ansonsten, wenn Sie erst an der Debatte und Antwortrunde teilnehmen möchten, geht das genauso.

**Klaus-Peter Waniek** (Landesbevollmächtigter für Informationssicherheit): Guten Tag, meine Damen und Herren! Herzlichen Dank für die Einladung! – Ich möchte mich ganz kurz positionieren. Ich bin der Landesbevollmächtigte für Informationssicherheit. Meine Rolle ergibt sich aus dem E-Government-Gesetz und dem Geltungsbereich des E-Government-Gesetzes, das heißt also, sie ist etwas begrenzt. Es ist nicht die Cybersicherheit, es ist die Sicherheit der Berliner Verwaltung. In § 21 E-Government-Gesetz ist geregelt, dass die IKT-Staatsekretärin mich zu dieser Tätigkeit bevollmächtigen darf. Ein weiterer wichtiger Paragraf ist § 23, wo die Standards, die umzusetzen sind, benannt sind. – Das erst mal zur Begrenzung des Ganzen. Weiteres würde ich in die Diskussion einbringen und erst mal die Stellungnahme des Senats

abwarten; aber das erst mal, damit Sie wissen, wo meine Grenze bei der Einordnung der Cybersicherheit ist an der Stelle. – Danke schön!

**Vorsitzender Florian Dörstelmann:** Vielen Dank, Herr Waniek! – Das hat die Sache jetzt gut eingeordnet. Ich darf dann dem Senat das Wort erteilen für die erste Stellungnahmerunde. – Herr Staatssekretär, Sie haben das Wort!

**Staatssekretär Christian Hochgrebe** (SenInnSport): Sehr geehrter Herr Vorsitzender! Sehr geehrte Damen und Herren Abgeordnete! Sehr geehrte Anzuhörende! Ich danke Ihnen ganz ausdrücklich für die bisherigen Beiträge und auch dafür, dass wir über das wichtige Thema der Cybersicherheit heute ganz ausführlich miteinander sprechen können. Die größte Herausforderung in der heutigen Cybersicherheit ist die sich regelmäßig ändernde Natur von Cyberbedrohungen. Cyberkriminelle erfinden sich ständig neu. Sie erfinden neue Technologien, sie erfinden neue Strukturen, um Schwachstellen in Netzwerken und Systemen auszunutzen. Es werden jeden Tag knapp 70 neue Schwachstellen in Softwareprodukten entdeckt. Der Cyberraum wird für viele Kriminelle immer attraktiver. Sie können mit verhältnismäßig geringem Aufwand sehr hohen Schaden verursachen, und sie müssen gleichzeitig kaum noch besondere technische Kenntnisse mitbringen, da Cyberangriffe oder jedenfalls Teile davon auch über das Darknet eingekauft werden können, also quasi Cybercrime as a Service. Außerdem wird das Entdeckungsrisiko für Kriminelle im Cyberraum oftmals relativ gering eingeschätzt.

Im Berichtsjahr 2021 und 2022 ist in der Polizeilichen Kriminalstatistik die Anzahl der erfassten Cybercrimedelikte zwar ein Stück weit zurückgegangen von 146 363 auf 136 865, aber das Bundesamt für Sicherheit in der Informationstechnik, das BSI, bewertet die aktuelle Cyberbedrohungslage in Deutschland als unverändert hoch. Dabei stellen Ransomeware-Angriffe derzeit den Schwerpunkt der Bedrohungslage dar. Dem BSI wurden im aktuellen Berichtsjahr, also vom 1. Juni 2022 bis zum 30. Juni 2023, 68 erfolgreiche Ransomeware-Angriffe auf Unternehmen und 27 auf kommunale Verwaltungen und Betriebe bekannt in Berlin. Darauf ist schon Bezug genommen worden, insbesondere den Angriff auf das KaDeWe und das Naturkundemuseum, die erfolgreich angegriffen worden sind. Der Angriff auf das KaDeWe konnte zwar teilweise abgewehrt werden, aber immerhin wurden offenbar 1,3 Terrabyte vertrauliche Daten kopiert. Im Naturkundemuseum wurden die Daten verschlüsselt, sodass die Mitarbeitenden danach nicht mehr arbeitsfähig waren. Sowohl das KaDeWe als auch das Naturkundemuseum wurden anschließend erpresst.

Ergänzend zu den Cyberangriffen aus monetären, aus finanziellen Gründen ist natürlich auch der russische Angriffskrieg gegen die Ukraine von Cyberangriffen begleitet, insbesondere durch die Denial-of-Service-Attacken auf Websites von verschiedenen Gruppierungen prorussischer Hacktivisten, die unter anderem am 12. Oktober 2023 Berlin.de angegriffen haben, zum Glück ohne Erfolg. Das Eskalationspotenzial im Cyberraum ist unverändert hoch; insbesondere Cyberangriffe auf kritische Infrastrukturen in Deutschland, auf kritische Infrastrukturen in Berlin bleiben nach Einschätzung des BSI auch weiterhin wahrscheinlich.

Cyberangriffe von Hacktivisten der Kriegsparteien können zudem zu Kollateralschäden und zu Missbrauch der gegnerischen Deutungshoheit führen. Sie bergen ein zusätzliches Risiko. Ein Beispiel für Hacktivismus gegen kritische Strukturen in Deutschland ist die Cyberattacke von Anonymous auf das russische Mineralölunternehmen Rosneft, das in Berlin seinen Sitz hat. Glücklicherweise hatte dieses Ereignis keine Auswirkungen auf die Versorgungssicher-

heit in der Region Berlin-Brandenburg. Im Kontext des Ukraine-Krieges stehen wir mit den Behörden des Bundes und auch der Länder in ganz engem ständigem Austausch zur Sensibilisierung, zur Förderung der Resilienzen in der Gesellschaft, in der Wissenschaft, in der Wirtschaft und haben dazu Strukturen geschaffen, um Informationen auf der einen Seite zu bündeln und sie auf der anderen Seite auch schnell den gefährdeten Bereichen ganz aktuell und zeitnah zukommen zu lassen.

Die Zuständigkeit – das ist insbesondere bei Herrn Dr. Herpig aufgeworfen worden – ist natürlich auch immer eine Frage, mit der wir uns befassen. Für die Cyberabwehr ist sie auf viele Beteiligte verteilt. Für den Raum der Behörden ist es neben der allgemeinen polizeilichen Zuständigkeit und der Zuständigkeit der Landesbehörde für Verfassungsschutz ein ganzes Bündel an Behörden, das sich mit diesem Themenkomplex befasst: Das Bundesamt für den Militärischen Abschirmdienst, das Bundeskriminalamt, das Bundesamt für Sicherheit in der Informationstechnik, das Bundesamt für Verfassungsschutz, das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, das Bundeswehrkommando Cyber- und Informationsraum, die Bundespolizei und auch der Bundesnachrichtendienst – all diese vorgenannten Bundesbehörden sind im Nationalen Cyber-Abwehrzentrum vernetzt. Wenn wir dann auf das Land Berlin schauen, ist es so, dass für das Berliner Landesnetz das CERT, das Computer Emergency Response Team, zuständig ist. Das ist im ITDZ angesiedelt. Die operative Cyberabwehr erfolgt also in Berlin durch das ITDZ. Dort befindet sich auch das Security Operations Center. Das ITDZ befindet sich in der Senatskanzlei und untersteht der Senatskanzlei beziehungsweise der dortigen Stabsstelle für die IKT-Sicherheit.

Bereits vor dem Ukraine-Krieg wurde zur Stärkung der IKT-Sicherheit und zur Verbesserung der Resilienz der IT-Systeme des Landes Berlin im ITDZ eine Zertifizierung nach ISO 27001 auf Basis des BSI IT-Grundschutzes durchgeführt. Das Berlin CERT übermittelt regelmäßig lageabhängige Sicherheitshinweise an die Behörden der Berliner Landesverwaltung. Zudem werden über einen Warn- und Informationsdienst Meldungen zu Schwachstellen in Softwareprodukten bereitgestellt.

Wenn wir dann den Bereich der Wirtschaft betrachten, stehen als Ansprechpartner die Zentrale Ansprechstelle Cybercrime für die Wirtschaft, ZAC, im LKA Berlin und die DAB, Digitalagentur Berlin GmbH, der Senatsverwaltung für Wirtschaft, Energie und Betriebe zur Verfügung. Daneben ist das Bundesamt für Sicherheit in der Informationstechnik als die nationale Cybersicherheitsbehörde und somit Bundesoberbehörde für die Umsetzung des IT-Sicherheitsgesetzes zuständig. Die Bundesländer wirken dabei im Rahmen ihrer Funktion als Aufsichtsbehörden über Organisationen, über Einrichtungen, die Dienstleistungen in den Bereichen der kritischen Infrastrukturen erbringen, natürlich mit. Sämtliche für die Abwehr von Gefahren für die IT-Sicherheit von kritischen Infrastrukturen relevanten Informationen werden beim BSI gesammelt, dort bewertet und an die Betreiber sowie die zuständigen Aufsichtsbehörden weitergeleitet.

Der Senatsverwaltung für Inneres und Sport und auch Innensenatorin Spranger ist das Thema Cybersicherheit insbesondere auch im Zusammenhang mit dem Schutz von kritischen Infrastrukturen sehr wichtig, denn die Sicherstellung der störungsfreien Versorgung der Stadt mit Energie, Wasser oder auch Dienstleistungen in den Bereichen Gesundheit oder Telekommunikation ist elementar und unabdingbar.

Wir streben deswegen eine noch weiter vertiefte Zusammenarbeit mit dem BSI an. Hierzu wird in Zusammenarbeit mit der Senatskanzlei eine Kooperationsvereinbarung mit dem BSI geschlossen und auch geprüft, ob wir in der Abteilung III eine zentrale behördliche Kontaktstelle für das BSI aufbauen. Mit der Erweiterung dieses Dienstleistungsangebots des BSI haben wir in Berlin auf jeden Fall einen starken Partner an unserer Seite.

Lassen Sie mich abschließend noch kurz etwas zu den letzten Ausführungen von Frau Krohn sagen, insbesondere was die kritische Beleuchtung von Technologien betrifft. Wir müssen feststellen, dass wir den Straftaten, der Lage von heute, nicht mit einem Werkzeugkasten von vorgestern begegnen können, sondern wir müssen da Augenhöhe herstellen. Dazu bedarf es moderner Technologien, dazu bedarf es auch KI. Ich hatte vorhin in dem Bericht über die IMK bereits ausgeführt, dass sich die EU-Ebene derzeit mit der Verordnung zu künstlicher Intelligenz, mit der KI-Verordnung befasst. Die IMK jedenfalls, und ich teile diese Auffassung ganz ausdrücklich, sieht es sehr kritisch, die KI-Verordnung noch einmal zu verschärfen. Dies würde zu schwerwiegenden Einschränkungen der Aufgabenerfüllung der Sicherheitsbehörden und Risiken für die öffentliche Sicherheit führen. Deswegen nochmals: Wir können der Lage von heute nicht mit dem Werkzeugkasten von vorgestern begegnen. Wir müssen dort Waffengleichheit und Augenhöhe herstellen. – Vielen Dank!

**Vorsitzender Florian Dörstelmann:** Vielen Dank, Herr Staatssekretär! – Wir treten dann in die Debatte ein. Ich habe verschiedene Wortmeldungen, zunächst von Herrn Abgeordneten Schrader. – Bitte, Sie haben das Wort!

**Niklas Schrader** (LINKE): Vielen Dank! – Vielen Dank auch an die Anzuhörenden für die interessanten Vorträge! Ich habe ein paar Fragen, die ich stellen will. Insgesamt ist das Thema ein meines Erachtens hier viel zu wenig priorisiertes Thema. Wir haben angeregt, den Ausschuss für Digitalisierung dazuzuladen; da sind jetzt, glaube ich, nur wenige gekommen, aber das ist ein Thema, das auch dort noch eine größere Rolle spielen sollte, zumal die Digitalisierung in Berlin zwar nur langsam voranschreitet, aber es kann nicht sein, dass die IT-Sicherheit noch langsamer hinterherläuft. Eigentlich müsste es umgekehrt sein. – So viel zum Allgemeinen.

Ich habe noch Fragen und möchte beginnen mit der grundlegenden: Wie steht es überhaupt mit unserem Wissen über das Gesamtbild? Insbesondere Herr Herpig hat das angesprochen und ein Lagebild gefordert, aber ich würde Sie alle gerne fragen, wie Sie die derzeitige Erfassung von Angriffen, von Verstößen gegen die IT-Sicherheit und der entsprechenden Kriminalität bewerten. Man liest in der Polizeilichen Kriminalstatistik zum Beispiel, dass ein Viertel der Fälle nicht in die Statistik eingeht, weil der Tatort im Ausland liegt. Es ist bei diesem Phänomen ein bisschen unlogisch, nach In- und Ausland zu trennen, wenn wir ein Gesamtbild haben wollen von den Bedrohungen, die wir haben. Was müsste man verbessern, um diese Erfassung wirklich umfassend zu machen? – Herr Herpig, noch mal konkret, wenn Sie von einem Lagebild sprechen: Was sollte da genau wie erfasst sein und drin stehen? Sind Ihnen Erfassungen in der Zivilgesellschaft bekannt, die das vielleicht etwas anders machen als staatliche Stellen? Wir kennen das aus dem Bereich Hasskriminalität, Opferberatungsstellen oder so etwas. Die machen eine Erfassung, erstellen Statistiken und haben eine etwas andere Herangehensweise als staatliche Stellen. Gibt es so etwas auch in diesem Bereich, was sich gegenseitig befruchten kann?

Herr Herpig sprach auch davon, dass man die Fachkräfteausbildung stärken muss. Daran angeknüpft die Frage: Wie bewerten Sie denn das Basiswissen der Beschäftigten im öffentlichen Dienst und auch in der kritischen Infrastruktur derzeit und entsprechende Aus- und Fortbildungsprogramme, also sozusagen das Einfallstor Mensch, das wir in den entsprechenden Strukturen haben? Wie steht es darum in Berlin nach Ihrem Wissen, und was kann man tun, um das zu verbessern?

