Abgeordnetenhaus BERLIN

19. Wahlperiode

Plenar- und Ausschussdienst

Wortprotokoll

Öffentliche Sitzung

Ausschuss für Inneres, Sicherheit und Ordnung

60. Sitzung
3. November 2025

Beginn: 09.00 Uhr
Schluss: 11.42 Uhr
Vorsitz: Florian Dörstelmann (SPD)

Vor Eintritt in die Tagesordnung

Siehe Beschlussprotokoll.

Punkt 1 der Tagesordnung

Besondere Vorkommnisse

Siehe Inhaltsprotokoll.

Vorsitzender Florian Dörstelmann: Ich rufe auf

Punkt 2 der Tagesordnung

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

Hierzu: Auswertung der Anhörung vom 11.12.2023

b) Besprechung gemäß § 21 Abs. 3 GO Abghs 0246
Cybersicherheit und Schutz kritischer Infrastruktur: Aktuelle Herausforderungen in Berlin InnSichO
(auf Antrag der Fraktion der CDU und der Fraktion der SPD)

Hierzu: Anhörung

Ich begrüße unsere Anzuhörenden insgesamt noch einmal ganz herzlich! Hier digital per Webex zugeschaltet Herr Manuel Atug, Arbeitsgemeinschaft Kritische Infrastrukturen, AG KRITIS – herzlich willkommen! – Herr Dr. Sven Herpig, interface – Tech analysis and policy ideas for Europe e. V. – herzlich willkommen! – Herr Henrik Holst, Public Affairs Manager Digitalpolitik und Unternehmenssicherheit, Bereich Wirtschaft und Politik der Industrie- und Handelskammer – herzlich willkommen! – Herr Thomas Rütting, Bereichsleiter Politik und Kommunikation, Prokurist der Stromnetz Berlin GmbH, und mit ihm ist erschienen Herr Jürgen Schunk, ebenfalls Prokurist, und beide werden uns hier zur Verfügung stehen, dafür danke ich Ihnen sehr, wir nehmen das sehr gern in Anspruch – herzlich willkommen! – Ich gehe davon aus, dass wir wieder ein Wortprotokoll fertigen sollen? – Ich sehe keinen Widerspruch, dann verfahren wir so. – Dann fangen wir mit der Begründung des Besprechungsbedarfs zu Punkt 2 a durch die Fraktion Bündnis 90/Die Grünen an. – Frau Abgeordnete Ahmadi, Sie haben das Wort.

Gollaleh Ahmadi (GRÜNE): Vielen Dank, Herr Vorsitzender! – Auch wenn es etwas ungewöhnlich ist, die Auswertung einer Anhörung von vor zwei Jahren mit einem neuen Besprechungspunkt zu verbinden, passt es trotzdem irgendwie, nicht zuletzt, weil die Ereignisse mit Cyberangriffen und Cybersicherheit aktueller denn je sind. Was wir in der damaligen Anhörung gehört haben, war nicht sehr erfreulich: dass wir nicht besonders gut vorbereitet sind. – Die sicherheitspolitische Lage hat sich seitdem nicht verbessert. Wir leben praktisch mit täglichen Angriffen auf kritische Infrastruktur, auf unser Gesundheitswesen, auf unsere Flughäfen und so weiter. Von daher würde ich gern in der heutigen Anhörung mit Ihnen diskutieren und die Diskussion mit unseren Experten führen und schauen, wie weit wir dann die Anhörung von damals abschließen oder auch nicht. – Vielen Dank!

Vorsitzender Florian Dörstelmann: Vielen Dank, Frau Abgeordnete Ahmadi! – Dann wird der dazu verbundene Tagesordnungspunkt b durch die Koalitionsfraktion begründet, zunächst durch Herrn Abgeordneten Dregger. – Bitte, Sie haben das Wort!

Burkard Dregger (CDU): Vielen Dank, Herr Vorsitzender! – In der Tat, wir hatten die Anhörung am 11. Dezember 2023, und es ist uns wichtig, bei dem Thema dranzubleiben, weil der Handlungsdruck nicht geringer, sondern größer geworden ist und uns das Thema wichtig ist. Leider ist es ja auch ein komplexes Thema, und deswegen sind wir dankbar, dass sich Anzuhörende finden, die versuchen, uns zu unterstützen.

Wir haben damals gehört, dass es in der Berliner Landesverwaltung noch sehr alte Server gibt. Es geht ja im Wesentlichen um den Schutz unserer eigenen digitalen Infrastruktur in der Landesverwaltung. Wir müssen uns im Grunde darüber klar werden, dass nicht nur die KRITIS-Betreiber kritische Infrastruktur sind, sondern die Landesverwaltung selbst ebenfalls.

Denn ohne Aufrechterhaltung der Staats- und Regierungsfunktionen ist in einem Katastrophenfall und erst recht in einem Zivilschutzfall die Ordnung überhaupt nicht aufrechtzuerhalten und die Sicherheit nicht zu gewährleisten. Deswegen ist das von großer Bedeutung.

Wir haben im E-Government-Gesetz, das inzwischen schon fast zehn Jahre alt ist, erste Regelungen zur IT-Sicherheit getroffen. In § 23 haben wir damals implementiert, dass alle Behörden den BSI-Grundschutz einzuhalten haben. Wir haben ebenfalls geregelt, dass etwaige Sicherheitsmeldungen im Rahmen eines Berlin-CERT zwischen den Behörden auszutauschen sind und dass ein Informationsaustausch stattfindet. Wir haben des Weiteren in § 4 damals geregelt, dass sämtliche digitale Kommunikation über Ende-zu-Ende-Verschlüsselung zu erfolgen hat, damit sie möglichst sicher ist. Ich glaube, es ist wichtig, auch jetzt wieder neu zu analysieren, wo wir stehen, um die Schwächen zu erkennen, und das als Handlungsauftrag für die Zukunft zu nehmen. – Danke!

Vorsitzender Florian Dörstelmann: Vielen Dank, Herr Abgeordneter Dregger! – Für die SPD-Fraktion Herr Abgeordneter Matz – bitte, Sie haben das Wort!

Martin Matz (SPD): Vielen Dank, Herr Vorsitzender! – Wir greifen das Thema nicht einfach nur wieder auf, was an sich auch schon sinnvoll ist, sondern wir haben dieses Mal noch einen anderen Schwerpunkt gesetzt, nämlich den Schutz der kritischen Infrastruktur im Allgemeinen. Dafür gibt es natürlich einen aktuellen Anlass mit dem Anschlag auf die Strommasten und dem daraus folgenden Stromausfall, den wir in Adlershof erlebt haben. Trotz aller Bemühungen um den Schutz kritischer Infrastruktur, die schon vorher eingeleitet worden sind, und trotz der aus meiner Sicht inzwischen guten Zusammenarbeit zwischen den Betreibern kritischer Infrastruktur ist so ein Vorkommnis natürlich trotzdem Anlass, immer noch mal zu überprüfen, was man alles schon gemacht hat und was man noch machen muss. Deswegen bin ich heute besonders froh, dass wir hier unter den Anzuhörenden auch die Stromnetz Berlin haben, damit wir noch mal relativ konkret hören können, was denn dort die Konsequenzen sein können. Wir haben ja alle zusammen schon im Plenum von der Wirtschaftssenatorin gehört, dass es die Planung gibt, die letzten oberirdischen Kabel noch zu Erdkabeln zu machen, damit sie etwas weniger leicht angreifbar sind, aber das mag auch nur eine Maßnahme sein aus vielen verschiedenen; Redundanzen sind sicherlich auch immer wieder ein Thema für Betreiber kritischer Infrastrukturen.

Von daher freue ich mich, dass wir heute Gelegenheit haben, aktuell zu diesem Themenkomplex noch einmal etwas zu hören und dabei natürlich auch gern – es geht ja auch immer um das Bundesgesetz, wenn es um die kritischen Infrastrukturen geht –, noch mal von allen Anzuhörenden Hinweise an uns aufzunehmen, inwieweit wir als Abgeordnetenhaus auf welche Weise auch immer, sei es als Gesetzgeber oder in anderer Form, etwas dazu beitragen können. – Vielen Dank!

Vorsitzender Florian Dörstelmann: Vielen Dank, Herr Abgeordneter Matz! – Der Senat hat bereits mitgeteilt, zunächst keine weitere einleitende Stellungnahme abzugeben, sodass wir direkt in die Stellungnahmen unserer Anzuhörenden einsteigen können. Ich würde mit Ihrem Einverständnis vorschlagen, dass wir bei Herrn Atug beginnen. – Bitte, Herr Atug, Sie haben das Wort!

Manuel Atug (AG KRITIS) [zugeschaltet]: Vielen lieben Dank! Vielen Dank auch grundsätzlich, Herr Vorsitzender, und vielen Dank für die erneute Einladung wie auch 2023! – Mein Name ist Manuel „HonkHase“ Atug; ich bin im Internet aktiv als HonkHase, das ist dort mein Name. Ich berate und prüfe seit weit über 23 Jahren kritische Infrastrukturen in der Cybersicherheit und Erhöhung der Resilienz.

Wer ist die AG KRITIS? – Kurze Einordnung: Wir sind ein unabhängiger Zusammenschluss von 42 Expertinnen und Experten aus dem KRITIS-Umfeld. Wir haben keine Sponsoren, agieren vollständig unabhängig von Staat und Wirtschaft und vertreten keine Interessen von Unternehmen, Wirtschaftsverbänden oder dergleichen. Das Engagement von uns als AG KRITIS ist einzig getrieben von der Motivation, unabhängig von wirtschaftlichen Interessen die Versorgungssicherheit der Bevölkerung zu erhöhen, eine nachhaltige Verbesserung der Sicherheit kooperativ mit allen Beteiligten herbeizuführen und auch im Katastrophenfall die öffentliche Sicherheit zu verbessern.