Dritter Punkt, Thema Sicherheit, Schutz und staatliche Instrumente und Befugnisse; Frau Krohn, Sie haben es insbesondere angesprochen mit zwei Beispielen. Ich möchte Sie noch auf einen anderen Passus im Berliner Koalitionsvertrag aufmerksam machen, dass das Vorhaben besteht – es wurde schon angekündigt –, für das nächste Jahr in Berlin die Befugnisse für die Quellen-TKÜ und für die Onlinedurchsuchung einzuführen. Ich glaube das, was Sie angemahnt haben: dass man eigentlich immer eine umfassende Prüfung auch der Kollateralschäden vornehmen muss und das Ziel der Sicherheit nicht nur in eine Richtung geht, sondern in verschiedene Richtungen. Vielleicht könnten Sie noch konkret darstellen, wie dieses Vorhaben, Quellen-TKÜ und Onlinedurchsuchung, das Ziel der IT-Sicherheit für die Verwaltung konterkarieren kann. – So viel erst mal von mir. Vielen Dank!

**Vorsitzender Florian Dörstelmann:** Vielen Dank, Herr Abgeordneter Schrader! – Frau Abgeordnete Kapek, Sie haben das Wort!

**Antje Kapek** (GRÜNE): Vielen Dank, Herr Vorsitzender! – Auch von meiner Seite noch mal ganz herzlichen Dank an die drei Anzuhörenden! Ich glaube, dass das Ausmaß, mit dem wir es hier zu tun haben, an vielen Stellen tatsächlich noch nicht im Ansatz bekannt ist. Ein Beispiel, das ich besonders krass fand, war die Lahmlegung der kompletten deutschen IHKen im letzten Jahr, ich glaube, für mehr als ein halbes Jahr, und zwar in einem Ausmaß, dass man dort teilweise nicht mehr das eigene Diensttelefon nutzen konnte. Das sind dann Bereiche, die die Versorgung und Funktionsweise unseres Landes tiefgreifend schädigen und beeinflussen.

Jetzt hat der Senat gerade so sehr schön gesagt, man darf die Probleme von heute nicht mit Instrumenten von gestern bekämpfen. Das würde ich genauso sehen. Allerdings ist die Frage, was die Instrumente von heute sind. Wir sind uns, glaube ich, alle einig, dass wir in Sachen Digitalisierung noch mehr als Luft nach oben haben, und dass wir diese Digitalisierung in ganz vielen Bereichen der öffentlichen Versorgung brauchen, um effizienter zu werden, um bürgerfreundlicher und serviceorientierter und so weiter zu werden. Gleichzeitig, das hat die Debatte im Europäischen Parlament zum Einsatz von künstlicher Intelligenz in der vergangenen Woche gezeigt, stehen wir so ein bisschen wie der Hase vor der Schlange bei der Frage: Was geht, und was ist denn überhaupt eine Risikoeinschätzung? Brauche ich eine Regulierung oder nicht? Da, finde ich mit Hinweis auf die Innenministerkonferenz, hat Deutschland keine besonders glänzende Rolle eingenommen.

Nichtsdestotrotz: Ich komme eigentlich aus dem Bereich Verkehr. Das ist, wenn ich mir den Nahverkehr anschaue, wirklich das Rückgrat von öffentlicher Versorgung. Wir haben gerade in Berlin eine veritable Krise im öffentlichen Nahverkehr, und die Instrumente, die dann schnell angeboten werden, sind Dinge wie autonomes Fahren von U-Bahnen, der Einsatz von KI in der Ampelschaltung und vieles mehr. Frau Krohn hat es, das finde ich sehr schön, mehrfach betont: Es geht beim Thema Cybersicherheit immer in allererster Linie darum, Menschen zu schützen. Wenn ich mir vorstelle, was so ein Hackerangriff auf kritische Infrastruktur im

Nahverkehr bedeuten kann, dann weiß ich, ohne viel rechnen zu können, da steht auf jeden Fall sehr viel Schutz von Menschenleben mit auf dem Zettel. Vor diesem Hintergrund stelle ich mir die Frage, und die würde ich gerne auch Ihnen stellen: Kann man es überhaupt verantworten, in diesen Bereichen heute schon solche Digitalisierungs-, Autonomisierungs- und KI-Schritte vorzunehmen, oder ist das gerade noch verantwortungslos? Wenn ja, welche Schutzmaßnahmen müssten wir dann einziehen? Wäre beispielsweise – Sie haben das Sicherheit by Design konzipieren genannt – hier eine open-source-basierte Strategie die richtige?

**Vorsitzender Florian Dörstelmann:** Vielen Dank, Frau Abgeordnete Kapek! – Bitte, Herr Abgeordneter Franco!

**Vasili Franco** (GRÜNE): Vielen Dank, Herr Vorsitzender! – Vielen Dank auch an die Sachverständigen! Ich finde, da sind einige spannende Punkte dabei gewesen, ganz abstrakt und auch sehr konkret. Ich würde Sie gern einmal nach Ihrer Einschätzung fragen, zum Beispiel mit Blick auf die Hackerangriffe, die wir jetzt schon erlebt haben, auch auf das Hauptstadtportal. Das waren verhältnismäßig eher simple Angriffe, haben aber zu massiven Schäden geführt, weil dort der Weiterbetrieb nicht mehr gewährleistet werden konnte. Kann man daraus schließen, dass es insgesamt um die IT-Sicherheit in Berlin schlecht bestellt ist? Wie würden Sie das beschreiben, wenn wir mehr oder weniger nicht mal die Basics so hinbekommen, dass wir zumindest arbeitsfähig bleiben?

Eine weitere Frage – ich weiß nicht, inwiefern Sie dazu Aussagen machen können – bezieht sich auf die Kenntnisse in den Sicherheitsbehörden. Herr Herpig hat die Strukturen dargestellt und aufgezählt, wer mit wem zusammenarbeiten muss. Ich frage mal ganz naiv: Wenn Firmen, Unternehmen, aber auch Privatpersonen kommen und Tatort Internet angeben, inwiefern sind unsere Sicherheitsbehörden derzeit darauf vorbereitet – gern auch in Richtung Polizei –, solche Fälle ernst zu nehmen und überhaupt Ermittlungsansätze verfolgen zu können, die zu irgendetwas führen, außer: Da können wir nichts machen, das Geld ist weg? – Das ist das, was zumindest an sehr vielen Stellen immer noch kommuniziert wird oder was die Resultate bei den Aufklärungsquoten zeigen.

Ein Thema, das Sie zumindest indirekt angesprochen haben, waren die Sicherheitslücken, die genutzt werden. Sie haben das geschildert, mit KI, mit neuen Programmen, Anwendungen, die integriert werden. Wie würden Sie die Gefahr von Sicherheitslücken ganz grundsätzlich beschreiben, und was können wir als Landesgesetzgeber oder als Landesbehörden tun, um diese Sicherheitslücken zu entdecken, sie zu schließen? Oder sind wir hoffnungslos verloren? Wie steht das in dem Konflikt, der vonseiten der Innenverwaltung formuliert worden ist, Versuche zu unternehmen, Sicherheitslücken für die eigene innenpolitische Agenda auszunutzen?

Ich möchte noch einen Punkt anmerken: Im Ausschuss für Digitalisierung und Datenschutz hatte sich unsere Fraktion nach dem Stand der Informationssicherheit in allen Verwaltungen erkundigt, und hier wurden die von den Behörden ergriffenen Maßnahmen zur Verbesserung der Informationssicherheit mit den Themenkomplexen ISMS-Ressourcen, Risikomanagement, IKT-Notfallmanagement sowie IT-Sicherheitskonzepte abgefragt. Es gab eine Verwaltung, die darauf nicht geantwortet hat, und das war ausgerechnet die Innenverwaltung; das hat mir etwas Sorge bereitet. Vielleicht kann die Innenverwaltung dazu Stellung nehmen. Wie sieht es mit einem IT-Sicherheitskonzept für die für Sicherheit zuständige Verwaltung aus? – Herr Waniek, wie würden Sie insgesamt den Überblick beschreiben? Haben wir eine massive

Divergenz zwischen den Sicherheitskonzepten, die es gibt? Gibt es auf der einen Seite Behörden, die schon sehr gut aufgestellt sind, auf der anderen Seite welche, die ganz schlecht aufgestellt sind? Liegt die ganze Kompetenz nur beim ITDZ? Wie würden Sie mit Ihrem Blick die Sicherheit der IT-Systeme in den Berliner Behörden beschreiben?

Abschließend die letzte Frage etwas grundsätzlicher: Ich habe immer den Eindruck, auch wenn wir hier auf Landesebene darüber reden, entweder ist das alles Thema beim ITDZ, oder es ist alles Thema beim BSI. Ich habe die Befürchtung, wir machen es uns damit ein bisschen zu einfach und sagen: Da gibt es zentrale Stellen, die kümmern sich um alles. – Vielleicht können Sie noch darauf eingehen, inwiefern das ein Kardinalfehler sein könnte. – Vielen Dank!

**Vorsitzender Florian Dörstelmann:** Vielen Dank, Herr Abgeordneter Franco! – Herr Abgeordneter Dregger, bitte, Sie haben das Wort!

**Burkard Dregger** (CDU): Herzlichen Dank, Herr Vorsitzender! – Vielen Dank auch an die Anzuhörenden für diese sehr hilfreichen Einblicke! Ich möchte mit dem E-Government-Gesetz des Landes Berlin beginnen, das die Koalition aus CDU und SPD 2016 erarbeitet und verabschiedet hat. Ich habe das damals mit dem sehr geschätzten ehemaligen Kollegen aus diesem Hause, Kohlmeier, federführend bearbeiten dürfen und habe noch beste Erinnerungen daran. Wir haben damals, 2016 war das, erstmalig eine gesetzliche Regelung zur IKT-Sicherheit eingeführt. Da ging es um fünf Punkte: erstens, dass die Berliner Behörden nach BSI-Grundschutz arbeiten – das ist heute auch angeklungen, Herr Atug hat darauf Bezug genommen –, zweitens, dass wir das Berlin CERT gründen, an das die Berliner Behörden anzuschließen sind, damit sie Warnmeldungen erhalten und auch Verhaltensempfehlungen, um etwaigen Angriffen zu begegnen. Drittens haben wir verschlüsselte, sichere IKT-Zugänge gesetzlich vorgeschrieben, damit die Berliner Verwaltung mit sicheren Zugängen arbeitet. Das Vierte war die zentrale Steuerung durch den IKT-Staatssekretär beziehungsweise den Bevollmächtigten, der heute da ist, und das Fünfte waren die Qualifikationsmaßnahmen für die Mitarbeiterinnen und Mitarbeiter, die wir gesetzlich zwingend vorgeschrieben haben. – Das war damals das Ergebnis einer mehrjährigen Befassung unter Einbeziehung von Sachverständigen im Hinblick auf die Fragen der IKT-Sicherheit. Nun sind wir viele Jahre später. Mein Eindruck ist: Sehr viel mehr Standards sind in Berlin jedenfalls in der Zwischenzeit nicht festgeschrieben worden. Deswegen meine Frage an die Sachverständigen, das ist ansatzweise schon angeklungen: Was sind die IKT-Standards, die wir als Update gesetzlich oder im Wege der Verordnung, das hatte Herr Atug angemerkt, regeln sollten? – Da bin ich für eine klare Orientierung sehr dankbar.

Dann habe ich eine zweite Frage: Ich lese in verschiedenen Fachforen über die Frage der nationalen Cyberabwehrsicherheitsstruktur; da geht es um das Nationale Cyber-Abwehrzentrum und anderes. Mir ist momentan nicht klar, inwieweit das Bundesland Berlin und die Bundesländer insgesamt dort eingebunden sind. Wie wird der Informationsaustausch sichergestellt, damit das, was an Erkenntnissen dort aufkommt, auch bei den Behörden der Länder ankommt, auch bei den Senatsverwaltungen? Ich kenne das aus dem Bereich der Terror- und Extremismusabwehr im GTAZ, wo alle Sicherheitsbehörden zusammengeschlossen sind, Bundesbehörden genauso wie Landesbehörden. Das ist natürlich eine ungeheure Anzahl von Behörden, aber so etwas gibt es derzeit nicht im Bereich der Cyberabwehr. Die Frage ist: Was empfehlen Sie uns da? Sollte das Land Berlin sich proaktiv darum bemühen, besser ange-

schlossen zu sein, oder beurteilen Sie es so, dass der Informationsaustausch gewährleistet ist? Mir fehlt da einfach eine Einschätzung. – Vielen Dank!

**Vorsitzender Florian Dörstelmann:** Danke, Herr Abgeordneter Dregger! – Ich habe jetzt noch zwei Wortmeldungen auf der Liste, nämlich Herrn Abgeordneten Matz und Herrn Abgeordneten Förster und würde mit Ihrem Einverständnis für diese Runde kurz schließen, damit die Anzuhörenden die Möglichkeit haben, hier in Ruhe Stellung zu nehmen. – Ich höre keinen Widerspruch, dann verfahren wir so. – Herr Abgeordneter Matz, Sie haben das Wort!

**Martin Matz** (SPD): Vielen Dank, Herr Vorsitzender! – Auch von meiner Seite vielen Dank für die bisher gehörten Beiträge und dass wir diese Anhörung genau auswerten können, wenn wir das Wortprotokoll vorliegen haben, und überlegen, was wir denn tun. Damit bin ich schon bei meiner Frage, denn wir können uns mit dem operativen Tun im Bereich der Cybersicherheit viel beschäftigten und diskutieren; das, was wir als Parlament, als Gesetzgeber am Ende tun können, ist vor allen Dingen, einen institutionellen Rahmen zu schaffen, in dem das angesiedelt werden kann, was für diesen Themenbereich besonders gebraucht wird.

Wenn ich mich jetzt ein bisschen umschaue, nicht vollständig, aber zumindest stichprobenartig: In Baden-Württemberg haben wir seit gut zwei Jahren ein Cybersicherheitsgesetz, nach dem eine Cybersicherheitsagentur errichtet wird, deren Befugnisse und Zuständigkeiten dort geregelt sind. In Nordrhein-Westfalen scheint mir die Struktur etwas anders zu sein: Dort haben wir eine Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen, die von einer gemeinnützigen GmbH betrieben wird, die im Auftrag des Landesinnenministeriums tätig ist. Dort scheint es keinen gesetzlichen Auftrag dahinter zu geben, sondern eher eine Form der Beauftragung durch ein Ministerium.

In Berlin haben wir durch das E-Government-Gesetz die Klärung, dass der zentrale IKT-Dienstleister des Landes Berlin das ITDZ ist, und in § 23 des Gesetzes unter der Überschrift „IKT-Sicherheit“ wird genauer geklärt, wie das in Berlin funktionieren soll. Da die Grundstruktur des E-Government-Gesetzes aber wiederum schon ein paar Jahre älter ist und in diesem Bereich die Entwicklungen schnell voranschreiten, ist meine Frage vor allen Dingen: Können wir inzwischen aus den Strukturen anderer Bundesländer etwas lernen? Können Sie uns etwas empfehlen? Haben wir einen gesetzgeberischen Bedarf in Berlin, oder würden Sie im Kern das, was durch § 23 E-Government-Gesetz in Berlin vorgegeben ist, nach wie vor für einen zeitgemäßen institutionellen Rahmen halten, bei dem der Gesetzgeber keinen Handlungsbedarf hat? Mir geht es nicht um Überschriften, so etwas wie zu sagen: Wir haben jetzt ein Cybersicherheitsgesetz. – Das klingt immer total toll, aber es müsste einen konkreten Fortschritt ergeben gegenüber dem, was wir in unseren bisherigen Strukturen gesetzgeberisch schon verankert haben. – Danke!

**Vorsitzender Florian Dörstelmann:** Danke, Herr Abgeordneter Matz! – Herr Abgeordneter Förster! Bitte, Sie haben das Wort.

**Christopher Förster** (CDU): Vielen Dank, Herr Vorsitzender! – Es ist schon viel gefragt worden, daher ergänze ich das nur noch um Kleinigkeiten. Herr Dr. Herpig sprach davon, dass ein Lagebild fehlt beziehungsweise es einen Lagebericht nicht gibt. Daher würde mich seitens des Senats interessieren, ob Sie imstande wären, das zukünftig umzusetzen und diesen

Lagebericht zur Verfügung zu stellen; oder woran hapert es, dass es diesen im Bereich der Cyberkriminalität bisher noch nicht gibt?

Dann noch eine Frage an die drei Anzuhörenden: Ich stelle mir immer die Frage, ob die Bevölkerung über das ganze Thema überhaupt ausreichend informiert ist. Es gibt regelmäßig Warnungen des BSI, und die Polizei informiert regelmäßig: Was kann man tun? Wie kann man sich schützen? – Gibt es Ihrerseits vielleicht noch Vorschläge, was man besser machen kann beziehungsweise wie man die Bevölkerung, aber auch Unternehmer et cetera zukünftig noch besser schützen und vor allem informieren kann? – Danke!

**Vorsitzender Florian Dörstelmann:** Danke, Herr Abgeordneter Förster! – Dann sind jetzt die Anzuhörenden dran, ich schlage vor, in umgekehrter Reihenfolge, wenn Sie einverstanden sind. – Frau Krohn, bitte, Sie haben das Wort!

**Caroline Krohn** (AGND) [zugeschaltet]: Herzlichen Dank! – Ganz herzlichen Dank für die Nachfragen! Das ist superspannend und ein sehr breiter Rahmen. Ich werde deswegen nicht alles beantworten, sondern nur die Sachen, die direkt an meine Person gerichtet sind, denn es gab Fragen, die in die andere Richtung gingen. Sie können noch mal nachfragen, wenn Sie es auch von mir wissen wollen, aber ich glaube, sachverständiger zu bestimmten Fragen sind die beiden Herren.

Ganz grundsätzlich möchte ich einmal zu allen Fragen sagen: Das, was IT-Sicherheit bringen muss, ist Resilienz. So sehr wir in allen Bereichen, mit denen wir so reden, darüber sprechen: Ist KI eine Option? Ist Hightech eine Option? Ist noch mal Bigger Data eine Option? Ist Blockchain eine Option? – Wir haben immer ganz verheißungsvolle Technologien, bei denen die Politik – ich zähle mich dazu, ich bin auch politisch aktiv – immer wieder der Versuchung erliegt, Glitzerlösungen zu verwenden, anstatt ganz graue, monotone, platte Hausaufgaben zu machen. Solche geschwungenen Sätze wie: Die Probleme von morgen nicht mit den Lösungsmitteln von gestern und so weiter –, die klingen total schön. Ich persönlich bin ein großer Fan von starken Passwörtern. Ich bin ein großer Fan von solider Ermittlungsarbeit der Polizei, überhaupt ein großer Fan der Polizei, insbesondere der Personen, die dort tätig sind. Ich bin kein großer Fan der technologischen Ideen, die ausgestattet werden müssen, weil ich glaube, das sind verheißungsvolle Lösungen, die aber das Kind mit dem Bade ausschütten.

Dasselbe gilt für das ganze Thema Quellen-TKÜ. Das ist eine gigantische Gefahr. Ich verstehe die Sehnsucht danach, ich verstehe die Probleme der Polizei. Die verstehe ich wirklich. Ich verstehe die Frustration, wenn Ermittlungserfolge vereitelt werden, weil es Gesetzgebungen gibt, die das erschweren, was wir eigentlich tun wollen, und ich verstehe wirklich die Traumata, die damit einhergehen, auch Schwerststraftäter nicht fassen zu können, weil wir uns rechtsstaatlich ausgebremst fühlen. Ich verstehe das. Quellen-TKÜ, also der Staatstrojaner, nutzt Schwachstellen aus. Er beschädigt bestehende Codes. Er beschädigt durch den Wunsch nachzugehen, die Barrieren zu mindern, dort die Ermittlungsarbeit ohne den doppelten Richtervorbehalt über scheinbar verheißungsvolle Mittel zu verbessern. Wenn wir uns tatsächlich die Zahlen angucken, stellen wir fest, dass bereits bestehende Versuche in die Richtung gar nicht zu den Ermittlungserfolgen geführt haben, jedenfalls nicht in der Zahl, wie wir wollen. Deswegen ist eine evidenzbasierte Polizeiarbeit wichtig und keine verheißungsvolle technische. Dazu zähle ich eindeutig auch die Quellen-TKÜ. Die Quellen-TKÜ hat diese Kollateralschäden, die ich vorhin versucht habe, deutlich zu machen. Sie bedroht Menschen. Sie be-

droht die Integrität der Privatsphäre. Sie bedroht auch Zugänge. Sie bedroht uns wegen möglicher Fehler, die nicht verzeihlich sind in diesem Kontext. Das persönliche Telefon, die persönlichen Smartphones und Handys gehören zum Allerpersönlichsten, und alles, was dort beeinträchtigt wird, hat eine immense Auswirkung auf die Sicherheit anderer, und zwar nicht nur des Besitzers eines Handys oder eines Smartphones, sondern auch all derjenigen, mit denen er verbunden ist. Das heißt, wenn ich mit jemandem zu tun habe, der Ziel einer Ermittlung ist, dann ist die Wahrscheinlichkeit, dass die Ermittlungen mich als Unschuldige und Unbescholtene betreffen, die einfach aus irgendeinem Grund im Kontakt steht, deutlich höher.

Das geht in die Richtung der zweiten Frage von Bündnis 90/Die Grünen – ich habe leider den Namen nicht mitbekommen, das tut mir wirklich leid –, der Schrei nach KI für Ampeln, alles soll autonom fahren und so weiter. Ich möchte nicht als Digitalskeptikerin daherkommen. Ich glaube, dass digitale Lösungen uns das Leben in vielen Teilen erleichtern, aber der klare Menschenverstand fragt: Ist das wirklich ein Problem, das wir mit KI lösen wollen, oder gibt es andere Lösungen? – Denn jede digitale Maßnahme, so modern und schick sie auch klingt – ich bitte, sich nicht verunsichert zu lassen durch Unkenrufe, wir wären in Deutschland so unmodern und würden nur verhindern –, alles, was wir digital tun, bietet neue Angriffsflächen. Ich komme aus der konventionellen Militärwissenschaft. Wir haben uns in meinem Studium sehr viel über Angriffsflächen unterhalten. Ich kann versichern, auch wenn wir darüber reden, ob die Mitarbeiter der Verwaltung ein zusätzliches Risiko sind oder nicht: Jeder Mitarbeiter, jede Mitarbeiterin der Verwaltung kann zum Schutz der Verwaltung beitragen, wenn sie richtig ausgebildet sind, das richtige Mindset haben und von der Politik die Rückendeckung bekommen. Jeder Einzelne kann aber gleichzeitig das Risiko erhöhen, vollkommen klar, weil wir es hier nicht nur mit Technologien zu tun haben, die Menschen ablösen, sondern wir haben es immer mit einer Interaktion zwischen Mensch und der Technologie zu tun. Das ist der Grund, warum ich dazu rate, wirklich einmal zu gucken: Was haben wir für ein Problem vor uns? Ist die digitale Lösung wirklich die allergeeignetste, und wenn sie geeignet ist, wie können wir sie so aufstellen, dass es keine Kollateralschäden gibt, dass wir keine weiteren Probleme aufmachen, die wir eigentlich zu lösen angetreten sind?

Nimmt die Polizei Cybercrime ausreichend ernst? – Ich glaube, es gibt einen Nachholbedarf für die polizeiliche Ausbildung. Der Polizeibericht zeigt sehr eindeutig, dass wir sehr einseitig über Cybercrime berichten und politische Dimensionen nicht in den entsprechenden Berichten haben, aber ich würde trotzdem die Polizei aus der Haftung nehmen wollen. Bei der Polizei ist Hate Speech auch schon angekommen. Wichtig ist nur: Wir haben nicht die Mittel vom Gesetzgeber, dass man anständig dagegen vorgehen kann. Da gibt es in der Tat sehr viele zivilgesellschaftliche Organisationen, die in der öffentlichen Sensibilisierung großartige Arbeit leisten. Ich kann nur bitten und empfehlen, dass die Politik sich dem anschließt und – das zur letzten Frage von Herrn Förster –, dass auch wir eine sehr aktive Rolle darin einnehmen, die Themen immer wieder zu thematisieren, und zwar in einer adäquaten Form. Ich weiß, ich bin etwas alarmierend in meinem Statement hier; ich bemühe mich normalerweise um hanseatische Zurückhaltung, aber ich hoffe, dass meine Message ankommt. Wir müssen keine Panik verbreiten, und wir müssen auch nicht anfangen, Leute besonders stark zu verunsichern. Das passierte ganz häufig, damit wir bestimmte restriktivere Gesetzgebungen beschließen können. Das würde ich nicht wollen, aber was ich immer will, ist, dass wir uns auf Landes- und Bundesebene, auf zivilgesellschaftlicher Ebene und überall auch dem Verbraucherschutz des BSI zum Beispiel anschließen würden und einfach Dinge distribuieren, damit Leute nicht nur eine Medienkompetenz erwerben, sondern vor allen Dingen eine Risikokompetenz; die fehlt näm-

lich gänzlich in all diesen bildungspolitischen Fragen. Wir müssen vielleicht wie bei der gesundheitlichen Aufklärung auch Kampagnen zur IT-Sicherheitsaufklärung machen. Das wären solche Maßnahmen, bei denen die Politik einen großen Beitrag leisten könnte.

Wir haben noch das ganze Thema Open Source. Open-Source-Sicherheit ist ein komplexes Thema. An der Stelle würde ich an Sven Herpig weitergeben, weil wir uns unter seiner Leitung an anderer Stelle mit diesem Thema sehr stark beschäftigt haben. Falls ich etwas vergessen haben sollte, bitte ich um Erinnerung.

**Vorsitzender Florian Dörstelmann:** Vielen Dank, Frau Krohn! Das können wir selbstverständlich später noch nachholen, falls etwas nicht beantwortet sein sollte. Das ist überhaupt kein Problem. – Herr Dr. Herpig, bitte, Sie haben das Wort!

**Dr. Sven Herpig** (Stiftung Neue Verantwortung e. V.) [zugeschaltet]: Vielen Dank! – Ich fange mal von hinten an: Ist die Bevölkerung gut informiert? – Ich glaube, die Firmen sind viel besser informiert als noch vor zehn Jahren. Auf jeden Fall kann man, glaube ich, jetzt davon ausgehen, dass, wenn eine Firma von einem Vorfall betroffen ist, sie nicht mehr sagen kann, sie hat noch nie etwas von IT-Sicherheitsvorfällen, Cybersicherheit und diesen Fragen gehört. Auch die Medien, gerade die öffentlich-rechtlichen, machen gute Arbeit, und wir haben hier einen starken Expertisezuwachs. Mittlerweile ist die Berichterstattung on point, was man vor zehn oder zwanzig Jahren vielleicht noch nicht hätte sagen können. Was kann man besser machen? – Man kann auf bestehende Leistungen verweisen. Zum Beispiel bietet „Deutschland sicher im Netz“ mobile Unterstützungsleistungen für Ältere und auch in Schulen an, und es gibt eine Telefonnummer, die Sie beim Bundesamt für Sicherheit in der Informationstechnik anrufen können; nicht, wenn Ihre Maus kaputt ist, aber wenn etwas mit Ihrem Rechner nicht funktioniert und man eine Außeneinwirkung vermutet. All das muss man natürlich in die Breite tragen, damit da Kenntnis ist.

Was sind die Probleme, die Kenntnisse in den Sicherheitsbehörden? Ich hatte mir notiert: Was tun, wenn Tatort Internet angegeben wird? – Im häufigsten Fall ist das wahrscheinlich Cybercrime im weiteren Sinne, das heißt, es wird irgendein informationstechnisches Medium bei der Begehung einer Straftat genutzt. Normalerweise Scam: Ich bin Ihre Tochter, bitte überweisen Sie mir Geld. – Das ist keine Qualifizierungslücke, sondern Scams gibt es schon seit langer Zeit in unterschiedlichen Ausmaßen. Hier fehlt es maximal an Personal, das diese Vorfälle abarbeiten kann; das ist der größte Grund. Sie brauchen Fachkräfte, die die Arbeit on the ground leisten. Die Qualifizierungslücke, zum Beispiel in der IT-Forensik, trifft in Nischen zu. Es gibt bestimmte Bereiche, wo das relevant wird. Aber wie gesagt, es ist ein hoher Ermittlungsaufwand, und bei Scams müsste man eigentlich in der Polizei ausgebildet sein, aber auch da ist es natürlich extrem schwierig, zu Ermittlungserfolgen zu kommen. Zumindest wissen wir, was dort passiert, und mit höherem Personaleinsatz würde man das auch schlagen können, aber ich glaube, wir müssen im Endeffekt auch sagen, ab einem bestimmten Punkt ist das einfach nicht mehr leistbar.