Wenn man in den gemeinsamen Koalitionsvertrag zwischen CDU und SPD für Berlin von 2023 bis 2026 schaut, besagt der – ich möchte kurz zitieren –:

> „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 für Vertrauen in digitale Dienstleistungen für Bürgerinnen und Bürger sowie für die Wirtschaft.“

Und er besagt auch:

> „Um den bestmöglichen Schutz unserer IKT-Infrastruktur zu gewährleisten, wird in besonderer Weise in ein landesweit verbindliches, transparent hohes gemeinsames Informationssicherheitsniveau der öffentlichen Verwaltung investiert.“

Starke Worte! Ich war sehr glücklich, das zu hören nach den Problematiken, die wir 2023 diskutiert haben. Schauen wir rein, und nehmen wir uns mal das wesentlichste Beispiel, das wirklich wichtig ist: die Umstellung von Windows 10 auf Windows 11. Als Konkretisierung zu September 2025 lässt sich gemäß Bericht über den Haushaltsplan 2026/2027 an den Ausschuss für Digitalisierung und Datenschutz feststellen, dass allein bei der Polizei Berlin und der Berliner Feuerwehr noch satte circa 18 000 Windows-10-Arbeitsplätze vorhanden sind, lediglich circa 5 000 Arbeitsplätze wurden bis dahin auf Windows 11 umgestellt – eine desolate Quote in Bezug auf die Strafverfolger und Rettungsdienste, also die wesentliche Sicherheit für die Bevölkerung. Selbst die Senatsverwaltung für Inneres und Sport hat noch 444 Windows-10-Arbeitsplätze zu dem Zeitpunkt gehabt und nur 206 Windows-11-Arbeitsplätze; eine Quote von eins zu drei aktuell, zu zwei Dritteln veraltet. Für ein Innenministerium ist das schon ein aussagekräftiges Ergebnis. Kostenfreie Sicherheitsupdates für Windows 10 gab es nur bis 10. Oktober dieses Jahres. Da es in der Verwaltung der Bundeshauptstadt Berlin offensichtlich noch Zehntausende Rechner mit dem Betriebssystem gibt, droht auch eine unnötige und vermeidbare Millionenrechnung oder die totale Unsicherheit auf den Arbeitsplätzen.

Ist das Thema jetzt neu und unerwartet? – Na ja, eher nicht. Wir hatten ja auch schon 2023 darüber geredet. Es gab darüber auch diverse Pressemitteilungen. Im Sommer 2019 beispielsweise war die Migration von 21 Prozent der rund 80 000 PCs damals beim Senat auf Windows 10 geschafft. Man hat zwar von den Grünen aus beispielsweise darauf gedrängt, mehr Open-Source-Alternativen einzusetzen, aber auch das hat nicht wirklich gut funktioniert. Es wurde dann 2023 bekannt, dass es in Berliner Ämtern noch Dutzende Windows-Server mit Windows 2008 liefen, die teilweise 15 Jahre alt waren und keinerlei Herstellersupport mehr erhielten. Das hat sich also nur in Teilen verbessert.

Statt also Palantir zu fordern, um in der Strafverfolgung Massenüberwachung und Rasterfahndung durch Zweckentfremdung der Daten der Bevölkerung vornehmen zu wollen und dafür Dutzende Millionen von Euros jährlich im Abonnement in die USA zu überweisen, sollte vielleicht lieber Cyberresilienz der Berliner Verwaltung oberste Priorität haben. Das heißt, Verwaltungsverantwortliche, die das ernst meinen, nehmen sich vielleicht mal Zeit und melden sich beim Zentrum für Digitale Souveränität der Öffentlichen Verwaltung, ZenDiS, brechen vielleicht mit deren openDesk die kritische Abhängigkeit von Produkten auf, denn echte digitale Souveränität frei Haus durch deren Open-Source-Lösungen hat schon 300 000-mal bewiesen, dass sie funktioniert. Das würde auch dem Versprechen des Koalitionsvertrages unaufgeregt und entspannt Rechnung tragen und das mit abdecken.

Wenn man in die Fachverfahren schaut, gibt es auch in Bezug auf Windows 11 Defizite. Der Bericht über den Haushaltsplan gibt auch da desolate Auskunft. Die Abfrage der Fachverfahren erfolgte seit 2024 regelmäßig, trotz wiederholter Nachfragen liegen nicht alle vor. Es gibt, Stand September dieses Jahres, 415 bekannte Fachverfahren; 259 sind Windows-11-fähig, 156 sind nicht Windows-11-fähig. Davon sind beispielsweise 133 Fachverfahren ohne Rückmeldung, werden sogar mit Risiko klassifiziert, und darüber hinaus heißt es noch:

> „Entgegen den Vorgaben der IKT-Steuerung noch im Einsatz befindliche sogenannte Kleinstverfahren, die auf der Software Microsoft Access oder der Programmierung mittels Makros in den Microsoft Office Produkten wie Excel oder Word basieren, sind von der Umstellung auf Windows 11 nicht unmittelbar betroffen, …“

Die werden halt echt abgeraten, und das ist – – Wir lassen das mal so stehen, das spricht ja für sich.

Schauen wir in die Cloud: Unter „Differenzierung nach Standardisierter und Legacy-Teil der ITDZ-Cloud“ gibt auch eine Erklärung, die zusammenfassend sagt: „Somit sind alle Fachverfahren, die im ITDZ laufen, derzeit im ‚Legacy-Teil‘ verortet.“ Das hat eben seine Gründe. Zu den Kosten des ITDZ Berlin, die durch den Betrieb veralteter Verfahren entstehen, besagt der Bericht dann auch: „Die Kosten betragen durchschnittlich 415% der ursprünglichen Betriebskosten des jeweiligen Verfahrens.“ Genau das ist das Problem: Archäologisch wertvolle Systeme und die Abhängigkeit von amerikanischen Techkonzernen sind teuer und vor allen Dingen ein kritischer Sicherheitsfaktor. Ich empfehle daher wirklich noch einmal dringend, sich mit ZenDiS in Verbindung zu setzen, massiv auf freie Software und Standards zu setzen, digitale Souveränität, um einen nachhaltigen sicheren Systembetrieb zu gewährleisten, so, wie es eigentlich auch der Koalitionsvertrag sagt.

Wie steht es um KRITIS in Berlin? – Wir haben als AG KRITIS geschaut. Die Arbeitsgruppe Kritische Infrastrukturen, Cybersicherheit betreibt eine Webseite und listet alle relevanten Gesetzgebungen auf. Nicht adressiert werden weiterhin die beiden landeshoheitlichen Sektoren Staat und Verwaltung und Medien und Kultur. Der Staat sollte insofern stringenter und rigider sein, wenn der Hebel des Bußgeldes nicht da ist oder auch sonstige Maßnahmen nicht vorhanden sind. Aktuell macht der Staat aber weniger als die KRITIS-Betreiber, das kann und darf einfach so nicht sein. Eine Lösung von uns konkret wäre, eine KRITIS-Verordnung für das Land Berlin zu erlassen, so wie es jedes andere Bundesland auch benötigt und umsetzen müsste, die das alles abdeckt. Man kann sogar eine gemeinsame Musterlösung für alle 16 Bundesländer als Verordnung erarbeiten und diese dann gemeinsam einheitlich umsetzen. Alternativ wäre es auch möglich, NIS2 für die Bundesländer und Kommunen und Landkreise und so weiter gelten zu lassen. Das machen aber weder der Bund noch das BMI noch der IT-Planungsrat. Insofern haben wir auch da weiterhin starke Defizite beziehungsweise gar nichts.

Die Leitlinie zur Informationssicherheit des Landes Berlin ist aktuell in Version 1.0.1 verfügbar, in Kraft getreten am 21. September 2017. Im Abschnitt „IT-Sicherheitskonzepte“ wird weiterhin auf die veralteten BSI-IT-Grundsatzstandards 100-1 bis 100-4 statt 200-1 bis 200-4 verwiesen. Diese Standards wurden schon vor acht Jahren erneuert. In der Schlussbestimmung wird weiterhin behauptet – ich zitiere –:

> „Im Rahmen des Informationssicherheitsprozesses wird diese Leitlinie zur Informationssicherheit regelmäßig (bei wesentlichen Änderungen von in der Leitlinie benannten Referenzdokumenten und mindestens alle zwei Jahre) auf ihre Aktualität hin geprüft und ggfs. aktualisiert.“

Die Leitlinie des Landes Berlin ist also von 2017, soll alle zwei Jahre beziehungsweise bei Bedarf aktualisiert und geprüft werden, ist aber leider hoffnungslos veraltet. Diesen Punkt hatte ich bereits in 2023 explizit bemängelt, aber nichts ist geschehen. Die AG KRITIS denkt daher, dass das immer noch für sich spricht und tief blicken lässt, welchen Stellenwert Cybersicherheit in der Berliner Verwaltung und Verantwortung hat.

Zuletzt: Es gibt eine Cybersicherheitsstrategie für den Sektor öffentliche Verwaltung im Land Berlin. Was diese daran ändern wird und ob sie etwas ändern wird? – Der wichtige Punkt ist: Man braucht zwar eine Papercompliance, aber die hilft allein nicht. Wichtig sind die danach folgenden Schritte, nämlich die Umsetzung in gelebten Sicherheitsprozessen, die Vollständigkeitsprüfung aller gelebten Sicherheitsprozesse und die Wirksamkeitsprüfung aller gelebten Sicherheitsprozesse. Diese drei Dinge scheinen, Stand heute, immer noch sehr unzureichend umgesetzt worden zu sein, und insofern haben wir da noch erhebliche Abweichungen und Defizite sowohl für Berlin selbst als auch für kritische Infrastrukturen in Berlin. – Danke sehr!

Vorsitzender Florian Dörstelmann: Vielen Dank, Herr Atug! – Dann kommen wir zu Herrn Dr. Herpig. – Ich darf kurz daran erinnern, dass wir uns ungefähr fünf Minuten für die Eingangsstatements vorgenommen haben. Das ist die Vorgabe, wenn die ungefähr eingehalten wird, reicht uns das aus. Wir liegen aber sehr gut in der Zeit. – Herr Dr. Herpig, bitte, Sie haben das Wort!

Dr. Sven Herpig (interface): Wunderbar, vielen Dank! – Sehr geehrter Herr Vorsitzender! Sehr geehrte Abgeordnete und Mitarbeitende, die mit beiden Beinen fest auf dem Boden unserer freiheitlichen demokratischen Grundordnung stehen! Sehr geehrte interessierte Öffentlichkeit! Vor fast genau zwei Jahren durfte ich an gleicher Stelle zusammen mit Manuel Atug als Sachverständiger zum Stand der Cybersicherheit hier in Berlin sprechen, und gern möchte ich heute skizzieren, wie sich die Lage aus meiner Sicht seither entwickelt hat.

Die Störung beim IT-Dienstleistungszentrum Berlin im Dezember 2023 – das war, glaube ich, kurz nach unserer Anhörung – hat eindrucksvoll gezeigt, wie eng die Funktionsfähigkeit staatlicher IT-Infrastrukturen mit dem Vertrauen der Bevölkerung in einen handlungsfähigen Staat verknüpft ist, da der Effekt direkt spürbar ist. Während es sich dabei offenbar um einen internen Störfall ohne äußeren Einwirkungen handelte, führte Cyberkriminalität im Jahr 2024 zu massiven Einschränkungen der medizinischen Versorgung in Berlin bis hin zur vorübergehenden Schließung mehrerer Berliner Notaufnahmen, vergleiche Antwort auf Schriftliche Anfrage 19/23205. Im Jahr 2025 wurde schließlich die IT-Infrastruktur der Senatsverwaltung für Justiz und Verbraucherschutz kompromittiert, vergleiche Antwort auf Schriftliche Anfrage 19/23630. Dass die zuständige Senatorin vorher Abteilungsleitern für Cyberabwehr im Bundesamt für Verfassungsschutz war, verlieh dem Vorfall zusätzlich öffentliche Brisanz.

IT-Zwischenfälle, ob durch Angreifer verursacht oder nicht, lassen sich nie vollständig ausschließen. Entscheidend ist, Schäden zu begrenzen und den Betrieb schnell wieder herzustellen. Das ist der Kern von Resilienz beziehungsweise Business Continuity Management, BCM. Leider verfügt die Berliner Landesverwaltung hier bis heute, Stand August 2025, über keine umfassend implementierte Informations-und-Kommunikationstechnologie-BCM, vergleiche Antwort auf Schriftliche Anfrage 19/23495. Dieser Befund ist ebenso ernüchternd wie symptomatisch. Erst im Sommer 2025 stellte der Bundesrechnungshof fest, dass keine der elf Bundesbehörden mit kritischen Regierungsaufgaben regelmäßig prüft, ob sich ihre Dienste auf Basis von Back-ups tatsächlich wiederherstellen lassen.

Neben der mangelnden Resilienz stellt sich die Frage nach der technischen Prävention. Ein Beispiel: Wie viele Rechner der Berliner Verwaltung laufen derzeit noch auf Windows 10, einem Betriebssystem, das im Oktober 2025 sein offizielles Supportende erreicht hat? – Das ist ein hypothetische Frage, Manuel Atug hat sie gerade beantwortet.

Auch bei weiteren schon 2023 vorgebrachten Kritikpunkten zeigt sich kaum Fortschritt; weder beim effektiven Umbau der Cybersicherheitsarchitektur des Landes Berlin, noch bei der Bekämpfung des Fachkräftemangels oder beim Aufbau eines belastbaren Cybersicherheitslagebildes, das operative und strategische Handlungsoptionen aufzeigt und ermöglicht. Die operative Unterstützung des Landes für Unternehmen, Wissenschaft und Zivilgesellschaft beschränkt sich im Wesentlichen auf Gesprächsangebote, Informationsaustausch und Sensibilisierungsveranstaltungen. Auf konkrete Fragen zur Cybersicherheit oder Zuständigkeit wird häufig auf die Bundesebene verwiesen, die hierfür jedoch nur begrenzt verantwortlich und, wie der Bundesrechnungshofbericht dargelegt hat, nur begrenzt geeignet ist. Diese Schieflage wird vermutlich auch die sich im Aufbau befindliche Koordinierungsstelle Cybersicherheit nicht wirklich ändern.

Während die Bedrohungslage in Berlin nachweislich zunimmt, wie neben den genannten Fällen zum Beispiel das gerade eben erschienene Cybersicherheitslagebild der Transferstelle

Cybersicherheit belegt, hat das Land in den letzten Jahren lediglich eine Cybersicherheitsstrategie für den Sektor öffentliche Verwaltung vorgelegt. Eine Strategie allein ersetzt jedoch weder Ressourcen noch rechtliche Verpflichtungen und schon gar nicht die konkrete Umsetzung von IT-Sicherheitsmaßnahmen. Sie ist im besten Fall ein Orientierungspapier und zeigt auf, wie die aktuelle Regierung über Cybersicherheit nachdenkt, im schlechteren Fall ist sie ein Feigenblatt für ausbleibendes Handeln. Da 2026 bereits die nächste Wahl ansteht, ist diese Strategie de facto schon bei ihrer Veröffentlichung veraltet. Die aktuelle Regierung wird kaum noch Maßnahmen umsetzen können, und eine künftige Regierung ist an die Strategie ihrer Vorgänger nicht gebunden. Statt weiterer Papiere, Verweise auf Bundeszuständigkeiten und Sensibilisierungsveranstaltungen sollte sich das Land Berlin auf das Wesentliche konzentrieren: konkrete IT-Sicherheitsmaßnahmen umsetzen, vorhandene Systeme modernisieren und die Fachkräfte ausbilden, die dafür notwendig sind. Ich möchte uns alle noch einmal daran erinnern: Wir haben in der Cybersicherheit kein Erkenntnisproblem, wir haben ein Umsetzungsproblem. – Vielen Dank!

Vorsitzender Florian Dörstelmann: Vielen Dank, Herr Dr. Herpig! – Dann Herr Holst, bitte, Sie haben das Wort!

Henrik Holst (IHK Berlin): Sehr geehrter Herr Vorsitzender! Sehr geehrte Abgeordnete! Sehr geehrte Frau Senatorin! Liebe Kolleginnen und Kollegen! Mein Name ist Henrik Holst. Ich bin bei der IHK Berlin für die Digitalpolitik und Unternehmenssicherheit zuständig. Vielen Dank, dass ich mich hier an der Anhörung beteiligen kann! Als IHK bieten wir eine Reihe von Informations- und Serviceangeboten rund um den Themenkomplex Cybersicherheit und Resilienz an, unter anderem einen Newsletter, wir haben Informationsveranstaltungen und stellen auch einige Leitfäden online. Außerdem sind wir Teil der Berliner Sicherheitspartnerschaft, in der wir regelmäßig die Sicherheitsbehörden mit Konzernsicherheitsexperten zusammenbringen. Ich möchte in meinem Statement, nachdem wir so viel KRITIS-Expertise haben, etwas stärker auf die Perspektive von Wirtschaft und KMU eingehen und einige Stellschrauben skizzieren, an denen vielleicht Senat und Politik drehen könnten.

Meine beiden Vorredner haben ja schon skizziert, wie sich die Bedrohungslage weiter dynamisch entwickelt. Das deckt sich auch mit unseren Zahlen, wir erheben das einmal im Jahr in unserer Digitalisierungsumfrage: Bundesweit war jedes fünfte Unternehmen im letzten Jahr von einem erheblichen Cyberangriff betroffen. Wenn man sich die Unternehmen anschaut, die mehr als 1 000 Beschäftigte haben, war es sogar jedes zweite Unternehmen, also die Hälfte. Aber wie die Sicherheitsbehörden und Geheimdienste eindringlich warnen und es auch meine Vorgänger skizziert haben, geht es lange nicht mehr nur um den Cyberraum, sondern um eine hybride Bedrohungslage. Die Grenzen zwischen digital und analog verschwimmen, zwischen kriminellen und staatlichen Akteuren, zwischen Cyberangriffen, Spionage und Sabotage, und um dafür gewappnet zu sein, müssen wir gesamtgesellschaftlich denken. Das ist eine Aufgabe für Politik, Verwaltung, Wirtschaft und Zivilgesellschaft, und diese Aufgabe heißt in erster Linie – auch das haben meine Vorredner bereits gesagt –, wir müssen die Resilienz stärken. Das klingt auf den ersten Blick vielleicht etwas abgedroschen, aber es hilft uns dabei, in der Diskussion den Fokus auf das zu legen, was wir überhaupt selbst kontrollieren können.

Erlauben Sie mir deshalb, dass ich einmal kurz dieses Buzzword Resilienz etwas mit Leben fülle. Wir können kaum kontrollieren, wer angreift, welche Methoden genutzt werden und wann etwas passiert. Es gibt keinen hundertprozentigen Schutz, weder digital noch analog. In unserer Hand liegt jedoch, wie wir uns vorbereiten, wie wir Basisgrundschutz umsetzen, wie wir reagieren und wie wir zusammenarbeiten. Es geht in erster Linie darum, einige Basics umzusetzen. Wir müssen uns mit Szenarien auseinandersetzen, Informationen teilen, Angriffsvektoren analysieren und geeignete Gegenmaßnahmen ergreifen. Wenn etwas passiert, dann geht es darum, Schaden und Auswirkungen, soweit es geht, zu minimieren. Dafür braucht es klare Abläufe, Zuständigkeiten und je nach Angriff etablierte Kontakte und Unterstützungsstrukturen.

Zu guter Letzt: Es braucht offene Kommunikation und kurze Wege. Unternehmen und Behörden müssen sich gegenseitig informieren können, Wissen zusammenführen und sich über Angriffe und Best Practice vertrauensvoll austauschen. Für all das braucht es einen institutionellen Rahmen und natürlich auch Ressourcen, und das möchte ich einmal kurz für Berlin durchgehen.

Die neue Cybersicherheitsstrategie der Senatskanzlei betont völlig zu Recht, wie wichtig die Vernetzung von Landes- und Bundesebene ist. Cyberangriffe und hybride Bedrohungen kennen schlichtweg keine Ländergrenzen. Es ist daher begrüßenswert, dass der Senat bis Ende des Jahres endlich eine Kooperationsvereinbarung mit dem BSI abschließen möchte. Zehn Bundesländer haben bereits solche Kooperationen mit dem BSI. Berlin ist also Nachzügler, kein Vorreiter, und das als Hauptstadt und kleiner Stadtstaat. Das BSI bündelt wichtiges Wissen, technisches Know-how, ist international bestens vernetzt und erhält durch die NIS2-Umsetzung zudem noch weitere Befugnisse. Von dieser Kooperation kann Berlin nur profitieren und sollte schnellstmöglich nachziehen.

Am Ende ist Sicherheit aber eine Frage von Ressourcen und Kapazitäten. Das gilt für Unternehmen genauso wie für Senat, Sicherheitsbehörden und Verwaltung. Wir begrüßen es daher sehr, dass die Zentrale Ansprechstelle Cybercrime beim LKA im neuen Doppelhaushalt mit einem ordentlichen Mittelaufwuchs bedacht wird, zumindest soweit wir das von außen beurteilen können. Als IHK arbeiten wir recht eng mit den Kollegen der ZAC zusammen, organisieren gemeinsam einmal im Quartal eine Cybersicherheitssprechstunde, und die wird von unseren Unternehmen bestens angenommen, genauso wie die ZAC-Vorträge bei uns am IT-Sicherheitstag, die regelmäßig sehr voll sind. Die ZAC leistet extrem wertvolle Arbeit, egal ob Awareness- und Öffentlichkeitsarbeit oder direkte Unterstützung und Beratung von Unternehmen bei IT-Sicherheitsvorfällen. Wir können dem Senat also nur empfehlen, die ZAC weiter konsequent zu stärken und für ihre weitreichenden Aufgaben mit entsprechenden Ressourcen auszustatten.