Deswegen ist der dauerhafte Verweis auf das BSI zwar ganz nett, aber auch so ein bisschen Ausflucht, denn das Bundesamt für Sicherheit in der Informationstechnik hat mittlerweile zwar anderthalbtausend Mitarbeitende, aber gleichzeitig ist es nicht dafür da, in die Bundesländer zu fahren und hier irgendwelche Ermittlungen zu unterstützen oder zu übernehmen. Dazu sind sie in meisten Fällen gar nicht berechtigt, sondern in einzelnen herausgehobenen Fällen, zum Beispiel, wenn ein KRITIS-Unternehmen betroffen ist oder wie damals, als mit Bitterfeld eine Kommune offline gegangen ist, können sie eingesetzt werden. Aber wie gesagt, hier sind die Bundesländer erst mal am Zug. Sie müssen selbst tätig werden, sie müssen selbst Fachkräfte vorhalten, um operativ on the ground Vorfälle bearbeiten können. Wenn das nicht gegeben ist, dann macht es keiner.

Am Anfang kam die Frage, wie wir die Erfassung bewerten. Zum einen geht es nicht nur um Cybercrime. Es geht um ein Lagebild, um Cybersicherheit generell. Das Bundeskriminalamt hat in einem der letzten Cybercrime Reports – ich glaube, 2021, aber nageln Sie mich nicht auf das Jahr fest – geschrieben: Die Dunkelziffer ist hoch, aber so genau wissen wir das gar nicht, denn es ist eine Dunkelziffer. – Das trifft auch zu. Wenn Sie kein vernünftiges Lagebild haben, zum Beispiel, weil Sie keine Meldepflicht haben, dann reden wir über Dunkelziffern von 30 Prozent, 40 Prozent, die Dunkelziffer könnte aber auch 300 Prozent sein. Das ist eine

Dunkelziffer, und wir müssen hier Licht reinbringen. Solange wir das nicht tun, gehen wir noch davon aus, dass diese Dunkelziffer zu hoch ist und wir hier was tun müssen.

Was kann man dagegen tun? – Eine Meldepflicht für Cybercrime im engeren Sinne dort, wo IT-Infrastrukturen betroffen sind. Warum brauchen wir eine Meldepflicht? – Weil es kaum Anreizstrukturen für Unternehmen gibt, zu melden. Es gibt zwei Anreizstrukturen: Die eine ist, wenn meine Cyberversicherung, die ich habe, mir gesagt, ich muss melden, und dann helfen sie mir, und die andere Anreizstruktur ist, wenn ich von der Polizei Hilfe erwarten kann. Wie wir gerade gehört haben, ist das in den meisten Fällen nicht der Fall. Also versuche ich selbst, das irgendwie hinzubiegen, zahle vielleicht das Lösegeld, und dann bin ich raus. Das ist aber kein Anreiz für mich, dann zur Polizei zu gehen. Wenn wir keine Anreize haben, müssen wir Verpflichtungen schaffen.

Zur Frage: Wie steht es um das Basiswissen der Beschäftigten bei KRITIS und so weiter? – Natürlich müssen wir Awareness schaffen, aber wir machen seit über 20 Jahren Awarenessmaßnahmen. Was wir machen müssen: Wir müssen die Brot- und Buttermaßnahmen umsetzen, müssen die IT sicherer machen. Wir müssen Patches einspielen, wir müssen Backups haben, müssen resilient sein, müssen die Backups üben und so weiter. Wenn Sie mir sagen: Na gut, da hat einer auf einen Link geklickt, dann ist alles kaputtgegangen, und deswegen ist der jetzt schuld –, dann sage ich Ihnen, da haben Sie das Problem nicht verstanden. Menschen müssen auf Links klicken, Menschen müssen auf E-Mails klicken, und wenn es Ihre IT-Menschen nicht fertigkriegen, die IT so sicher zu machen, dass Menschen auf Links klicken können, dann haben wir ein anderes Problem, dann ist nicht der Mensch schuld, der auf einen Link geklickt hat.

Damit möchte ich überleiten auf die Aussage des Staatssekretärs, dass wir den Gefahren von heute nicht mit dem Werkzeugkasten von gestern begegnen können. – Vielleicht fangen Sie erst mal mit dem Werkzeugkasten von gestern an; Patches einspielen, IT-Sicherheitsmaßnahmen umsetzen, Fachkräfte ausbilden. So lange Sie das nicht haben, brauchen wir über KI, Quanten und so weiter gar nicht zu reden. Natürlich kann es unterstützen, aber Sie brauchen Patches, Sie brauchen funktionelle Backups, Sie brauchen Übungen. Sie brauchen vernünftige Organisationsprozesse, um Patches einzuspielen und zu testen. Setzen Sie die Basismaßnahmen – von mir aus von gestern – um, dann können wir noch mal reden. Wir können uns alle Vorfälle angucken, zum Beispiel das Kammergericht, und können gucken, ob KI geholfen hätte oder ob diese Maßnahmen von gestern geholfen hätten. Ich bin da für eine Diskussion durchaus offen. Das soll gar nicht polemisch klingen, aber ich möchte nur mal verdeutlichen: Es ist nicht sexy, Brot- und Buttermaßnahmen umzusetzen, aber das ist das, was wir jetzt brauchen, denn auch diese Heilsbringer wie KI haben natürlich eigene Probleme. Wir haben zum Beispiel schon Angriffe gegen KI-IT-Sicherheitssoftware gesehen, also künstliche Intelligenz, die alles sicherer machen soll. Sogar die ist angreifbar. Das heißt, natürlich schaffen Sie vielleicht unterstützende Leistungen mit dem Einsatz von künstlicher Intelligenz, gleichzeitig eröffnen Sie aber eine ganz andere Angriffsoberfläche.

Dann kam die Frage, ich glaube von der Grünen-Fraktionen, zum Thema: Was machen wir jetzt? – 2020 haben wir eine Studie veröffentlicht, wie man maschinelles Lernen absichern kann, vor allem im Bereich safety-kritische Umgebungen und kritischen Infrastrukturen. Da sind erste technische und organisatorische Maßnahmen aufgelistet, die ich jetzt nicht alle runterrattern will, aber dazu können wir gern in den Austausch treten. Aber auch das, was die

Sachverständige gerade gesagt hat: Nein, wir müssen uns nicht scheuen, neue Sachen einzusetzen, aber wir müssen sie vernünftig entwickeln, und wir müssen sie vernünftig einsetzen. Ansonsten haben wir das gleiche Problem in zwanzig Jahren, das wir jetzt haben. Jetzt haben wir das Problem: Wir haben Software nicht vernünftig abgesichert, wir haben sie nie vernünftig implementiert, und jetzt fällt uns das auf die Füße. Wenn wir jetzt mit KI wieder das Gleiche machen und sagen: Oh, bloß nicht regulieren, aber komplett einsetzen und überall raufschmeißen –, dann sitzen wir in zehn oder zwanzig Jahren da, haben unsere Systeme, die dann alle ganz schön KI machen, aber noch unsicherer sind als heute. Davon haben wir nichts gewonnen, da wird der Schaden im Endeffekt nur noch größer, gerade dann, wenn wir autonomes Fahren und so weiter haben.

Jetzt kurz zu den letzten zwei Punkten, zum Thema Akteure und Struktur: Berlin ist nicht fest im Nationalen Cyber-Abwehrzentrum vertreten. Meines Wissens ist der aktuelle Stand, dass Hessen und Niedersachsen die Bundesländer im Nationalen Cyber-Abwehrzentrum vertreten. Natürlich kann man diskutieren – das haben wir im Januar im Bundestagsausschuss zu dem Thema gemacht –, ob alle Länder vertreten sein sollten. Man kann es so machen. Hierbei ist zu beachten, dass es sich hauptsächlich um einen strategischen Austausch handelt, um einen Austausch über herausgehobene Fälle und so weiter. Hier muss auch ein bestimmtes Maß an Vertrauen zwischen den Akteuren gegeben sein. Wir können nicht auf einmal 14 neue Akteure oder so reinkippen, sondern das muss nach und nach iterativ aufgebaut werden. Gleichzeitig fehlt dieser Plattform aber noch eine vernünftige rechtliche Grundlage, die wir dafür noch bauen müssen. Also ist die Teilnahme Berlins am Nationalen Cyber-Abwehrzentrum kein Problem, aber auch kein Heilsbringer; etwas, was man mittelfristig anpeilen sollte, würde ich sagen. Wichtiger ist – und das findet schon statt – der Austausch auf operativ-technischer Ebene über die CERT, über die Computer Emergency Response Teams. Das CERT Berlin ist im Austausch mit dem CERT vom BSI, und da wird sich über konkrete operative Vorfälle ausgetauscht. Das heißt, dieser Austausch ist da, der ist wichtig, und was man tun könnte, ist, dort mehr warme Körper, also mehr Fachkräfte, reinzubringen.

Letzter Punkt: Das Parlament kann einen institutionellen Rahmen schaffen, ja, und das sollte es, und das müsste es. Der Blick nach NRW und nach Baden-Württemberg ist gut. Man kann den Blick auch nach Bayern und Hessen richten, auch davon kann man ein wenig lernen. Natürlich muss das auf Berlin angepasst sein, aber ich glaube nicht, dass wir um ein neues Gesetz herumkommen, ein IT-Sicherheitsgesetz für Berlin, das eine zentrale Stelle benennt, mit den vernünftigen und ausreichenden operativen Befugnissen, das nicht nur die Landesverwaltung schützt, sondern auch Schutz für Wirtschaft, Wissenschaft und Gesellschaft darstellt und operativ bei Vorfällen unterstützen kann. Es muss eine Meldepflicht mit aufgenommen werden und/oder zumindest die Umsetzung der Verpflichtungen aus der europäischen Gesetzgebung NIS2 für die Bezirke. – Vielen Dank!

**Vorsitzender Florian Dörstelmann:** Vielen Dank, Herr Dr. Herpig! – Dann haben wir jetzt Herrn Atug. – Bitte, Herr Atug, Sie haben das Wort!

**Manuel Atug** (AG KRITIS) [zugeschaltet]: Vielen lieben Dank! – Vorab: Ich bin ein Fan der des demokratischen Rechtsstaats und der Verfassung sowie der Grundgesetze. Daher mag ich auch die Sicherheitsbehörden; genauso wie Caroline vorhin erwähnt hat, sie mag die Polizei. Aber ich kritisiere die wunden Punkte, sowohl um diese immer in die Richtung des Grundge-

setzes und der Verfassung zu verbessern als auch die kritischen Infrastrukturen zu stärken; das ist ja das Hauptthema der AG KRITIS.

Ich mag auch Digitalisierung und sogar so etwas wie KI, sollte man kaum glauben, aber wenn es ordentlich gemacht wird; so wie ich ordentliche Autos toll finde mit funktionierenden Bremsen zum Beispiel oder mit zündendem Airbag, aber bitte keine Hipsterautos ohne Sicherheit. Die mag ich wie hier sicherlich alle eher nicht so.

Es wurde gesagt, Bedrohungen ändern sich; klar, die Auswirkungen davon. Vielleicht eine Anmerkung zu den DoS- und DDoS-Angriffen, die vorhin auch angesprochen wurden: Das ist ein Problem der Neunzigerjahre, und die Neunziger wollen ihr Problem zurück. Das ist schon lange adressiert in der Industrie, in der Wirtschaft, in der Forschung, in zivilgesellschaftlichen Webseiten und bei Privatmenschen – nur noch nicht so richtig in den staatlichen Infrastrukturen. Insofern sind das Fragestellungen von gestern, die mit Technologie nicht mal von gestern adressiert werden. Das sollte man wirklich mal angehen.

Das Problem ist aber Basisschutz wie Backups und aktuelle Software, statt so etwas wie archäologisch wertvolle Systeme zu betreiben und die dann auch noch aus dem Internet erreichbar zu machen. Das schützt tatsächlich vor Auswirkungen der Ransomware wie auch vor Cyberkriminellen und anderen staatlichen Akteuren oder auch vor Totalausfällen: ein Basisschutz wie er im BSI-IT-Grundschutz drinsteht und nicht ein Basisschutz via so etwas wie Palantir, Überwachung, Glitzer-Hypes wie KI, sondern solide Cyberresilienz.

Weil wir KI jetzt so ein bisschen gebasht haben: Übrigens wurden kürzlich 1,6 Milliarden Euro für KI-Forschung freigegeben. Raten Sie mal, ob und wie viel Sicherheit damit erforscht wird oder werden soll. – Richtig! – Hype-Förderung ist nicht sichere Digitalisierung. Das haben wir auch in diesen Themenfeldern nicht so richtig adressiert.

Schauen Sie auf den Schutz in Form von Resilienz. Alle reden von Resilienz. Was ist Resilienz wirklich? – Resilienz ist eine Widerstandsfähigkeit gegen Bedrohungen und Gefährdungen, die durch ein Ereignis ausgelöst werden. Das heißt, es gibt ein Ereignis, es gibt vielleicht Bedrohungen und Gefährdungen, und jetzt muss ich geeignete Gegenmaßnahmen haben, damit diese Ereignisse wirkungslos verpuffen oder maximal eine Störung bewirken, aber genau nicht zu einer Krise oder Katastrophe werden. Wir können uns im Ahrtal angucken, wie wir das gemacht haben: definitiv desolat. – Gucken wir uns das mal mit KI an: Läuft gerade desolat vor die Wand. – Gucken wir uns das mit Blockchain an: Ist schon vor die Wand gelaufen worden. – Gucken wir uns die Luca-App damals an: Gruselig! Ich kann die Hände vor den Kopf schlagen. – Das ist nicht Resilienz, die wir machen, indem wir auf die Herkunft der Täter zum Beispiel gucken, sondern wir brauchen Resilienz durch die Resilienzmaßnahmen der basistechnischen Umsetzung von IT-Sicherheit. Insofern ist es egal, ob ein Täter aus Russland kommt, aus Pakistan, Afrika, von mir aus auch Israel oder den USA. Der CyberBunker stand übrigens mitten in Deutschland, und der Betreiber der kriminellsten und größten Marktplatzwebseite im Darknet war ein sympathischer mitdreißiger Deutscher als Admin. Von daher sind das die echten Fragestellungen, die wir adressieren sollten. – Ich gehe noch auf ein paar Fragen konkreter ein. Das war eher zur allgemeine Lage.

Wie wird die derzeitige Erfassung von Angriffen und Verstößen gegen Cybersicherheitsrecht gesehen? – Tatort Ausland in einem Cyberraum halten wir für komplett sinnlos und veraltet.