Genauso wichtig sind die Kooperation und der Informationsfluss zwischen Behörden, Wirtschaft und Wissenschaft. Auch das unterstreicht die Cybersicherheitsstrategie. Unternehmen wünschen sich besseren Zugang zu aktuellen Informationen, Lageberichten und Einschätzungen der Behörden. Das hat der Stromausfall in Adlershof gezeigt, bei dem uns mehrere Unternehmen im Nachgang kontaktiert haben und über einen teils unzureichenden Informationsfluss geklagt haben. Teilen ist dabei keine Einbahnstraße. Gerade größere Konzerne, KRITIS-Betriebe und IT-Sicherheitsfirmen verfügen über wertvolle Informationen und Kompetenzen, um in Krisensituationen zu unterstützen. Darauf sollten die Berliner Behörden besser zugrei-

fen können. Diese Diskussion um das Teilen von Informationen ist definitiv nicht neu. Das BSI baut seit längerer Zeit ein Information Sharing Portal auf, und in der Cybersicherheitsagenda ist sogar von einem zivilen Cyberabwehrsystem die Rede.

In Berlin haben wir, so haben wir es schon skizziert, die SiPa, die AG KRITIS und auch das Lagebild Berlin. Aber dieser Status quo reicht aktuell nicht aus, um mit den hybriden Bedrohungen und immer engeren Einschlägen mitzuhalten. Wenn die Senatskanzlei in der Cybersicherheitsstrategie selbst betont, dass – ich zitiere einmal – „eine der größten Herausforderungen“ „die Entwicklung eines kohärenten und belastbaren Rahmens“ für die Zusammenarbeit von öffentlichen und privaten Akteuren ist, dann sollten dem auch konkrete Ideen und Maßnahmenvorschläge folgen, wie wir uns besser aufstellen, wie Wirtschaft und Behörden zusammenarbeiten können, und das bestenfalls direkt operationalisiert mit Zeitplänen, Beteiligten und Zuständigkeiten. Hier hätten wir uns deutlich mehr Klarheit, Commitment und Beteiligungsmöglichkeiten gewünscht.

Ein letzter Punkt noch, weil es eben angeklungen ist: das Thema digitale Souveränität. Auch da sind wir als IHK recht aktiv. Wir haben Anfang des Jahres eine größere Umfrage durchgeführt, an der sich 500 Unternehmen beteiligt haben. Das Thema ist in der Wirtschaft wahnsinnig relevant. 80 Prozent der Unternehmen haben uns zurückgemeldet, dass sie glauben, das Thema wird angesichts der aktuellen geopolitischen Verschiebungen weiter an Bedeutung gewinnen. Viele Unternehmen setzen schon Open-Source-Lösungen ein, und – da hat Berlin den Segen als Digitalhauptstadt – es gibt genug Anbieter, die schon gute Arbeit im Bereich Open Source und Digitalsouveränität leisten. Wenn es, wie Herr Atug skizziert hat, Ideen gibt, stärker die ZenDiS einzubinden, sollte Berlin das auf jeden Fall wahrnehmen. Dazu gibt es hoffentlich in den nächsten Monaten die lange angekündigte Strategie für Open Source oder digitale Souveränität, die die Senatskanzlei vorbereitet. – Vielen Dank!

Vorsitzender Florian Dörstelmann: Vielen Dank, Herr Holst! – Dann für Stromnetz Berlin Herr Rütting – bitte, Sie haben das Wort!

Thomas Rütting (Stromnetz Berlin GmbH): Herzlichen Dank! – Sehr geehrter Herr Vorsitzender! Sehr geehrte Abgeordnete! Sehr geehrte Frau Senatorin! Sehr geehrte Damen und Herren! Ich bedanke mich im Namen von Stromnetz Berlin für die Einladung zur heutigen Anhörung! Wir verstehen uns als wichtiger Partner der Politik, um die Krisenresilienz unserer Stadt gemeinsam zu stärken. Ich bin Leiter des Politik- und Kommunikationsbereichs bei Stromnetz Berlin. Zusätzlich fungiere ich als Mitglied unserer dreiköpfigen Krisenstabsleitung. Beim Anschlag in Johannisthal war ich daher eng eingebunden. Unser Vorsitzender des Krisenstabs und Bereichsleiter Systemführung und Betrieb, Herr Schunk, ist ebenfalls anwesend.

Lassen Sie mich zum heutigen Thema einleitend ein paar wichtige Punkte für den größeren Kontext aus Sicht von Stromnetz Berlin sagen. Das Berliner Stromnetz steht vor einem gewaltigen Wandel. Bis 2033 verdoppeln wir unsere Leistungskapazität. Das ist ein Wachstumsschub, wie ihn unser Netz noch nie gesehen hat. Das allein ist eine immense, aber auch sehr sinnstiftende Aufgabe, der wir uns gern stellen. Doch wir stehen auch vor Aufgaben, von denen wir wünschen würden, dass sie nicht notwendig werden, nämlich unser Netz krisenfest zu machen gegen äußere Bedrohungen. Die Herausforderungen für kritische Infrastruktur haben sich durch geopolitische Spannungen, Cyberangriffe und hybride Gefahren fundamen-

tal verändert. Drohnenüberflüge, Hackerangriffe, Sabotage – wir müssen künftig eher mit mehr als mit weniger davon rechnen. Wir selbst hatten Brandanschläge oder Fälle von Brandstiftungen in den Jahren 2018, 2021 und nun zuletzt im September 2025. Andere Betreiber kritischer Infrastruktur in Berlin sind ebenfalls betroffen, aber auch Netzbetreiber in benachbarten Bundesländern berichten von Sabotage, Einbrüchen ohne Diebstahl oder Manipulationen an Zäunen.

Für den Bereich Cybersicherheit sieht es ähnlich aus. Seit 2022 haben sich die an das BSI gemeldeten Sicherheitsvorfälle im Energiesektor um circa 60 Prozent erhöht. Unser Security Operation Center bearbeitet mehr als 10 000 Sicherheitsereignisse und Alarme pro Jahr. Das alles sind Puzzleteile einer veränderten Sicherheitslage. Das müssen wir bei allen weiteren Planungen im Hinterkopf haben. Was dabei stets unverändert bleibt, ist unser Selbstverständnis: Verantwortung tragen, vorausschauend und vorsorgend für unsere Stadt handeln. Darum widmen wir uns diesen Herausforderungen mit aller Kraft und wollen gemeinsam mit der Stadtgesellschaft weitere Schritte in Richtung mehr Krisenresilienz unternehmen.

Lassen Sie mich ein paar Beispiele dafür geben, was wir bereits ganz konkret tun. Resilienz beginnt mit der eigenen Organisation. Deshalb haben wir eine neue Abteilung Unternehmenssicherheit für eine höhere interne Priorität und Sichtbarkeit geschaffen. Wir sensibilisieren unsere Belegschaft fortlaufend durch Security-Newsletter zur Krisenvorsorge oder durch Auswertung und Verteilung von Sicherheits- und Warnhinweisen. Wir schulen zu Sabotage, Spionage und Anbahnungsversuchen und üben regelmäßig Krisenszenarien.

Unsere Infrastruktur – das klang schon an –: 99 Prozent unseres Netzes verlaufen unterirdisch, der beste Schutz vor physischen Angriffen. Womöglich verlegen wir weitere Leitungen unterirdisch. Wir bauen Versorgungswege in ausfallsicherer Trassenführung aus. Das sind zusätzliche Leitungen, die im Ernstfall einspringen können. Wir verstärken kritische Netzknoten und setzen auf intelligente Netztechnologien, die Störungen leichter erkennen und Lastflüsse umleiten lassen. Dabei ist Zusammenarbeit entscheidend. Wir pflegen gemeinsam mit unserer Mutter, der BEN, eine enge Zusammenarbeit mit Polizei, Feuerwehr, Bezirken und Senatsverwaltungen. Wir nehmen an Austauschrunden der bezirklichen Katastrophenschutzbeauftragten teil, etwa am Blaulichtstammtisch in Marzahn-Hellersdorf, und sprechen mit Feuerwehr, Polizei und THW über Erfahrungen aus Krisenfällen. Diese Vernetzung hat sich auch im Fall von Johannisthal bewährt.

Cybersicherheit hat für uns höchste Priorität und ist ja heute Teil dieser Anhörung. Während aktuell die Aufmerksamkeit sehr auf dem Schutz physischer Infrastruktur liegt, sollten wir diese Bedrohungslage nicht unterschätzen. Wir implementieren umfassende Schutzmaßnahmen nach anerkannten Standards und regulatorischen Auflagen. Unser Netzleitsystem unterliegt strengen Anforderungen aus dem Energiewirtschaftsgesetz und muss konkrete ISO- und IEC-Normen erfüllen. Die Empfehlungen des BSI fließen fortlaufend in unsere Schutzkonzepte ein. Wir setzen eine strenge Segmentierung der Netzwerke zwischen Verwaltungs-IT einerseits und Operational Technology andererseits um, wie es die BSI-Handlungsempfehlungen vorgeben. Implementierte Maßnahmen prüfen wir regelmäßig auf Wirksamkeit. Reaktive Maßnahmen üben wir szenariobezogen mit sogenannten Playbooks. Wir haben ein eigenes Security Operation Center etabliert, das die Bedrohungslage analysiert, Schwachstellen bewertet und Sicherheitsalarme auswertet, und wir nehmen wo möglich an firmen- und branchenübergreifenden Notfallübungen teil, die auch Cyberangriffe umfassen. Der Anschlag in

Johannisthal hat gezeigt: Wir sind handlungsfähig. Unsere Meldeketten, Einsatzpläne, das Lagemonitoring haben funktioniert. Die Katastrophenschutzleuchttürme waren wichtige Anlaufstellen für die Anwohnerinnen und Anwohner. Die angesichts des großen Schadens schnelle Wiederherstellung war nur möglich, weil wir Material, Personal, Know-how und Partnerfirmen direkt vor Ort hatten, alles Ergebnis unseres Resilienzkonzepts.