Das ist definitiv ein Punkt, der dringend adressiert werden muss. Es wird nicht erfasst, wie viele Ransomware-Angriffe es in welchen Branchen gab; wie viele Lösegeldforderungen wurden angesetzt? Wie viele haben bezahlen müssen? Wie viel wurde bezahlt? – Das wären mal Fakten, über die man reden kann, aber diese Datenpunkte, diese Messpunkte, bringen wir nicht in eine Transparenz, sagen aber andauernd: Ransomware ist schlimm, ist alles aus dem Ausland, und übrigens waren es die Russen – oder so, und nehmen dann aber in der Ukraine mitten im Kriegsgebiet Leute fest, die internationale Tätergruppierungen sind und regelmäßig betonen: Wir sind international, wir kommen aus allen Ländern –, und Deutsche sind da auch mit dabei, genauso wie Westliche. Also, es gibt viele Stuhlkreise und Lagebilder, die helfen aber nicht. Dauernd kommen welche dazu. Weniger, aber konsolidierter wäre mehr, und ich gebe Ihnen auch das Lagebild der AG KRITIS. Das ist seit Jahrzehnten sehr easy: Desolat. Machen Sie Cybersicherheit durch Basissicherheitsmaßnahmen. Selbst das BSI hat in den über 30 Jahren Bestehen dreimal Alarmstufe Rot ausgerufen. Der Angriffskrieg von Putin gegen die Ukraine hat es nur bis Alarmstufe Orange geschafft, weil die Russen echt nicht unsere Fragestellung sind und dieser Krieg auch nicht. Unsere Fragestellung war in den letzten zwei Jahren – tatsächlich zwei der drei Alarmstufe-Rot-Meldungen – Hafnium. Da wurde großflächig einheitliche Microsoft-Windows-Software kompromittiert, die ungepatcht im Netz stand. Das andere war eine Open-Source-Bibliothek, eine kleine Library für Logfiles. Ja, auch Open Source ist toll – darauf komme ich nachher noch –, aber man muss es prozessual und auch sicher betreiben und umsetzen.

Jetzt gab es die Frage: Viele staatliche Befugnisse, Quellen-TKÜ, Onlinedurchsuchung sollen kommen. Was würde das an Sicherheit konterkarieren? – Es unterwandert einfach uns alle, unsere Demokratie, unser aller Systeme komplett durch Offenhalten von Lücken und Schwachstellenmanagement statt Schwachstellenschließen, wenn wir Sicherheitslücken in iPhones und Androids festhalten. Gucken Sie mal kurz auf Ihr Gerät, dann werden Sie feststellen: Auch Sie werden betroffen sein von den Lücken, die dafür freigehalten werden. Es ist heutzutage nicht mehr so, dass die Sicherheitsbehörden in Deutschland Sicherheitslücken erforschen und dann heimlich zurückhalten. Nein, die kaufen sich meistens aus unserem Partnerland Israel eine Software-as-a-Service-Lösung. Das heißt, die Israelis sorgen dafür, großflächig Sicherheitslücken eklatanter Sorte zu ermitteln, zurückzuhalten und für unsere Dienste bereitzuhalten. Diese Lücken sind in all diesen Windowssystemen, Linuxsystemen, Androids, iPhones dieser Welt einfach vorhanden, und immer wieder werden diese Unternehmen plötzlich bekannt, weil Diktaturen und andere Nicht-Demokratien diese Software dann doch irgendwie auch bekommen haben, weil man damit schweineviel Geld macht, wenn man es an genau solche Interessensgemeinschaften verkauft, und die Deutschen kaufen es auch noch mit, sind also Kunden von Diktaturförderern. Das ist ein Unding. So sind diese staatlichen Befugnisse wirklich demokratiegefährdend, kritische-infrastruktur-gefährdend und auch behörden- und institutionsgefährdend.

Es wurde gesagt: Krass, die komplette IHK wurde lahmgelegt. Wo sind die Instrumente von heute zur Bekämpfung von aktuellen Angriffen? – Die Instrumente von heute sind immer noch die Instrumente von gestern, von vorgestern und von vorvorgestern: Resilienz, wie ich sie erklärt habe, Basissicherheit, auf die wir alle drei eingegangen sind. Wir brauchen, wie es Caroline gesagt hat, Ermittler. Wir brauchen Ausstattung, und wir brauchen Ausbildung. Wir haben 300 000 Polizistinnen und Polizisten in Deutschland. Jede und jeder von diesen kann Ihnen ein Knöllchen ausstellen. Unter 1 Prozent davon ist in der Lage, eine Onlinestrafanzeige entgegenzunehmen oder zu verstehen, was ein Cyberangriff war und wie man dagegen

vorgeht. Wir brauchen nicht Spezial-Cyber-Cyber-Behörden oder Cyber-Cyber-Staatsanwälte, nein, wir sind immer noch nicht im Digitalen angekommen und können nicht digital Vorfälle behandeln wie analoge Vorfälle, und genau das ist das große Defizit, das wir da haben. Die Spezialeinheiten helfen da nicht, denn es ist inzwischen normal, dass wir Cyberangriffe haben und auch Cyberdelikte.

Kann man verantworten, Autonomie und Digitalisierung wie KI in den Verkehr et cetera einzubringen? Wenn ja, mit welchen Schutzmaßnahmen? – Ich fasse noch mal zusammen: Resilienz, Basissicherheit, Schwachstellen schließen, Geheimdienste dringend einfangen, denn die drehen frei, und da ist eine Büchse der Pandora geöffnet, dass die alle mögliche Cyberunsicherheit machen dürfen oder sollen, und das ist in diesem einen Cyberraum mit diesem einen Betriebssystem und Software und Anwendungs- und Telefonlandschaften nun mal für alle gefährdend. Sie müssen Befugnisse bewerten, Sie müssen die prüfen und gegebenenfalls besser nutzen oder einfach mal loswerden, weil sie nicht mehr hilfreich sind.

Wie steht es um die gesamte Sicherheit oder die Sicht der Sicherheit in Berlin? – Kurz und knapp: Gruselig und desolat wie in allen Bundesländern und auch auf der Bundesebene, weil alle von Befugnissen, Tätern oder Palantir und KI und Quellen-TKÜ reden, statt von Resilienz und Basissicherheitsmaßnahmen. Ich komme immer wieder auf diese zwei Punkte, weil das die wirkliche Abwehr von Angriffen ist, und dann verpuffen die wirkungslos.

Zur Gefahr von Sicherheitslücken grundsätzlich: Was kann man dagegen tun? – Ja, die bestehen auch in Bundeslandinfrastruktur inklusive KRITIS. – Schwachstellen schließen statt zu managen; Ausnutzen sollte man nicht zulassen. Schwachstellenmanagement halte ich für eine ganz gefährliche Idee. Es ist sogar noch lustiger: Manche Schwachstellen können nicht mehr gefixt werden. Wenn Sie Windows 2000, Windows 2008, Windows 2012 einsetzen – hatten wir ja als Beispiele –, dann gibt es keine Patches mehr vom Hersteller. Wenn wir dann sagen, wir wollen Schwachstellen managen, und die Behörden sollen die so lange nutzen, bis die geschlossen werden, sagen wir eigentlich, dass unsere Sicherheitsbehörden, der Verfassungsschutz und alle anderen Geheimdienste und staatlichen Akteure, auch die ZITiS et cetera, einfach mal für alle Ewigkeit all diese Dinge missbrauchen sollen – und zwar die alle Ewigkeit, die sie auch unsere Behördeninfrastruktur, warum auch immer, aktuell immer noch einsetzt und noch für Jahre einsetzen wird. Damit machen wir uns nicht sicherer, sondern wir fördern diese Eskalationsstufe. Wir müssten unabhängig an Hersteller melden. „Unabhängig“ – da haben wir schon einen Konflikt beim BSI; mit Verlaub, ein Verfassungsschutz, ein BND oder ein BKA sind nicht unabhängig. Alle Behörden müssten umgehend melden, und die Geheimdienste müssten eingefangen werden, und das Ausnutzen muss verboten werden. Erhöhte Resilienz bekommt man, indem man, wie Caroline sagte, Security und Privacy by Design macht, nicht anders. Das ist das wichtigste, oberste Prioritätsziel.

Es war noch die Frage: Welche IKT-Standards sollten genutzt werden? – Kurz zur Einschätzung: Es geht um gelebte Security-Prozesse, nicht direkt um Standards. Das heißt, wir brauchen Informationssicherheitsmanagementsysteme und Business Continuity Management als Prozessvorgehensweise, und dann ist es egal, ob man das nach BSI-IT-Grundschutz, ISO-Normenreihe oder anderen Vorgehensweisen als Standards nutzt. Das heißt, die Standards sind Mittel zum Zweck, und der Zweck ist, ein ISMS und BCM aufzubauen, um eine Resilienz zu haben, um eine Cybersicherheitsresilienz zu haben, widerstandsfähig gegen diese Angriffe zu sein.

Zum Thema Open Source eine Anmerkung: Open Source ist nicht die alleinige Lösung. Es braucht auch da geeignete Prozesse drumherum. Ich habe als Zitat einen Auszug unserer politischen Forderungen der AG KRITIS. Es gibt noch mehr davon, aber nur kurz:

> Im KRITIS-Umfeld eingesetzte Software soll grundsätzlich quelloffen gestaltet sein. Dort wo dies nicht möglich ist, sollen Quellcode und Build-Chain zumindest in treuhänderischer Verwaltung aufbewahrt werden. Dies sorgt dafür, dass ein Patch zur Behebung einer kritischen Sicherheitslücke auch dann noch erstellt werden kann, wenn der ursprüngliche Hersteller nicht mehr existiert oder eine Fehlerbehebung durch den Hersteller unwahrscheinlich ist.

Mehr zu solchen Vorgehensweisen und Methoden, wie man Open Source sinnvoll in kritischen Infrastrukturen einsetzen kann inklusive Sektor Staat und Verwaltung, inklusive Sektor Medien und Kultur, gibt es auf ag.kritis.info, und dann dort unter „politische Forderungen“ schauen.

Dann gab es noch die Frage zum gesetzgeberischen Bedarf in Berlin. Reicht der, oder brauchen wir mehr? Ich hatte ganz konkret gesagt: Wir bräuchten eine KRITIS-Verordnung für die beiden genannten Sektoren, und wir müssen vielleicht auch hingehen und sowohl incentivieren, dass Cybersicherheit und -resilienz erhöht werden, aber vielleicht auch sanktionieren, wenn sie nicht umgesetzt werden. Wir müssen die Ressourcen schaffen, eventuell auch gesetzgeberisch, dass wir genug Ausbildung haben, genug administrative Leute, genug neuere Hardware und nicht jeden Hype implementieren, sondern Lösungen von gestern, die aktuell genutzt werden, einfach mal auf gestrigen oder heutigen Schutz umgesetzt werden.

Die letzte Frage, die ich noch beantworten will: Ist die Bevölkerung ausreichend informiert? – Die Bevölkerung hat im Querschnitt keine Ausbildung in Digitalisierung und Medienkompetenz. Wir bilden Fabrikarbeiterinnen für die Industrie in den Schulen aus, auch heute noch, wo wir eine Informationsgesellschaft geworden sind. Die Bildungspolitik ab Kita über Schule bis einschließlich IHK-Ausbildung – wir haben gerade von der IHK gesprochen – müsste einfach mal angepasst werden, sonst kommen nur Glitzer-Hype-Themen in der Presse durch und Datenschutz wird nicht als essenzielles Grundrecht für eine Demokratie und als Basis gegen Fake News et cetera gesehen, sondern als irgendwie doof. Dieses Verständnis führt nicht dazu, dass wir Basissicherheitsmaßnahmen implementieren können, weil alle nicht wissen, was eigentlich Digitalisierung und Medienkompetenz bedeutet und was die Sicherheit darin ausmacht. Ich verweise noch mal auf meinen Vergleich eingangs: Tolle Autos sind super, aber wenn Airbag und Bremse nicht funktionieren, wird jeder sagen: Ich setze mich da nicht rein. – In der Digitalisierung ist alles immer super. Da fragt keiner nach Bremsen und Airbag, und wenn die nicht zünden, sagt man: War höhere Gewalt. – Diese Bevölkerung mit genau diesen Defiziten, und das kann man denen nun mal nicht vorwerfen, sitzt in den Behörden, Landesinstitutionen und Einrichtungen. Die sitzt auch in den Sicherheitsbehörden. Deswegen haben wir diese erheblichen Defizite, dass alle Resilienz wollen, aber die falschen Forderungen dafür ansetzen und auch die falschen Fragen stellen: Ich brauche KI wegen – – Ja, warum eigentlich? – Na ja, wegen KI. – Das Mittel wird zum Zweck. Oder: Ich brauche mehr Befugnisse und muss mehr Überwachung machen oder Palantir einsetzen. – Nein, das ist nicht die Lösung. Ich muss mir erst die Frage stellen: Was will ich eigentlich erreichen? –, und dann kann ich überlegen: Für diesen Zweck ist das das geeignete Mittel. – Ganz oft, das

haben wir jetzt festgestellt, ist das richtigen Mittel die Resilienz, und zwar durch Basissicherheitsmaßnahmen. – Danke!

**Vorsitzender Florian Dörstelmann:** Vielen Dank, Herr Atug! – Jetzt wäre eine gute Gelegenheit, wenn Herr Waniek als Landesbevollmächtigter für Informationssicherheit anschließen möchte. – Dann haben Sie das Wort. Bitte!

**Klaus-Peter Waniek** (Landesbevollmächtigter für Informationssicherheit): Vielen Dank! – Es ist viel über die Verwaltung und die Sicht der Verwaltung gesagt worden. Ich kann erst mal eines sagen: Die Sorge, dass die Bezirke stärker gefährdet sind als der Rest der Landesverwaltung, kann ich Ihnen nehmen. Wir sind eine Einheitsgemeinde in Berlin, das heißt, die IT-technische Ausstattung und Absicherung der Bezirke als kommunale Einrichtungen ist durch Landesregelungen der Verwaltung geregelt. Wir haben dort keine Differenzierung zwischen Senatsverwaltungen und Bezirken. Die gleichen Absicherungsmaßnahmen gelten für die Bezirke wie für andere. Wir haben ein Berliner Landesnetz, das nach außen geschützt ist und genau die Anforderungen erfüllt, dass, falls irgendwo Schwachstellen und Sicherheitslücken sind, diese nicht von außen erreichbar sind. Das leistet das ITDZ. Mit dem Landesnetz schützen wir auch die Bereiche der Verwaltung, die sich durch das E-Government-Gesetz nicht im Geltungsbereich befinden – das kann man nachlesen –, das ist die Justiz, und das sind Teile der Steuerverwaltung. Das heißt, sobald die an das Landesnetz angeschlossen sind, müssen sie die Sicherheitsanforderungen erfüllen. Das ist in der Architektur festgelegt.