Natürlich nehmen wir solche Störungen zum Anlass, unsere Maßnahmen zu überprüfen und neue Verbesserungspotenziale zu identifizieren. Wir müssen und werden uns weiterentwickeln und hier als Stromnetz verantwortungsvoll vorangehen. Aber eines ist mir wichtig: Einen hundertprozentigen Schutz vor Ausfällen wird es nie geben. Jeder weiß, dass beim Betrieb eines Stromnetzes Störungen auftreten können. Grundsätzlich sind wir auch hier gut aufgestellt. Unsere durchschnittliche Unterbrechungsdauer lag 2024 bei 8,5 Minuten pro Kunde, das ist deutlich unter dem Bundesdurchschnitt. Doch durch die neue Sicherheitslage ist nun ein weiterer Risikofaktor hinzugekommen, und darauf müssen wir uns gemeinschaftlich neu einstellen. Wir tun unsererseits alles, um die Wahrscheinlichkeit von Ausfällen auf das minimal mögliche Maß zu reduzieren sowie auf einen Störungsfall optimal vorbereitet zu sein. Dabei ist eines klar: Resilienz ist eine Gemeinschaftsaufgabe. Wir brauchen gute Koordination aller Akteure – Behörden, Politik, Infrastrukturbetreiber, Hilfsorganisationen –, und natürlich müssen auch unsere Kundinnen und Kunden auf den Ernstfall vorbereitet sein. Jeder kann und muss seinen Teil dazu beitragen. Das ist kein Alarmismus, sondern vorausschauende Vorbereitung. Wir als Stromnetz Berlin leisten unseren Anteil und gehen verantwortungsvoll voran. Lassen Sie uns gemeinsam daran arbeiten, Berlin jederzeit am Laufen zu halten! – Vielen Dank! Wir freuen uns auf Ihre Fragen.

Vorsitzender Florian Dörstelmann: Vielen Dank, Herr Rütting! Vielen Dank auch, dass Sie so freundlich waren, Herrn Schunk als Bereichsleiter Systemführung und Betrieb zu benennen, denn das ist mir vorhin bei der Begrüßung entfallen. – Herr Schunk, bitte, Sie haben das Wort!

Jürgen Schunk (Stromnetz Berlin GmbH): Ich habe keinen Vortrag am Anfang. Ich würde gern auf die Fragen eingehen, die von Ihnen oder Ihren Kollegen gestellt werden.

Vorsitzender Florian Dörstelmann: Vielen Dank! Dann verfahren wir so. – Dann hat zunächst der Senat das Wort für eine Stellungnahme. – Frau Senatorin Spranger, Sie haben das Wort!

Senatorin Iris Spranger (SenInnSport): Vielen Dank! – Sehr herzlichen Dank auch für die Ausführungen der Fachleute, die das gerade aus ihrer Sicht vorgenommen haben. Herzlichen Dank dafür! Ich möchte nicht nur allein hier reden, sondern Sie haben selbst ausgeführt, dass die Senatskanzlei selbstverständlich für das ITDZ, die IT-Struktur im Land Berlin, zuständig ist. Deshalb habe ich Unterstützung aus der Senatskanzlei, und zwar Herrn Dr. Kroll-Peters und Frau Gieseler, die dann aus ihrer Sicht die Bewertung der Anzuhörenden vornehmen können. Zur Polizei selbst kann Herr Steiof noch etwas sagen. Ich unterstütze das natürlich und bedanke mich, dass Ihnen das im Haushalt aufgefallen ist, dass das LKA mehr Geld bekommt. Das ist für uns aufgrund der aktuellen Situation sehr wichtig. Ich habe das gemeinsam mit der Polizei in den Vordergrund stellen können. Das war mir sehr wichtig, und deshalb herzlichen Dank, dass Sie sich unseren Einzelplan auch in dieser Hinsicht mal angeschaut haben! Das ist so, und selbstverständlich werden wir das stärken.

Um den aktuellen Herausforderungen für kritische Infrastruktur in allen Bereichen zu begegnen, haben wir uns innerhalb der Senatsverwaltung für Inneres und Sport stark aufgestellt. Es wurde hier schon gesagt: Wir haben bereits im Jahr 2023 unsere Koordinierungsstelle Kritische Infrastruktur aufgebaut und befinden uns hier im kontinuierlichen Austausch mit den relevanten Akteuren und in der Weiterentwicklung der Zusammenarbeit. Unsere Koordinierungsstelle KRITIS koordiniert einerseits die jeweiligen KRITIS-Fachaufsichten und ist andererseits selbst Wissensspeicher. Sie haben es ausgeführt, und ich habe es schon mehrfach gesagt: Die Katastrophenschutzbehörden sind die Bezirke und die einzelnen Senatsverwaltungen. Wir koordinieren. Die Koordinierungsstelle organisiert für Betreiberinnen und Betreiber von kritischer Infrastruktur regelmäßig Austauschveranstaltungen, den sogenannten Arbeitskreis Infrastrukturbetreiber. Erst im Sommer ist die Koordinierungsstelle KRITIS in diesem Format bei zwei Terminen persönlich sowohl mit den Fachebenen als auch mit den Leitungsebenen zu einem intensiven persönlichen Austausch zusammengekommen. Diese Formate werden von den Unternehmen sehr wertgeschätzt und positiv angenommen. Die Koordinierungsstelle KRITIS zieht im Gegenzug aus den Terminen wertvolle Impulse für die Ausgestaltung der Zusammenarbeit und der Bedarfe der Unternehmen. Daneben finden selbstverständlich zahlreiche anlassbezogene direkte Gespräche miteinander statt. Hierbei darf man nicht vergessen, dass die Fachaufsicht und die Verantwortung im Sinne des Katastrophenschutzes für den jeweiligen KRITIS-Betreiber in der jeweiligen für das Ressort und den Sektor zuständigen Senatsverwaltung liegt und der Senatsverwaltung für Inneres und Sport, ich habe es eben schon gesagt, durch das Katastrophenschutzgesetz Berlin vorrangig ein koordinierender Auftrag zukommt.

Unser Schwerpunkt lag und liegt in diesem Rahmen zunächst auf der physischen Sicherheit von kritischer Infrastruktur, da die Unternehmen mit dem Bundesamt für Sicherheit in der Informationstechnik im Bereich Cybersicherheit bereits einen starken Partner an ihrer Seite haben. Das Bundesamt für Sicherheit in der Informationstechnik unterstützt die Betreiberinnen und Betreiber von KRITIS. Ihm gegenüber weisen sie entsprechende Zertifizierungen nach, und sie sind dem BSI gegenüber bei Sicherheitsvorfällen direkt meldepflichtig. Dazu wird die Senatskanzlei noch etwas ausführen.

Die Betreiberinnen und Betreiber von KRITIS haben den Wunsch geäußert, und das kam auch hier noch mal zum Ausdruck, dass wir ihnen ergänzend dazu zu Herausforderungen der Cybersicherheit ein regelmäßiges Austauschformat bieten sollten. Unsere Koordinierungsstelle wird gemeinsam mit der in diesem Jahr gegründeten Koordinierungsstelle Cybersicherheit selbstverständlich in Kürze ein solches Austauschformat aufstellen. Unsere Koordinierungsstelle Cybersicherheit ist zudem so mit dem Bundesamt für Sicherheit in der Informationstechnik verzahnt, dass wir der Single Point of Contact für das Land Berlin in strategischen und koordinativen Angelegenheiten sind.

Die Senatskanzlei wird das jetzt ausführen. Herr Steiof wird noch für die Polizei etwas ausführen, weil die Polizei ein eigenes System hat. Insofern trifft vieles, was Sie hier an Fragestellungen genannt haben, für die Polizei in der Form nicht zu. Aber wir alle wissen, und deshalb bin ich dankbar dafür, dass das heute gemeinsam mit den Anzuhörenden als Anhörung gemacht wird, wie hoch die Zahl der Cyberangriffe jeden Tag in Berlin auf KRITS beziehungsweise auf die Verwaltung ist. Deshalb würde ich jetzt sehr gern mit Zustimmung des Ausschussvorsitzenden an die Senatskanzlei übergeben.

Vorsitzender Florian Dörstelmann: So machen wir es. Vielen Dank, Frau Senatorin Spranger! – Dann beginnen wir mit Herrn Dr. Kroll-Peters und im Anschluss machen wir mit dem LKA-Chef weiter. – Herr Dr. Kroll-Peters! Sie haben das Wort.

Dr. Olaf Kroll-Peters (SKzl): Schönen guten Tag! Für alle, die mich noch nicht kennen: Ich bin der Landesbevollmächtigte für Informationssicherheit – in Klammern: v – und heute kurz hierhergekommen. Leider muss ich in sechs Minuten meinen Zug bekommen. Demzufolge habe ich meine Kollegin mitgenommen. Ich werde jetzt ganz schnell reden und versuchen, noch ein paar Anmerkungen zu machen.

Zu den Leitlinien: Ja, es ist richtig, die im Internet sind tatsächlich alt. Allerdings rede ich immer von beiden Leitlinien. Wir haben beide Leitlinien überarbeitet. Für mich sind das wahnsinnig wichtige strategische Eckpfeiler. Wir haben die noch nicht veröffentlicht, weil gerade der BSI-Grundschutz überarbeitet wird. Ich sitze mit im Expertengremium und arbeite mit daran, wie der Grundschutz++ aussehen wird. Der wird auch ein bisschen auf die Leitlinien Rückwirkungen haben. Der IT-Planungsrat, da sitze ich auch mit in der Bearbeitungskommission, überarbeitet auch seine Leitlinie. Damit Sie eine Vorstellung haben: Wir haben früher gedacht, man muss Mitarbeiter schulen, jetzt reden wir davon, dass man das Sicherheitspersonal auf jeden Fall qualifizieren muss. Da wird es direkte Ergüsse für unsere Leitlinie geben. Demzufolge werden sie, hoffe ich, noch dieses Jahr gezeichnet. Sie liegen vor. Wer mal draufgucken möchte, kann gern mitarbeiten. Das sind für mich aber zwei strategische Dokumente.

Die Kooperation mit dem BSI haben Sie angesprochen. Wir haben vor einem Jahr bei dem BSI die Dokumente ausgefüllt, dem BSI gegeben. Leider gibt es da gerade so einen kleinen Fragenkatalog zwischen BMI und BSI, und wenn sie das irgendwann geklärt haben, werden sie uns vielleicht auch mal in den Kreis der Erlauchten, die so eine Kooperationsvereinbarung haben, aufnehmen. Das wäre für uns letztens ganz hilfreich gewesen, denn da haben wir extra wegen Diensten angefragt, die wir ganz gern gehabt hätten. Wir sind auch proaktiv unterwegs. Wir sind letztens auf der it-sa, einer große Sicherheitskonferenz, rumgerannt und haben mal nachgefragt, warum die Bayern ihre Kooperationsvereinbarung kriegen und wir noch nicht. Da hat man vonseiten der Kollegen gelobt, dass wir uns irgendwann auch dazu machen.

Dann NIS2: Da war ich gerade ein bisschen verwundert, denn natürlich gilt die NIS2 auch für uns. Wir haben für die NIS2 das eine Feigenblatt, das der Kollege gerade genannt hat, erlassen, die Cybersicherheitsstrategie, denn das ist eine Forderung, dass wir die haben müssen. Für mich noch viel relevanter – hier gerade noch nicht thematisiert, das wundert mich ein bisschen –, ist das Festsetzungsschreiben zur NIS2, weil da der Informationssicherheit sehr viel größere Rechte gegeben werden. Allerdings ist das auch sehr juristisch benannt, und wir sind gerade dabei, wirklich klar zu belegen: Was bedeutet denn „Der Landesbevollmächtigte für Informationssicherheit stellt sicher, dass die Maßnahmen beaufsichtigt und umgesetzt werden“? – Das muss noch klarer gefasst werden. Da sind wir gerade dran.

Die Windows-10-Umstellung haben Sie noch angesprochen, für mich ein total relevantes Thema, allerdings ist es für mich, ehrlich gesagt, nicht wirklich ein technisches Thema. Für mich ist das ein Thema im Kopf, denn so einen Rechner von Windows 10 auf Windows 11 zu bringen, ist für mich als Techi nicht wirklich schwierig, aber bei den ganzen Fachverfahren, den Fragestellungen, die im Zusammenhang damit zu klären sind, haben wir ein echtes Prob-

lem, dass man sich denkt, der Support läuft irgendwann aus, und dann stellen wir unsere Fachverfahren um. Nein! Wir haben beim ITDZ eine Arbeitsgruppe, um die End-of-Life-Systeme im ITDZ zu vermeiden. Da haben wir mittlerweile ein kleines Projekt gestartet, wo wir drei Jahre im Vorfeld schon erkennen und auch Maßnahmen ergreifen, wann Sachen End of Life laufen beziehungsweise nicht mehr supportet werden. Zurzeit behilft man sich damit, dass man diesen sogenannten erweiterten Support, die ESU, kauft. Das ist meiner Meinung nach nicht der Goldstandard. Das muss sich irgendwann ändern, aber es muss in den Köpfen anfangen, dass wir verstehen, dass wir bei einer Software, wenn sie beispielsweise am 31. Oktober 2025 End of Life ist, spätestens drei Jahre vorher schon mal darüber nachdenken müssen, diese aus dem Verkehr zu ziehen und was da alles dranhängt. Da reden wir, machen wir. Das Monitoring, das wir gerade im ITDZ aufgesetzt haben, drei Jahre in die Zukunft zu gucken, müssen wir irgendwann noch auf das Land Berlin ausbreiten. Da sind wir gerade dran. – So viel zu den Sachen, die ich mir schnell notiert habe.

Vielleicht auch noch zur Windows-10-Umstellung: Das ist ja nur eines der Themen, die wir gerade rocken müssen, wo man in die Zukunft gucken muss, hätte gucken sollen. So ähnlich ist es bei der IPv6-Umstellung, und da haben wir als Informationssicherheit diesen Weg beschritten, dass wir in die Expertengremien und Konferenz des Bundes mit reingehen, um da schon mal dieses Wissen für das Land Berlin abzugreifen und im Land Berlin zu verteilen, auch wenn ich, ganz ehrlich gesagt, denke, Informationssicherheit ist da nicht der beste Stakeholder, aber ich finde es interessant, und demzufolge machen wir das einfach. – Jetzt muss ich leider ganz schnell zu meinem Vortrag rennen, den ich gleich in Köln halten muss. Ich habe Ihnen aber eine super Vertretung mitgebracht, meine Vertreterin Frau Gieseler wird bestimmt sämtliche Fragen beantworten können. – Vielen Dank!

Vorsitzender Florian Dörstelmann: Vielen Dank, Herr Dr. Kroll-Peters! Dann verfahren wir mit Einverständnis des Senats so, dass nun Frau Gieseler direkt anschließt und danach Herr Steiof. So habe ich es verstanden. – Frau Gieseler, bitte, Sie haben das Wort!

Sonja Gieseler (SKzl): Im Prinzip nur zur Ergänzung: Wir arbeiten natürlich noch bundesweit in vielen anderen Gremien mit. Dadurch, dass Berlin den Vorteil hat, ein Bundesland und auch eine Einheitsgemeinde zu sein, gilt die NIS2 auch für die Bezirke, und im Rahmen des einen Sektors, der die Informationssicherheit im Land Berlin ist, haben wir auch Qualifizierungsmaßnahmen. Es findet im November eine Qualifizierungsmaßnahme der hohen Leitungsebene im Parlament statt. Das ist gerade alles geregelt worden. Von daher haben wir schon viele Sachen durch das Festsetzungsschreiben als Ermächtigung durchführen können. Es ist natürlich noch die Spitze des Eisbergs. Wir werden ganz viel machen. Es ist bekannt, wie mein Kollege gerade sagte: Wir haben alleine 52 Maßnahmen für die Etablierung des Berlin-CERT auf die NIS2-Ebene identifiziert. Da sind wir gerade im engen Austausch mit dem ITDZ, um auch Roadmaps zu sehen, denn Sie können sich vorstellen, die Personaldichte in diesem Bereich ist nicht so hoch, dass wir gleich auf 100 Prozent Erfüllung gehen werden. Aber diese Sachen sind alle bekannt, und wir reden über einige Artikel der NIS2, die noch mit Leben zu befüllen sind. Also von daher: Es ist bekannt. Das Land Berlin wird es umsetzen, und durch das Festsetzungsschreiben, das zum Glück am 30. Mai erfolgt ist, haben wir die Ermächtigung genau in diesem Sektor die ganzen Herausforderungen anzunehmen. Dazu gehört Schwachstellenmanagement, Spam-Analyse-Sachen. Wir wollen, dass sich die Mitarbeiter, denen entsprechend der Sensibilisierung immer mehr auffällt, was ich sehr schön zu bemerken finde, immer mehr melden: Da ist eine Mail ein bisschen komisch –, und jetzt werden

sie das nötige Werkzeug bekommen, damit sie nur noch ihren Verdacht melden und auch Rückmeldungen bekommen, immer im Feedbacksystem. Wir sind sehr dankbar, solche Sachen zu haben. Wir sind uns einig, wie auch die Experten gesagt haben: Es geht nicht mehr darum, ob wir angegriffen werden, sondern nur noch um das Wann und wie schlimm und wie schnell wir alles wiederherstellen können. Von daher gibt es ja gerade die Maßnahmen, die wir jetzt machen. Wir nehmen auch an der Bearbeitung der Sicherheitsvorfälle, so wie wir sie identifizieren, oder auch bei Verdacht nehmen Herr Dr. Kroll-Peters und ich schon in Person teil.

Zu mir: Ich bin eine ausgebildete BSI-Beraterin. Von daher bin ich beratungstechnisch sehr gut in der Lage zu fragen, was das BSI-Grundschutz-Kompendium angeht. Ich habe 31 Jahre im ITDZ gearbeitet, ich bin trotzdem nett, und war dort im BSI-Team. Mir tut es manchmal leid für die Kollegen, denn dort gibt es sehr fähige und sehr fortschrittliche Sachen. Ich gehörte zum BSI-Team, weil das der Dienstleister ist, BSI-zertifiziert, und bitte nicht immer nur, wie alle denken, aufgrund eines Systems, sondern die gesamte Basisinfrastruktur ist bereits seit 2018 BSI-zertifiziert, und dazu gehören auch die standardisierten Schnittstellen des Netzes des Bundes.

Vorsitzender Florian Dörstelmann: Vielen Dank, Frau Gieseler! – Dann kommen wir noch zum Leiter des LKA. – Herr Steiof, bitte, Sie haben das Wort!

Christian Steiof (LKA Berlin): Zu den alarmierenden Zahlen von Herrn Atug eine kleine Korrektur: Stand jetzt sind von den 17 300 PCs der Berliner Polizei gegenwärtig 16 112 umgestellt auf Windows 11, und wir planen, bis 10. November komplett umgestellt zu haben. Insofern Entwarnung, zumindest für die Polizei kann ich das sagen.

Ich möchte ein paar Bemerkungen machen, weil bei uns sehr häufig das Thema Cybercrime sehr diffus und sehr unterschiedlich gehandhabt wird. Wir als Polizei haben seit vielen Jahren bundesweit eine einheitliche Definition, bedeutet, wir unterscheiden zum einen Cybercrime im weiteren Sinne. Das ist im Grunde genommen: Alles, was Sie in der analogen Welt an Kriminalität haben, passiert auch irgendwie im Cyberraum, sämtliche Straftaten, die man sich vorstellen kann, Rauschgifthandel, Waffenhandel, Hasskriminalität, Betrug und so weiter. All diese Dinge bearbeiten wir nicht speziell, sondern in den zuständigen Bereichen der Polizei.

Der zweite Bereich ist Cybercrime im engeren Sinne. Das sind die Dinge, die auf informationstechnische Systeme abstellen. Ein Teil dieses Cybercrime im engeren Sinne sind die sogenannten Cyberangriffe, wo das System selbst entweder durch Menschen oder ein anderes System automatisiert angegriffen wird. Da gibt es im Wesentlichen die Dinge, die uns sehr stark beschäftigen und sehr viel Spezialwissen erfordern, Verschlüsselungsangriffe, im Wesentlichen Dinge, die mit Ransomware erfolgen, wo ganze Systeme lahmgelegt werden, oder solche Überlastungsangriffe, die man gemeinhin als DDoS-Angriffe bezeichnet. In beiden Bereichen verzeichnen wir erstaunlicherweise nicht nur Steigerungen, aber wir verzeichnen, dass immer weniger Privatpersonen betroffen werden, sondern immer mehr Unternehmen, Firmen und KRITIS, aber auch Behörden, und dass die Maßnahmen, die von der Gegenseite getroffen werden, immer höheren Schaden verursachen und immer im wahrsten Sinne kritischer für uns werden. Deswegen sind wir im Landeskriminalamt vor fünf Jahren dazu übergegangen, eine spezialisierte Dienststelle, ein Cybercrime-Abwehrzentrum, zu gründen, wie es im Übrigen jedes Landeskriminalamt und das Bundeskriminalamt auch haben, und uns sowohl mit der

Wirtschaft, mit den KRITIS, zu vernetzen, mit anderen Behörden, aber natürlich auch untereinander. Es gibt gerade in diesem Bereich sehr viele Kooperationsvorhaben mit anderen Bundesländern und mit dem Bundeskriminalamt, weil die Angriffsvektoren zum Teil so spezialisiert sind, dass es einer oder ein Land in aller Regel nicht alleine hinkriegt, sondern sie Spezialisten mit unterschiedlicher Ausprägung aus allen Ländern brauchen, um bestimmte Analysen durchführen zu können.