Zur Kritik an unserer Dokumentation, sprich Sicherheitsleitlinie: Wir haben darin eine Fußnote, in der auf die neuen BSI-Standards verwiesen wird und dass die umzusetzen sind. Wir haben die neuesten BSI-Standards immer in der aktuellen Architektur drinstehen, und die wird nahezu jährlich aktualisiert. Es gibt da Verzögerungen – wir haben sicherlich auch Ressourcenprobleme bei der Gestaltung in der IKT-Steuerung –, aber wir sind dicht dran.

Meldeprozesse innerhalb der Verwaltung sind das – wie wir im jährlichen Sicherheitsbericht erfassen –, was am besten funktioniert. Die Verwaltungen melden ihre Vorfälle und Ereignisse immer unverzüglich, und das CERT koordiniert das Ganze. Wir haben eine Sicherheitsinfrastruktur mit dem Berlin CERT als Schnittstelle. Das Berlin CERT ist eingebunden in übergeordnete Strukturen des Verwaltungs-CERT-Verbundes, erfüllt die Anforderungen der Beschlüsse des IT-Planungsrates damit. Wir sind eng vernetzt nicht nur mit dem BSI, sondern auch mit anderen Bundesländern und sind da ganz dicht dran. Das ist die koordinierende Aufgabe des CERT. Das Cyber Defense Center der Landesverwaltung, dazu gehört auch das SOC, sorgt für den operativen Teil des Schutzes und sichert das Ganze ab.

Wir haben Rechtskonformität, und der Beschluss des IT-Planungsrates ist etwas bedauerlich gelaufen, denn da steht in der Begründung, dass die Ausnahme für die Kommunen und die Bildungseinrichtungen deswegen gilt, weil die betroffene Richtlinie, die NIS2-Richtlinie der EU, eine einheitliche Umsetzung verlangt. Schauen Sie sich die Strukturen der Bundesländer und der Stadtstaaten an: Da kriegen Sie auf kommunaler Ebene keine einheitliche Festlegung hin. Das ist die Begründung für diese Beschlusslage gewesen. Bedauerlicherweise ist das nicht veröffentlicht, aber wie gesagt, es steht genau so in der Begründung. Unbenommen davon dürfen die Länder weitere Festlegungen für die Kommunen und Bildungseinrichtungen treffen. Für Berlin ist das durch die Einheitsgemeinde und die Einbindung der kommunalen Infrastrukturen in die Landesinfrastruktur, in die Verwaltung des Landes Berlin, keine Frage.

Das steht an der Stelle nicht zur Diskussion. Wir haben für NIS2 ein Identifizierungskonzept. Der IT-Planungsrat hat beschlossen, dass Einrichtungen identifiziert werden können. Mit der Umsetzung der NIS2-Richtlinie, die bis Oktober des nächsten Jahres erfolgen muss, ist das Land Berlin, sind Staat und Verwaltung wichtige kritische Infrastruktur. Als Abgrenzung dazu: Die Bundesverwaltungen sind sehr wichtige kritische Infrastrukturen. So ist die Umsetzung zu sehen. Wir haben noch keinen Gesetzentwurf, aber sicher gibt es dort auch für das Land Berlin Regelungsbedarf.

Sie reden die ganze Zeit von Cybersicherheit, Informationssicherheit und IT-Sicherheit. Ich habe dafür einen ganz anderen Begriff. Ich sage, wir reden über digitale Sicherheit. Die digitale Sicherheit ist für mich die IT-Sicherheit, die technische Seite, die Informationssicherheit, die wir im Land Berlin für die Verwaltung gestalten, und auch der Schutz gegen außen, Cybersicherheit. Darum geht es uns, und wir haben durchaus die Bevölkerung mit im Blick, worauf wir uns fokussieren müssen. Was nützt es, wenn die Verwaltung digitale Angebote macht und die sicher gestaltet, und dann kommt der Bürger mit unsicheren Endgeräten. Dagegen müssen wir auch gewappnet sein. Ich kann Ihnen sagen, mir sind bereits Informationen bekannt geworden, wo Forschende mir mitgeteilt haben: Es wurden digitale Angebote genutzt mit dem und dem digitalen Endgerät vom dem und dem Nutzer mit der Identität. – Darauf kann ich nicht reagieren, das ist nicht meine Tätigkeit. Da kann ich nur sagen: Diese Forschungsergebnisse gehören nicht in den Bereich der Informationssicherheit des Landes, sondern in Richtung der Cybersicherheitsbehörden, Polizei und Staatsanwaltschaften. Ich kann Ihnen versichern, dass die Informationssicherheit des Landes Berlin eng vernetzt ist mit der Zentralen Ansprechstelle Cybercrime, dem ITDZ und auch mit der Staatsanwaltschaft. Das heißt, die Akteure kennen sich und reagieren entsprechend, sodass klar darauf reagiert wird.

Was die DDoS-Angriffe betrifft: Ja, es gibt DDoS-Angriffe. Die gibt es permanent, nicht alle werden öffentlich bekannt. Aber DDoS-Angriffe haben natürlich Auswirkungen. Selbst wenn sie reduziert werden, also in ihrer Angriffsstärke mitigiert werden, sodass die Angebote weiter erreichbar sind, gibt es bei den Angeboten kritische Prozesse. Wenn Sie da Verzögerungen haben, können Sie die nicht mehr wahrnehmen. Sprich: Wenn Sie ein digitales Angebot der Verwaltung nutzen wollen, und es läuft gerade ein DDoS-Angriff, dann können Sie einen Zahlungsprozess mit einem externen Dienstleister nicht mehr in dem erforderlichen Zeitfenster umsetzen, weil zu viel Last auf den Maschinen ist. Demzufolge leiden die Angebote darunter. Aber wir schaffen es immer wieder, gegen DDoS-Angriffe wirksam zu reagieren. Wir haben wirksame Schutzmaßnahmen etabliert, und das ist wichtig.

Was ist mein Hauptproblem als Landesbevollmächtigter für Informationssicherheit? – Wir gestalten die Managementprozesse für Informationssicherheit, das heißt, wir müssen das Management in die Pflicht nehmen, Informationssicherheit mitzugestalten, und das ist eine große Frage. Fachkräftemangel und dann so ein Managementprozess zu gestalten, ist extrem anstrengend und erfordert sehr hohes Bewusstsein dafür, ein Bewusstsein, das Informations- und digitale Sicherheit nicht nur das Fundament oder das Tragwerk, die Statik der digitalen Prozesse ist, sondern eigentlich auch das Immunsystem. Das heißt, wir haben an der Stelle mehrere Dimensionen zu betrachten. Wir müssen es veranschaulichen und nicht mit IT-Begriffen überlasten.

Um auf die Fragen einzugehen: Ein Gesamtbild zur Informationssicherheit der Landesverwaltung habe ich. Ich habe einen jährlichen Informationssicherheitsbericht, den wir regelmäßig abfragen und erstellen. Ich kann Herr Atug nur recht geben: Der Bericht ist nicht so, dass ich ihn nach einer Bewertung auf einer Skala mit Grün bezeichnen würde, sondern wir bewegen uns in einem Bereich, wo wir maximal befriedigend bis mangelhaft erreichen, mit Schulnoten ausgesprochen. Das ist die einfache Ehrlichkeit, die wir an der Stelle haben müssen. Aber wir haben es, und das ist wichtig. Wir arbeiten daran, und die Fortschritte sind, gemessen am Fachkräftemangel, defizitär, sie müssten viel stärker werden. Wir werden daran arbeiten.

Wir haben das Einfallstor Mensch. Wir wissen, dass der Mensch nicht schuld ist, wenn er etwas anklickt, sondern dann hat er zu wenige Kenntnisse. Daran arbeiten wir ebenfalls, an Aus- und Fortbildungen, an Sensibilisierungsmaßnahmen, und die führen wir auch durch.

Richtig ist auch, Open Source in der Verwaltung einzusetzen, aber Open Source ist nur die Transparenz des Quellcodes. Sie brauchen Open Source auch mit einem Support, dass Ihnen die Sicherheitslücken gemeldet werden. Open Source geht nicht so einfach von der Stange weg. Sie brauchen einen Unterstützer, einen Supporter, der Ihnen im Prinzip die Open Source mit der Unterstützung liefert, dass Sie schnell auf die Schwachstellen reagieren können. Das heißt, der Unterschied ist marginal. Es wird dadurch nicht billiger, muss man einfach sagen.

Zum Hauptstadtportal habe ich schon etwas gesagt; Auswirkungen und Weiterbetrieb.

Sicherheitslücken und Ausnutzung: Wir haben einen Perimeterschutz des Landesnetzes, der relativ stark ist, aber ich sage Ihnen, 100 Prozent Sicherheit gibt es nie. Wir können uns gegen vieles schützen, aber 100 Prozent werden wir nie erreichen; dann würden wir auch niemals krank werden – das ist die Sicht, die ich habe.

Eine enge Zusammenarbeit mit dem BSI haben wir, auch mit der Innenverwaltung, denn wir sind erst vor Kurzem, nach der Wiederholungswahl, in das Ressort der Senatskanzlei gewechselt. Deswegen lösen wir unsere gute Zusammenarbeit nicht auf.

Zu den Themen von Herrn Dregger aus dem E-Government-Gesetz: Wir arbeiten am BSI-Grundschutz. Wir haben das Berlin CERT, es ist etabliert, es erfüllt alle Anforderungen der Normen des IT-Planungsrats. An dem Thema verschlüsselte Zugänge wird gearbeitet. Wir haben ein Projekt für eine Public-Key-Infrastruktur. Das ist eine Sache, die man nicht von heute auf morgen aus dem Boden schnipst, das ist ein fünfjähriges Projekt. 2025 haben wir eine PKI für das Land, wo wir dann Entsprechendes anbieten können, auch nach außen hin offen. Wir steuern das alles zentral. Wir arbeiten, wie gesagt, auch daran, die Konzepte für die Fortbildung der Beschäftigten weiter voranzutreiben, aber wir haben an vielen Stellen auch ein gewisses Ressourcenproblem an Personen, auch in meinem Bereich, sage ich Ihnen ganz ehrlich, und da können Sie mir nicht helfen.

Mit der Umsetzung der EU-Richtlinie NIS2 muss wahrscheinlich auch rechtlich etwas in Berlin passieren, aber dazu brauchen wir erst mal das Umsetzungsgesetz des Bundes, damit wir ableiten können, was für Berlin erforderlich ist. Aber dann ist das Thema, dass Staat und Verwaltung nicht mehr kritische Infrastrukturen sind, weil sie nicht in der KRITIS-Verordnung drin stehen, vom Tisch. Das kann man jetzt schon absehen.

Wie gesagt, wir arbeiten auch gerne zu einem Lagebild Cybercrime zu, das haben wir in der Vergangenheit gemacht, die Zahlen und Fakten liegen der Innenverwaltung vor. Das Wichtige ist: Wir müssen nicht nur den Blick auf uns und die Polizei oder jemanden richten, sondern auch auf die Bevölkerung. Was nützt es, wenn wir Tausende DSL-Anschlüsse im Land Berlin haben, die kompromittiert werden können und dann für einen DDoS-Angriff gegen das Land zusammengeschaltet werden? – Das heißt, wir brauchen vor allen Dingen sichere Infrastrukturen auch bei den Kunden, wir brauchen ein Bewusstsein in der Bevölkerung. Vielleicht sollte Berlin auch mal darüber nachdenken, ähnlich wie andere Städte das gemacht haben, etwas für mehr Sicherheit für die Bürger zu tun, also so eine Initiative, wie Darmstadt sie gemacht habt, „Bleib wachsam“, zu machen, der Bevölkerung anzubieten, das in die Schulen zu tragen und dort stärker im Unterricht zu etablieren, und zwar nicht nur im Informatikunterricht und den Kursen. Wo digitale Bildungsangebote sind, wenn sie dort mit Tablets oder ihren privaten Geräten arbeiten, sollte eigentlich permanent eine Sensibilisierung erfolgen, die sagt: Achtung, das ist kritisch, das ist gefährlich. – Dafür müssen wir aber auch die Lehrer ausbilden und weiterbilden. Dabei haben wir, glaube ich, noch viel Investitionsbedarf in die Zukunft.

Das erst mal in der Kürze eine Antwort, die ich geben kann, damit Sie ein paar Fragen beantwortet bekommen. Ich hoffe, ich bin auf die meisten Fragen eingegangen, sonst müssen Sie bitte noch mal nachfragen. Vielen Dank für Ihre Aufmerksamkeit!

**Vorsitzender Florian Dörstelmann:** Vielen Dank, Herr Waniek! – Wir haben jetzt ohnehin eine zweite Rederunde eröffnet. Sie beginnt mit Frau Abgeordneter Kapek. – Bitte, Sie haben das Wort!

**Antje Kapek** (GRÜNE): Vielen Dank, Herr Vorsitzender! – Auch noch mal vielen Dank an alle Sachverständigen! Jetzt ist so viel gesagt worden, dass ich glaube, dass es den Rahmen sprengen würde, auf jeden einzelnen Punkt einzugehen. Ich habe es für mich so zusammengefasst, dass es unter dem Strich meines Erachtens eher ein verheerendes Zeugnis für die Sicherheit in unserer Stadt darstellt, auch wenn Herr Waniek – das verstehe ich psychologisch auch, das war jetzt bestimmt ein bisschen viel Kritik an der Verwaltung – es so darstellt, als hätten wir gar kein Problem, und nur die Bürgerinnen und Bürger müssten sich ein bisschen anstrengen. Das wird der Sache auch nicht gerecht, vor allem, wenn es um die kritische Infrastruktur geht, die durch den Staat angeboten wird. Es ist mehrfach darauf hingewiesen worden: Hier muss ich in die Strukturen investieren, hier muss ich Strukturen aufbauen, hier muss ich Menschen schulen, die Strukturen zu bedienen, hier brauche ich ganz klare Resilienz- und Basismaßnahmen. – Die sind in dieser Form nicht ausreichend vorhanden.