In dieser Cybercrime-Stelle, die aus sehr hochengagierten und -spezialisierten Ermittlern, aber auch Fachleuten, die wir von außen eingekauft haben, besteht, haben wir die vorhin von Herrn Holst benannte ZAC angesiedelt, die Zentrale Ansprechstelle Cybercrime, die im Grunde genommen eine Anlaufstelle für möglicherweise polizeilich relevante Feststellungen aufseiten von Unternehmen oder Behörden darstellt, andererseits aber auch Vorträge und Sensibilisierung macht und sehr kompetent in verschiedenen Fachkreisen auftritt und auch sehr gefragt ist, kann ich sagen. Wir haben mittlerweile im Jahr etwa 3 000 Anfragen, die zum Teil in Ermittlungsverfahren münden; etwa 700 im Jahr werden allein aus diesem Kontakt durch die Zentrale Ansprechstelle Cybercrime generiert.

In den letzten Jahren stellen wir vermehrt fest, dass Ransomware, Angriffe oder DDoS-Attacken nicht ausschließlich aus wirtschaftlichen, also erpresserischen Gründen, gefahren werden. Das war in der Regel bis vor drei, vier Jahren der Fall. Da wurden dann in Kryptowerten Lösegelder erpresst. Der vorhin erwähnte Fall der Berliner Krankenhäuser war einer dieser Fälle. In den letzten Jahren stellen wir aber vermehrt Fälle fest, wo wir bundesweit sagen, das sind zumindest staatlich gelenkte oder autorisierte Akteure, die sich im Netz tummeln und solche Angriffe fahren, die dann keine wirtschaftlichen Interessen haben, sondern Interessen der Spionage oder einfach nur der Verunsicherung.

Intern: Wir haben eine Mischkalkulation bei der eigenen Sicherheit zum Schutz vor solchen Angriffen. Fast unser gesamter E-Mail-Verkehr läuft über das ITDZ, sodass wir da auch im engen Verbund sind. Allerdings haben wir als Behörde mit Ordnungs- und Sicherheitsaufgaben ein eigenes Netz, wo wir polizeiliche Vorgangs- und Fallbearbeitungssysteme fahren, wo wir unser Schmutzdatennetz zur Auswertung und Analyse fahren. Das wird von uns selbst gehostet und die Sicherheit hergestellt. Es sind im zweistelligen Bereich Menschen der zuständigen Stelle IKT in der Polizeidirektion Zentraler Service tagtäglich damit beschäftigt, im Netzwerk zu schauen: Wo sind neue Schwachstellen? Wo müssen wir Lücken schließen und Firewalls anpassen? –, sodass wir da, glaube ich, sehr gut aufgestellt sind. Allerdings stellen auch wir regelmäßig Versuche fest, insbesondere über Phishing-Mails, in die Systeme einzudringen. Wir sensibilisieren regelmäßig unsere Mitarbeitenden und bieten Fachvorträge an, wie man sich verhalten muss, verhalten sollte, wie die Meldewege sind. Wir haben einen internen Verbund zwischen interner Revision, IT-Sicherheitsmanagement, der IKT, dem LKA, sodass wir einen relativ schnellen Austausch haben, um gut einschätzen zu können, ob es neue Angriffsvarianten gibt, um die wir uns kümmern müssen. – Das soll es erst mal von mir gewesen sein. Danke!

Vorsitzender Florian Dörstelmann: Vielen Dank, Herr Steiof! – Dann kommen wir zur Aussprache. – Frau Abgeordnete Ahmadi, Sie haben das Wort!

Gollaleh Ahmadi (GRÜNE): Vielen Dank, Herr Vorsitzender! – Auch an unsere Experten vielen Dank für die Darstellungen! Was man im Großen und Ganzen zusammenfassen kann: Wir sind nicht vorbereitet. Auf der Berliner Landeswebseite heißt es, die kritischen Infrastrukturen seien besonders gefährdet. Ihre Ausfälle können nachhaltige Versorgungsengpässe oder erhebliche Sicherheitsstörungen verursachen. Der Verfassungsschutz Berlin weist in seinem Bericht darauf hin, dass Cyberspionage komplexer geworden ist und Berlin auf das Know-how des Bundes setzt, um Cyberangriffe gezielt abzuwehren. Wir sehen, wir leben mitten in hybriden Bedrohungen, so, wie eins zu eins aus Putins Playbook: tägliche Cyberangriffe, Cyberspionage, Angriffe auf kritische Infrastrukturen, auf Drittanbieter, wie wir es zum Beispiel am BER erlebt haben oder wie vor einem Jahr auf unser Gesundheitswesen – ein großes Beispiel ist das Berliner Johannesstift, das sich bis heute noch nicht ganz von dem Angriff erholt hat –, Desinformationskampagnen zur Destabilisierung der Gesellschaft und unserer Demokratie. Wir sehen, die Cybersicherheit ist nicht nur mit der Zuständigkeit komplett bei der Senatsinnenverwaltung – ich komme gleich dazu, Frau Senatorin –, sondern zurzeit eine der Kernaufgaben unserer sicherheitspolitischen Herausforderungen. Daher ist dieses Behördenpingpong zwischen IT-Sicherheit und Senatskanzlei unverständlich, aber auch, dass zum Beispiel eine Anfrage zum Angriffen auf Stromnetz Berlin von der Senatswirtschaftsverwaltung beantwortet wird und nicht von der Senatsinnenverwaltung. Wie die Zuteilungen da erfolgen, wissen Sie im Senat besser, jedoch zeigt es, dass man in besonderen Punkten nicht die Sensibilität der Lage erkennt.

Ich habe ein paar Fragen, zum einen an Sie, Herr Dr. Herpig. Wir haben von einigen unserer Anzuhörenden gehört, was die nächsten Schritte sein können. Herr Atug hat unter anderem das Windows-Update als einen der nächsten Schritte genannt. Was wären aus Ihrer Sicht die nächsten Schritte, die wir in Berlin unbedingt gehen müssen?

Weitere Fragen gehen direkt an den Senat: Der Senat beteuert in seinen Antworten auf unsere Anfragen regelmäßig, die Resilienz sei ausreichend, doch das Chaos am BER hat gezeigt: Berlins kritische Infrastruktur ist hochgradig verwundbar. Wie definiert der Senat überhaupt „ausreichend“, und auf welcher Grundlage kann eine solche Bewertung angesichts dieser Realität überhaupt noch aufrechterhalten werden?

Dann würde ich gern wissen, was der Senat konkret unternimmt, um Betreiber kritischer Infrastruktur nicht mit ihrer Verantwortung allein zu lassen, sondern sie aktiv und verbindlich in eine landesweite Sicherheitsarchitektur einzubinden. – Drittens: Wie viele zusätzliche Expertinnen- und Expertenstellen für das Berlin-CERT wurden tatsächlich geschaffen und besetzt, und wie will der Senat sicherstellen, dass diese Fachkräfte angesichts des massiven Wettbewerbs um IT-Sicherheitspersonal langfristig im öffentlichen Dienst gehalten werden? – Ich würde gern noch wissen: Berlin verfügt inzwischen über eine Cybersicherheitsstrategie, die im August 2025 veröffentlicht wurde. Es fehlt jedoch an klaren, überprüfbaren Meilensteinen. Wie will der Senat Transparenz über Fortschritte schaffen, wenn es keine messbaren Ziele dafür gibt? Reicht ein unverbindliches Rundschreiben des Senats wirklich aus, um eine der großen Sicherheitsbedrohungen unserer Zeit abzuwehren?

Des Weiteren – ich komme gleich zum Ende, Herr Vorsitzender – sprechen Sie von umfassenden Maßnahmen, aber ohne ausreichende finanzielle Mittel bleiben selbst die besten Strategien wirkungslos. Wie hoch sind die tatsächlich verfügbaren Mittel für die Weiterentwicklung des Berlin-CERT und des IKT-Notfallmanagements? Drohen die ambitionierten Pläne

nicht eine reine Schaufensterpolitik zu werden, wenn ich das hier so sagen darf, wenn das Budget dafür nicht ausreichend gesichert ist?

Zuletzt würde ich gern wissen: Die vorliegende Strategie beschreibt vor allem den Ist-Zustand, statt einen klaren Zukunftspfad zu zeichnen. Warum wagt der Senat nicht, klare, messbare Ziele für die kommenden Jahre zu definieren? Wir haben vorhin auch gehört, die Cybersicherheitsstrategie des Landes tritt erst in Kraft, wenn diese Legislaturperiode vorbei ist. Daher zur Reaktionszeit bei Angriffen oder zum Schutz kritischer Infrastrukturen: Verlieren wir dadurch nicht wertvolle Zeit? Wie wollen wir diese Zeit in den nächsten Monaten der Legislaturperiode noch nutzen? – Vielen Dank!

Vorsitzender Florian Dörstelmann: Vielen Dank, Frau Abgeordnete Ahmadi! – Ich habe als nächsten Herrn Abgeordneten Schrader, dann Herrn Abgeordneten Weiß, Herrn Abgeordneten Dregger und Herrn Abgeordneten Matz. Weitere Wortmeldungen liegen zurzeit nicht vor, sodass ich Ihnen vorschlagen würde, wenn Sie einverstanden sind, dass wir danach die Antwortrunde unserer Anzuhörenden haben und natürlich auch den Senat hören. – Dann verfahren wir so. Ich darf bitte alle noch mal daran erinnern, vielleicht die Beiträge im Bereich von maximal zwei bis drei Minuten zu halten. – Herr Abgeordneter Schrader, Sie haben das Wort!

Niklas Schrader (LINKE): Das werde ich schaffen. Danke, Herr Vorsitzender! – Ich glaube, Herr Herpig hat es ganz gut zusammengefasst, indem er gesagt hat, wir haben in den allermeisten Punkten überhaupt kein Erkenntnisproblem, sondern ein Umsetzungsproblem. In dem Sinne ist es unsere Aufgabe, hier weiter die Umsetzungsfragen auf die Tagesordnung zu holen und weiter darauf zu drängen. Insofern habe ich erst mal nur ein paar kurze Fragen.

Herr Kroll-Peters hatte in seinem Vortrag darauf hingewiesen, dass man bei der Überarbeitung der Leitlinie für die Informationssicherheit der Landesverwaltung mithelfen, sich beteiligen kann. Da wollte ich fragen, wie genau das funktionieren kann, an wen sich das konkret richtet oder inwieweit das institutionalisiert ist, und an die Anzuhörenden, welche Erfahrungen Sie bislang mit dieser Möglichkeit gemacht haben.