Es gibt dieses Bild: Na ja, da macht man einfach so weiter –, oder dann heißt es: Man muss einfach nur ein bisschen technologieoffen sein –, ohne sich im Ansatz darüber Gedanken zu machen, welche Gefahren damit einhergehen, wo wir alle wissen, dass jede Wahl, die hier ins Haus steht, das Risiko noch mal um etliches erhöht. Wir haben wahrscheinlich in den nächsten Wochen eine Wahlwiederholung in Berlin, wir haben daraufhin eine Europawahl in Berlin, dann haben wir die Wahl in Brandenburg und so weiter. Wir sind also eigentlich in einer Dauerrisikosituation. 2025 kommt wieder die Bundestagswahl. Was das bedeutet, wenn ich mir vorstelle, dass ich natürlich richtigerweise viele weitere Bereiche unseres täglichen Lebens digitalisiere, seien es die Gasversorgung und der Nahverkehr, sei es was auch immer, dann muss ich mir, glaube ich, auf einem ganz anderen Niveau noch mal Gedanken um mehr Sicherheit machen.

Ich weiß, dass wir auch im Ausschuss für Digitalisierung noch kurz vor der Wahlwiederholung beschlossen haben, dass wir eine Open-Source-Strategie für Berlin auf den Weg bringen wollen. Ich glaube, das ist der richtige Ansatz, weil hinter all diesen Cyberattacken natürlich auch Interessen aus Ländern stehen, die uns nicht wohlgesonnen sind. Gleichzeitig deren IT-Infrastruktur zu nutzen, ist ja wohl so ein bisschen die Katze, die sich selbst in den Schwanz beißt. Deshalb, glaube ich, sollten wir das in Berlin oder in Deutschland selbst entwickeln.

Langer Rede kurzer Sinn: Ich glaube, dass wir heute nicht die Hände in den Schoß legen können, sondern dass das eher beunruhigend ist. Deshalb fände ich es richtig und wichtig zu sagen, wir setzen das Thema in einem halben Jahr hier noch mal auf, und dann sehr gerne mit einem Lagebericht versehen, am besten auch schon mit einem Bericht darüber, welche Instrumente wir dann für die Zukunft hier identifiziert haben und anwenden wollen. – Vielen Dank!

**Vorsitzender Florian Dörstelmann:** Vielen Dank, Frau Abgeordnete Kapek! – Wir werden das sicherlich sogar früher aufrufen, dadurch, dass wir noch die Auswertung des Wortprotokolls haben und voraussichtlich vertagen werden; das bietet dann auch eine Gelegenheit. Wir haben ja mit Bedauern zur Kenntnis genommen, dass bei Ihnen krankheitsbedingt eine Kollegin ausgefallen ist, die auch gerne teilgenommen hätte. Das wird dann die Möglichkeit bieten, noch mal intensiv auf diese ganzen Punkte einzugehen. Das wird selbstverständlich geschehen, gegebenenfalls auch noch mal in einem eigenen Tagesordnungspunkt zu späterer Zeit.

Jetzt hat sich Herr Kollege Förster noch gemeldet. – Bitte, Herr Abgeordneter, Sie haben das Wort!

**Christopher Förster** (CDU): Vielen Dank, Herr Vorsitzender! – Der Senat hat sich jetzt leider nicht geäußert, aber damit die Frage nicht untergeht, würde mich dennoch die Antwort bezüglich des Lageberichts sehr interessieren. – Danke!

**Vorsitzender Florian Dörstelmann:** Vielen Dank, Herr Abgeordneter Förster! – Weitere Wortmeldungen sehe ich aktuell nicht. Dann schlage ich vor, dass wir zunächst den Senat noch mal um eine ergänzende Stellungnahme bitten und dann gegebenenfalls, falls noch jemand von den Anzuhörenden beziehungsweise Herr Waniek etwas ergänzen möchten, besteht dazu natürlich noch die Gelegenheit. – Herr Staatssekretär, Sie haben das Wort!

**Staatssekretär Christian Hochgrebe** (SenInnSport): Sehr geehrter Herr Vorsitzender! Sehr geehrte Damen und Herren! Ich will es mal von meiner Seite aus ganz kurz machen. Wir dürfen, glaube ich, zwei Dinge nicht miteinander vermischen, denn die richtigen Ausführungen zur Schaffung einer ausreichenden Resilienz – sie ist ja vielfach thematisiert worden – betreffen zum einen natürlich die Fragen: Haben wir die richtigen Betriebssysteme auf den Rechnern installiert? Sind die Netze ausreichend sicher? Sind die Mitarbeitenden in ausreichender Weise geschult? – Das machen wir übrigens. Wir hatten gerade bei uns in der Senatsverwaltung für Inneres und Sport letzte Woche die Sicherheitsschulung. Das machen wir regelmäßig in allen Verwaltungen des Landes Berlin. Insofern ist es vollkommen richtig, da die Frage der Resilienz immer wieder nach oben zu halten. Die andere Frage – insofern möchte ich darauf hinweisen, dass wir diese beiden Fragen nicht miteinander verquicken und vermischen dürfen – ist, wie wir die Kriminalität, soweit sie sich auch ins Internet verlagert, bekämpfen. Da-

rauf bezog sich meine Aussage bezüglich des Werkzeugkoffers, und die ist auch im Lichte der gemachten Ausführungen weiterhin richtig.

Ich würde mit Erlaubnis des Vorsitzenden den Abteilungsleiter der Abteilung III, Öffentliche Sicherheit und Ordnung, Herrn Klaus Zuch, bitten, zu den weiteren aufgeworfenen Fragen noch ergänzende Ausführungen zu machen, und darum bitten, anschließend die Polizeipräsidentin aufzurufen.

**Vorsitzender Florian Dörstelmann:** Gerne, Herr Staatssekretär, vielen Dank! – Herr Zuch, bitte, Sie haben das Wort!

**Klaus Zuch** (SenInnSport): Vielen Dank, Herr Vorsitzender! – Meine sehr geehrten Damen und Herren Abgeordnete! Sehr geehrte Damen und Herren! Einige Dinge hat Herr Waniek eben in seinem Beitrag schon mal klargestellt, es gibt einiges an Fragen. Was mir auch wichtig ist, ist, noch mal auf diese Abgrenzung hinzuweisen: Wir sprechen eigentlich über zwei Themen und sollten Cybersicherheit oder, wie er es sagte, IT- und digitale Sicherheit, nicht mit Cyberkriminalität verknüpfen. Das sind im Grunde genommen zwar zusammenhängende Dinge, aber eigentlich zwei verschiedene Themen.

Zur Frage nach dem Lagebild: Er hat ja etwas zur IT-Sicherheit gesagt. Ich kann etwas zum Thema Cyberkriminalität sagen und kann ganz einfach darauf hinweisen, dass wir sowohl im Rahmen der PKS-Berichterstattung im Land Berlin regelmäßig einen Beitrag dazu leisten, was Cybercrime betrifft, als auch auf das hinweisen, was das Bundeskriminalamt jährlich veröffentlicht, nämlich entsprechende Lageberichte zu Cybercrime immer für das vorangegangene Jahr. Der Lagebericht für 2022 ist im Netz abrufbar. Diese Abgrenzung ist wichtig.

Vorhin kam mehrfach die Fragestellung auf, wie das mit der Erfassung von solchen Straftaten ist und ob uns nicht etwas fehlt, insbesondere wenn Auslandstaten eine Rolle spielen. Das ist in der Tat im Moment so, das ist so richtig dargestellt worden. Wir haben eine bundeseinheitliche Erfassungsrichtlinie für die Polizeiliche Kriminalstatistik, danach werden solche Taten bisher nicht erfasst. Ich kann aber bekanntgeben, dass in den Gremien, die sich mit diesen Fragen beschäftigen, mit der Erfassung von Straftaten in der Polizeilichen Kriminalstatistik, im Moment schon darüber diskutiert wird, wie man es zumindest hinbekommen kann, auch diesen Anteil besser darzustellen. Das BKA macht sich entsprechende Gedanken dazu und wird in den entsprechenden Lagebildern der Zukunft darauf eingehen.

Für uns ist es immer wichtig gewesen, eine schnelle Informationsvernetzung hinzubekommen. Herr Waniek, aber auch andere, hatten darauf hingewiesen, welche Kooperationspartner hier am Start sind, im engeren Sinne, wenn ich aus meiner Aufsichtsfunktion heraus gucke, auf das Landeskriminalamt, aber natürlich auch jetzt mit der Senatskanzlei oder auch mit anderen Akteuren, die uns hier wichtig sind. Wir haben gerade in meiner Abteilung eine Umorganisation durchgeführt. Ich hatte seinerzeit eine sehr kleine, aber sehr feine Einheit einführen können, die sich mit Cybersicherheitsfragen beschäftigt, und zwar aus dem Blickwinkel der IT-Sicherheit, von der KRITIS-Verordnung ausgehend. Das ist ausgebaut und jetzt nach dieser Neuorganisation im Referat A angesiedelt worden. Das Referat III A beschäftigt sich mit Fragen des Katastrophenschutzes und des Bevölkerungsschutzes, und wir haben in der Arbeitsgruppe III A 3 neu die Symbiose der Koordinierungsstelle kritische Infrastrukturen und die Einheit Cybersicherheit zusammengefasst, weil wir denken, dass wir dort mit der kleinen

Einheit die größten Synergien hinbekommen können. Im Rahmen der Arbeitsgemeinschaft mit den KRITIS-Betreibenden, die regelmäßig stattfindet, die übrigens auch außerhalb von gesetzlichen Vorgaben stattfindet, wird über die Thematik Cyberkriminalität und Cyberangriffe, auch Cybersicherheit regelmäßig ein Austausch herbeigeführt.

Zur NIS2-Richtlinie hat Herr Waniek etwas gesagt. Ich will noch darauf hinweisen – ich glaube, einer der Experten hatte es vorhin kurz angesprochen –: Wir haben in Berlin auch die Digitalagentur. Das ist eine Einheit, die die Senatsverwaltung für Wirtschaft zu verantworten hat, wo es möglich ist, dass insbesondere die kleinen und mittelständischen Unternehmen bei Fragen zum Thema Cybersicherheit schnell entsprechende Hilfe bekommen können.

Es gab vorhin die Befürchtung, dass Kolleginnen und Kollegen, die Anzeigen aufnehmen, nicht das Wissen über die Cyberkriminalität hätten. Ich glaube, dieser Befürchtung kann man ein wenig entgegentreten, weil die Fachdienststellen, die wir im Landeskriminalamt vorhalten, für Nachfragen übrigens rund um die Uhr verfügbar sind.

Wir haben die Thematik auch in unserer regelmäßigen Besprechung mit dem Verband für Sicherheit in der Wirtschaft Berlin-Brandenburg, wo insbesondere die Unternehmen, auch die IHK, regelmäßige Teilnehmer sind. Da gibt es einen konkreten Beitrag zum Thema Cybersicherheit und Cyberkriminalität, den das LKA immer am Anfang bringt.

Ich hatte gesagt, dass wir eine relativ kleine Einheit sind; der Arbeitsgruppenleiter Herr Creutz sitzt hier hinten auf der Verwaltungsbank. Es ist eine relativ kleine Einheit, und deswegen war es uns immer wichtig, uns im Grunde genommen auch Expertenwissen von außen hinzu zu holen. Wir arbeiten daran, eine Kooperationsvereinbarung mit dem BSI abzuschließen. Das liegt in der Finalisierung, gemeinsam mit der Senatskanzlei. Andere Bundesländer haben das im vergangenen Jahr schon abschließen können.

Es gab die Frage, wie das mit den Fachkräften ist. – Ja, natürlich könnten wir alle in den Behörden, bei der Polizei, überall viel mehr Fachkräfte aus dem IT-Bereich einsetzen. Es ist schwierig. Der Fachkräftemangel ist das Eine, wir haben in der Vergangenheit aber durch die Änderung der Laufbahnverordnung in der Polizei schon etwas gemacht. Wir bieten Damen und Herren, die einen entsprechenden Master- oder auch Bachelorabschluss haben, die Möglichkeit, mit einer verkürzten Ausbildung auch in die Polizeilaufbahn zu kommen. Wir versprechen uns davon, Cyber-Cops stärker in unsere Reihen zu bekommen, um hier mehr und sachkundiges Personal zu bekommen.

Mein Staatssekretär hat auf die Sicherheitsschulungen hingewiesen. Ich kann auch nur noch mal sagen, dass das regelmäßig bei uns getan wird. Der Faktor Mensch spielt überall eine Rolle, nicht nur in Behörden, übrigens auch bei den Unternehmen; die Phishingversuche sind ja all bekannt. Man versucht natürlich, Awareness, wie es neudeutsch heißt, zu schaffen, um zu verhindern, dass Leute bestimmte Anhänge anklicken und dann irgendwelche Schadsoftware bei uns aufgestellt wird.

Ein Abschluss vielleicht noch: Herr Hochgrebe hat noch mal auf den Bekämpfungsteil hingewiesen. Als jemand, der aus der Kriminalitätsbekämpfung kommt, sage ich Ihnen, dass wir die Onlinedurchsuchung und die Quellen-TKÜ als Werkzeuge in dem Werkzeugkasten der StPO brauchen. Das ist natürlich unter höchster Sorgfalt anzuwenden, weil es entsprechende

Eingriffe gibt. Das wird auch so geregelt werden. Sowohl in der Gefahrenabwehr als auch in der Strafverfolgung ist es so, dass richterliche Entscheidungen erforderlich sind. Das wird mit Sicherheit von den Behörden nicht ausufernd angewandt, sondern nur bei Fällen von absolut schwerster Kriminalität. Genau das ist von den Obergerichten mit dem Blick auf die Vorratsdatenspeicherung gesagt worden, die vorhin hier angesprochen wurde. Auch da ist es ja zulässig, die Gerichte haben nicht gesagt, das ist vollkommen unzulässig. – Soweit von mir einige ergänzende Anmerkungen. Herzlichen Dank!

**Vorsitzender Florian Dörstelmann:** Vielen Dank, Herr Zuch! – Dann wurde uns angekündigt, dass auch die Polizeipräsidentin noch mal Stellung nehmen wird. – Frau Dr. Slowik, bitte, Sie haben das Wort!

**Dr. Barbara Slowik** (Polizeipräsidentin): Vielen Dank, Herr Vorsitzender! – Ich versuche mit Blick auf die Zeit, es kurzzumachen. Ich teile uneingeschränkt alles, was Herr Zuch gerade ausgeführt hat. Insbesondere auch immer wieder der Hinweis, dass die Begrifflichkeiten ständig verrutschen: Cybersicherheit, Cybercrime, das verrutscht ständig in den Diskussionen. Das ist für uns durchaus von erheblicher Bedeutung. Die Cybersicherheit gewährleisten das ITDZ und andere gemeinsam. Wenn das nicht gelingt, dann sind wir irgendwo bei Cybercrime, und dann sind wir in der Tat beim Landeskriminalamt. Aber ich glaube, wir wären nicht die richtige Stelle, um die Cybersicherheit zu gewährleisten.

Vielleicht auch mal anhand von Zahlen: Im Jahr 2022 wurden 22 500 Cybercrimeverfahren bearbeitet, davon 21 370 Fälle von Computerbetrug, in Relation dazu 342 Fälle der Datenveränderung und der Computersabotage.

Vielleicht ganz kurz zur Zentralstelle Cybercrime – ich denke, es ist insbesondere unseren Experten und der Expertin bekannt, aber vielleicht auch sonst –: Wir haben schon 2020 im Landeskriminalamt die Zentralstelle Cybercrime gegründet. Dort bündeln wir, wie auch alle anderen Bundesländer, die Fachexpertise durch eine Fachdienststelle für Cybercrimeermittlungen, die auch regelmäßig beschult wird, denn das ist ein Phänomen, das sich sehr schnell verändert. Wir lassen die entsprechenden Kolleginnen und Kollegen im europäischen Ausland schulen, aber auch in anderen Bereichen, wo es nötig ist. Die Herausforderung, Ermittlungen vor allem in der schnellen Sicherung und Auswertung und zur Verfolgung digitaler Spuren stets auf der Höhe der Zeit zu halten, ist natürlich eine große, auch die Nachverfolgung von IP-Adressen. In diesen Bereichen werden auch die Ermittlungen bei entsprechenden Straftaten zum Nachteil von Behörden geführt.

Diese Zentralstelle führt auch regelmäßig Sensibilisierungsveranstaltungen in Form von Vorträgen, Fachbeiträgen und Beratungsgesprächen für Wirtschaftsunternehmen durch; darauf hat auch Herr Zuch schon hingewiesen. Wir machen das sehr intensiv. Wir haben, wie ich denke – so höre ich es aus der IHK auch immer –, einen guten Ruf im Bereich der Unternehmen und sind erster Ansprechpartner im Falle eines Sicherheitsvorfalls. Da hat der Kollege bezüglich des BSI recht, und das ist für uns auch selbstverständlich, da würden wir jetzt nicht das BSI einbinden, sondern das machen wir natürlich selbst.

Durch die weltweit agierenden Gruppen sind strafprozessuale Maßnahmen natürlich auch stark von der internationalen Zusammenarbeit der Strafverfolgungsbehörden geprägt. Hier versuchen wir stets, unser Netzwerk auszubauen, zu erhalten und natürlich auch mit dem

BKA sehr eng zusammenzuarbeiten, was uns auch gelingt. Die nationale Ebene ist klar: Da gibt es einen engen Austausch zwischen den verschiedenen Cybercrimedienststellen der Länder und des Bundes. In jedem Bundesland gibt es entsprechende Einrichtungen, die in der Zusammenarbeit verbunden sind.

Trotzdem – es ist mir wichtig, das noch mal zu betonen – haben wir natürlich Know-how in jeder Fachdienststelle, denn logischerweise finden sich in allen Phänomenbereichen Nutzungen von entsprechenden Geräten, zum Beispiel der angesprochene WhatsApp-Betrug, wie vorhin geschildert, den wir in Berlin im Jahr 2023 in 3 880 Fällen gesehen haben. Dort werden die Ermittlungen sehr erfolgreich in der zuständigen Fachdienststelle geführt, natürlich auch unter Nutzung internationaler Kontakte, denn es ist ja bekannt, dass das kein nationales Geschehen ist, sondern oft grenzüberschreitend. Mit JITs und Action Weeks und so weiter gibt es dort durchaus größere Erfolge, auch bei Erpressungen und Hatespeech. Das sind die Fachdienststellen, die teilweise das Know-how nutzen, das wir in der Spezialdienststelle, in der Zentralstelle Cybercrime, gebündelt haben, sie haben aber natürlich auch eigenes Know-how erworben, wie gesagt, auch im Austausch mit anderen internationalen Strafverfolgungsbehörden.

Wir sollten auch nicht vergessen: Wir haben in der Polizei Berlin eine neue Generation am Start. Gerade die Polizei Berlin hat sehr viele junge Nachwuchskräfte, Digital Natives, die ein hohes Interesse und ein hohes Verständnis haben und sich sehr auch in die Ermittlungsarbeit einbringen, hier alles zu nutzen, was nutzbar gemacht werden kann, auch in den jeweiligen Fachdienststellen.

Vielleicht ein ganz kurzer abschließender Blick noch: Wie schützen wir als Polizei Berlin uns vor Cyberangriffen? – Unsere Netzwerksicherheit erfüllt selbstverständlich den BSI-Grundschutz. Wir halten die Sicherheitskriterien laufend à jour. Unsere Firewall wird nahezu im Sekundentakt angepingt, um Schwachstellen zu entdecken. Natürlich sind wir, wie wir alle, zahlreichen Angriffsversuchen durch Spam und Phishingmails ausgesetzt, die immer wieder in der Qualität zunehmen. Es werden nicht immer alle Phishingmails gemeldet, das ist so, es gibt also sicherlich eine große Zahl, die direkt gelöscht wird, wo die entsprechenden Mitarbeitenden es vielleicht nicht weitermelden. Allein in unserer IKT-Abteilung beschäftigen wir zehn Mitarbeitende, die ständig das Polizeinetz mit entsprechenden Maßnahmen sichern und den Traffic überwachen.

Nur am Rande zum Thema Risikokompetenz: Auch hier sensibilisieren wir unsere Mitarbeitenden immer wieder durch das zentrale IT-Sicherheitsmanagement und bieten und raten an, an Veranstaltungen teilzunehmen. Eine Veranstaltung, die sich konkret damit befasst, in der live gezeigt wird, wie PCs und Smartphones manipuliert werden können, erfreut sich Gott sein Dank großer Nachfrage. – Vielleicht so viel von mir.

**Vorsitzender Florian Dörstelmann:** Vielen Dank, Frau Dr. Slowik! – Weitere Wortmeldungen aus den Reihen der Abgeordneten habe ich hier nicht. Gibt es gegebenenfalls noch kurze Anmerkungen vonseiten der Anzuhörenden oder von Herrn Waniek? – Hier gibt es noch zwei Wortmeldungen. – Herr Atug, vielleicht fangen Sie einfach kurz an. Aber ich bitte mit Hinblick auf die Sitzungszeit, das ganz kurzzufassen. Vielen Dank!

**Manuel Atug** (AG KRITIS) [zugeschaltet]: Ich wollte noch mal auf vier oder fünf Punkte eingehen. – Cyberkriminelle und andere staatliche Akteure fragen übrigens nicht nach Compliance, ob die KI cool oder hip ist oder ob das System nicht im Scope zur Compliance war oder es verboten ist, das zu hacken. Das ist eine ganz wichtige Erkenntnis, die man auch noch mal mitnehmen sollte.

Richterliche Entscheidungen bei Quellen-TKÜ wurden angemerkt. Ich frage mich immer noch: Wie sollen Richter und Anwälte das beurteilen? – Wir haben ja festgestellt, wie die Digitalisierungskompetenz ist. Eine Quellen-TKÜ ist ein hochkomplexer Eingriff in technische und soziale Fragestellungen. Das Soziale können die gut bewerten, das Technische können sie eigentlich nur durchwinken, wenn man sagt: Wir empfehlen eine Quellen-TKÜ, weil böse. – Sehr viel Sachverstand ist da einfach an vielen Stellen nicht vorhanden, weil das hochkomplexe Fragestellungen sind.

Es wurde angemerkt, dass es das nur bei schwersten Straftaten gibt. Damals wurde die Quellen-TKÜ wegen Terrorismus eingeführt, heutzutage ist sie schon für Drogenhandel und Wohnungseinbrüche möglich. So viel zu schweren Straftaten. Solche Befugnisse normalisieren sich mit der Zeit. Das ist eine Gefährdung der Demokratie und des Verständnisses der Bevölkerung gegenüber den Sicherheitsbehörden. Damit macht man der Polizei das Leben irgendwann wirklich schwer. Stille SMS oder Kontostandsabfragen waren irgendwann auch mal sehr selten, jetzt gibt es mehrere Zehntausend Anfragen im Jahr durch Normalisierung und Etablierung. Das ist eine Marodierung der Demokratie, und das ist wirklich gefährlich.

Soziale Defizite können auch heute nicht mit technischen Lösungen und Überwachungen wie Palantir oder sonst etwas gefixt werden. KIs haben einen Bias durch die Testdaten, und der spiegelt den Hass der Gesellschaft wider. Hass und Hetze kann man jetzt schon oft nicht genug ermitteln, weil es eben schwierig ist, weil die Ausstattung und so weiter – das habe ich hier alles ausführlich erklärt – nicht da ist. Journalisten oder Sicherheitsforscherinnen und die Community recherchieren ein wenig und finden direkt die Namen der Täter. Eine Anzeige ist meist leider nutzlos, das sagen sehr viele. Eine Täter-Opfer-Umkehr ist oft genug der Fall. Das ist wirklich ein Problem, das man hart angehen muss. Da ist es dann nicht besser, wenn Chatnachrichten von polizeilichen Akteuren, von Sicherheitsbehördenmitarbeitern öffentlich werden, wo gröbster Hass und gröbster Rassismus kommuniziert werden, und diese Leute sind immer noch im Dienst.

Digitalisierungs- und Cybersicherheits-Know-how in den Behörden und Institutionen ist eine zwingende Voraussetzung für eine erfolgreiche Digitalisierung. Auch da noch mal: Sie müssen in alle Bezirke, in alle Bereiche, in alle Institutionen dieses Know-how einbringen. Damit meine ich nicht Cybersicherheits-Awareness-Schulungen für Mitarbeitende, sondern ich meine damit die Digitalisierungs- und Cybersicherheitskompetenz im Einkauf, in der Führung und auch wirklich Security als Mittel zum Zweck. – Danke!

**Vorsitzender Florian Dörstelmann:** Vielen Dank, Herr Atug! – Dann haben wir jetzt noch eine kurze Anmerkung von Herrn Dr. Herpig. Wir sind fast am Ende der Sitzungszeit, Herr Dr. Herpig, ich wäre Ihnen also verbunden, wenn Sie das ganz kurz fassen könnten. – Sie haben das Wort, vielen Dank!

**Dr. Sven Herpig** (Stiftung Neue Verantwortung e. V.) [zugeschaltet]: Vielen Dank! – Ich habe nur anderthalb Punkte. Der erste Punkt ist: Wie sieht die Lage in Berlin aus? – Mir ist es egal, ob Sie über Datensicherheit reden, über Cybersicherheit, über was Sie auch immer reden wollen; wir sind uns bewusst, über was wir reden. Wir haben kein einheitliches Lagebild, wie es in den Landesverwaltungen bei der Spionage, bei der Kriminalität gemeinsam aussieht, keinen transparenten Bericht, der die Lage über diese Bereiche zusammenfasst und beschreibt, Handlungsoptionen liefert, denn das rechtfertigt dann möglicherweise einen weiteren Personaleinsatz an verschiedenen Stellen.

Der zweite und letzte Punkt: Meine Kritik bezieht sich vor allem auf das, was das Land Berlin für Wirtschaft und Gesellschaft machen kann. Ich möchte sie nicht als Kritik an Herrn Waniek und seiner Arbeit verstanden wissen, denn er macht mit den Mitteln das, was er machen kann. Hier ist es aber Ihre Aufgabe, die Aufgabe der Legislative und der Exekutive, ihm bessere Mittel, mehr Personal und mehr Ressourcen zur Verfügung zu stellen, damit er die Landesverwaltung sicherer machen kann und die anderen Behörden die Wirtschaft und die Gesellschaft besser schützen können. Denn egal, was das Land Berlin alles tut – wir haben gerade gehört, was alles gemacht wird, das zweifle ich auch gar nicht an –, am Ende sind wir uns ja einig, dass es nicht genug ist, weil die Bedrohungslage ist, wie sie ist. Es geht nicht darum, einen Schuldigen zu finden, sondern es geht darum, mehr zu tun, Weiteres zu tun, neue Sachen zu tun. Dafür haben die Sachverständigen heute mehr als genug Ideen geliefert, und für die sind wir natürlich im Austausch und sprechen gerne mit Ihnen, falls Sie unsere Ideen gut fanden und weiter erarbeiten wollen. – Vielen Dank!

**Vorsitzender Florian Dörstelmann:** Vielen Dank, Herr Dr. Herpig! – Vielen Dank Ihnen allen als Anzuhörenden, dass Sie uns hier mit Ihrer Expertise zur Verfügung gestanden haben, uns Ihre Zeit geopfert haben! Herzlichen Dank dafür natürlich auch dem Landesbevollmächtigten für Informationssicherheit! Herr Waniek, herzlichen Dank auch Ihnen, dass Sie uns zur Verfügung gestanden haben! Wir schließen das heute hier noch nicht ab, sondern wir vertagen das und warten auf das Wortprotokoll, um das Thema wieder aufzurufen und noch einmal in Ruhe zu erörtern. Danke schön für heute, und zu gegebener Zeit gegebenenfalls noch mal! Ich wünsche Ihnen noch eine erfolgreiche und angenehme Woche! Vielen Dank!

Punkt 4 der Tagesordnung

| | |
|---|---|
| Antrag der Fraktion Die Linke | 0129 |
| Drucksache 19/1225 | InnSichO |
| **Sofortigen Winterabschiebestopp anordnen und ausnahmslos einhalten!** | Haupt |

Siehe Inhaltsprotokoll.

Punkt 5 der Tagesordnung

| | |
|---|---|
| Antrag der AfD-Fraktion | 0110 |
| Drucksache 19/1013 | InnSichO |
| **Einsetzung einer Enquete-Kommission „Aus Corona lernen – Berlin für die Zukunft resilient aufstellen“** | GesPfleg(f) Recht |

Vertagt.

Punkt 6 der Tagesordnung

**Verschiedenes**

Siehe Beschlussprotokoll.

* * * * * *