Eine Frage habe ich an Herrn Atug. Sie hatten darauf hingewiesen, dass es wichtig wäre, eine KRITIS-Verordnung zu erlassen, dass viele Bundesländer das schon gemacht hätten. Hätten Sie dort ein Beispiel für ein gutes Vorbild? Sind die in den Bundesländern eher alle gleich, oder unterscheiden die sich qualitativ, sodass Sie sagen könnten, was ein gutes Best-Practice-Modell für uns wäre?

Dann habe ich noch eine Frage, die wir, glaube ich, in der letzten Anhörung schon angesprochen hatten, aber die ich hier trotzdem noch mal aufwerfen will, weil wir gerade ein oder zwei konkrete Gesetzentwürfe im Geschäftsgang haben, die die Instrumente der Quellen-TKÜ und der Onlinedurchsuchung für Polizei und Verfassungsschutz vorsehen. Das ist in Berlin sehr konkret, aber es ist auch ein bundesweiter Trend, dass diese Instrumente bei den Sicherheitsbehörden auf dem Vormarsch sind und mehr angewandt werden, die Eingriffsschwellen tendenziell eher sinken. Wie würden Sie das beschreiben? Steht das nicht im deutlichen Widerspruch zur IT-Sicherheit und auch zum Berliner Koalitionsvertrag, den Herr Atug anfangs zitiert hat, und den dort genannten ambitionierten Zielen?

Die dritte Frage richtet sich an Herrn Rütting beziehungsweise Herrn Schunk zum Thema Stromnetz. Es wurde im Nachgang des Vorfalls in Adlershof diskutiert, dass bestimmte Informationen über das Stromnetz, die für den Anschlag relevant waren, im Internet frei verfügbar waren. Daher die Frage: Was sind denn Daten über das Stromnetz, die Sie proaktiv ins Netz stellen? Sie haben vielleicht als öffentliches Unternehmen noch einen anderen Maßstab an Transparenz und an Open Data als andere. Das hat alles erst mal seinen Sinn, aber was davon wäre möglicherweise ein Problem, was die Angreifbarkeit angeht, und inwieweit denken Sie gerade grundsätzlich bei der Auswertung der Ereignisse dieses Anschlags darüber nach? – Das wäre es erst mal. Vielen Dank!

Vorsitzender Florian Dörstelmann: Vielen Dank, Herr Abgeordneter Schrader! – Herr Abgeordneter Weiß, bitte, Sie haben das Wort!

Thorsten Weiß (AfD): Vielen Dank, Herr Vorsitzender! – Das Thema ist nicht neu, sondern begleitet uns schon länger. Auch wenn ich es gut finde, dass nach dem Brandanschlag in Treptow-Köpenick das Thema hier wieder auf die Tagesordnung gesetzt wurde, ist unsere Hoffnung, dass sich dahinter nicht nur wohlfeile Worte und Absichtserklärungen verbergen, sondern tatsächlich etwas Substanzielles dabei herauskommt. Tatsache ist, dass wir schon in der Vergangenheit immer wieder Empfehlungen erhalten haben, die wir teilweise heute auch von den Experten – bei denen ich mich auch bedanke – gehört haben. Ich verbinde das gleichzeitig mit der Frage an den Senat, was davon konkret angedacht beziehungsweise umgesetzt wurde.

Ich darf das hier noch mal ganz kurz zusammenfassen: Es wurde gefordert, dass wir auch in Berlin ein IT-Sicherheitsgesetz nach dem Vorbild von Baden-Württemberg mit einer zentralen Cybersicherheitsstelle bekommen sollen, Anbindung an das ITDZ, operative Befugnisse, Melde- und Koordinierungsfunktion sollen damit verbunden sein. Es wurde gefordert, dass ein jährlicher Lagebericht zur Cyber- und Informationssicherheitslage an das Abgeordnetenhaus gesendet werden soll, verpflichtende Anwendung der BSI-Standards in allen Behörden, regelmäßige Sicherheits- und Wiederherstellungsübungen, Einführung eines Cyber-Trainee-Programms und gezielte Förderung von Digitalfachkräften, Kooperation mit Berliner Hochschulen, Förderung quelloffener Softwarelösungen mit Wartungsverträgen, Ausschluss von Software, die Sicherheitslücken absichtlich offenhält. Da haben wir heute schon nicht nur die Forderung gehört, sondern teilweise auch Vollzugsmeldungen wie vom LKA, bloß ist das nur ein Baustein des Ganzen. Ergänzend dazu vielleicht noch die Fragen: Wird ein IT-Sicherheitsgesetz in Berlin vorbereitet, und gibt es zum Beispiel regelmäßige Cyber-Krisenübungen auf Landesebene?

Abschließend eine Frage, die mich noch interessiert: Diese ganzen Brandanschläge auf die Sicherheitsinfrastruktur in Berlin, sei es auf den öffentlichen Nahverkehr oder auch der Brandanschlag in Treptow-Köpenick, kommen nachgewiesenermaßen fast alle aus dem linksextremistischen, antifaschistischen Umfeld, und jedes Mal, wenn man den Senat oder die Innensenatorin dazu befragt, wie auch ich vor einiger Zeit im Plenum, wird richtigerweise darauf verwiesen, dass das alles im Sinne von Strafverfolgung aufgeklärt werden muss, aber mir fehlt total: Sie pumpen unfassbare Summen in einen politischen Kampf gegen rechts, aber ich habe überhaupt noch nie gehört, was Sie tun, um präventiv darauf hinzuwirken, dass sich diese Menschen, die diese Anschläge auf unsere Infrastruktur durchführen, überhaupt gar nicht in dem Maße radikalisieren, dass es zu diesen Anschlägen kommt. Das gehört im Zuge eines

Gesamtkonzeptes meiner Ansicht nach auch dazu. Vielleicht kann der Senat, wenn er auf diesem Auge nicht blind bleiben möchte, noch etwas dazu sagen. – Danke schön!

Vorsitzender Florian Dörstelmann: Danke, Herr Abgeordneter Weiß! – Herr Abgeordneter Dregger, Sie haben das Wort!

Burkard Dregger (CDU): Danke, Herr Vorsitzender! – Ich habe zunächst eine Frage an die Vertreter der Stromnetz Berlin GmbH, nämlich ob es bereits Cyberattacken gegeben hat, die zu Ausfällen im Bereich des Stromnetzes in Berlin geführt haben. Ich erinnere daran, dass der Anschlag auf die beiden Strommasten im Südosten, der einen nennenswerten Einfluss hatte, kein Cyberangriff, sondern ein analoger Angriff, im Grunde ein ganz simpler Brandbeschleunigerangriff gewesen ist, und ich würde gern mal wissen, ob Derartiges oder Ähnliches oder auch kleinere Ausfälle auf Cyberattacken zurückzuführen sind, um mal die Dimension verstehen zu können.

Zweite Frage an die Beteiligten: Es gibt diverse Webseiten im Netz, die unsere kritischen Infrastrukturen veröffentlichen, und zwar in jedem Detail. Die Webseite flosm.org veröffentlicht jedes Detail unserer Strominfrastruktur im Netz. Das ist ein privater Betreiber aus Hannover. Ich habe das gerade aufgerufen. Sie können hier jeden einzelnen Stromkasten in Berlin aufrufen, jeden einzelnen Strommasten, Sie können jedes einzelne Umspannwerk sehen. Ich frage mich, wie wichtig uns Open Data ist, wenn es um kritische Infrastrukturen und deren Veröffentlichung geht. Ich würde gern wissen, ob es aus Gründen der Sicherheit vor Anschlägen geboten wäre, derartige Veröffentlichungen zu unterbinden. Das würde allerdings eine gesetzgeberische Initiative erfordern.

Die dritte Frage richtet sich an die Landesverwaltung, insbesondere an das ITDZ und die Vertreterin der IT-Sicherheitsbevollmächtigten des Landes Berlin. Ich war damals an dem Gesetzgebungsverfahren zum E-Government-Gesetz beteiligt. 2016 haben wir uns in bester Zusammenarbeit mit dem Kollegen Kohlmeier von der SPD-Fraktion entschlossen, erste IT-Sicherheitsmaßstäbe gesetzlich zu regeln, ich hatte es vorhin genannt, den BSI-Grundschutz, das Berlin-CERT und die verschlüsselte Kommunikation innerhalb der Behörden, aber auch das Angebot, nach außen verschlüsselt zu kommunizieren. Sehen Sie Bedarf, weitere Standards gesetzlich zu regeln? Dann wäre es unsere Aufgabe hier als Gesetzgeber, das zu verschärfen. Die Frage nach dem IT-Sicherheitsgesetz für Berlin, die schon gestellt worden ist, geht in dieselbe Richtung. Brauchen wir ein eigenes IT-Sicherheitsgesetz, oder sind die Regelungen in § 4 und § 23 des E-Government-Gesetzes ausreichend?

Dann noch eine vierte Frage, wenn ich darf: Das ITDZ hat für uns eine zentrale Funktion. Das ITDZ soll die IT-Infrastruktur für die Berliner Behörden grundsätzlich liefern. Es gibt sogar eine Regelung über den Anschluss- und Benutzungszwang. Die dahinter stehende Überlegung damals bei unserem Gesetzgebungsakt war, dass wir erstens standardisieren und natürlich auch im Hinblick auf die IT-Sicherheit ein bestimmtes Mindestniveau dadurch erzwingen, dass wir die Zusammenarbeit mit dem ITDZ gesetzlich vorschreiben. Das ITDZ betreibt ja auch das Landesnetz. Ich würde jetzt gern von Ihnen die Bestätigung haben, dass das ITDZ jedenfalls die erforderlichen Kriterien des BSI-Grundschutzes vollständig erfüllt. So war es 2018, und es hat sich hoffentlich nicht geändert, obwohl die Anforderungen wachsen. Wenn das so ist, können Sie durch Ihre Dienstleistung für Berliner Behörden und auch für die Bezirke dieses Schutzniveau weiter gewährleisten? Sie betreiben das Landesnetz. Sie haben

selbst die Voraussetzungen, die Sie erfüllen. Was können die Bezirke und anderen Behörden noch falsch machen, um nicht dieses Schutzniveau selbst zu erfüllen? Das wäre meine weitere Frage. – Danke!

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

Martin Matz (SPD): Vielen Dank erst mal für die Beiträge in der ersten Runde und die weiterführenden Fragen! Da kann ich mich gern anschließen. Ich würde aber gern noch mal konkreter zu dem Vorfall mit dem Anschlag nachfragen, welche Rolle Redundanzen im Netz an der Stelle spielen können, um kurzfristig Auswirkungen schon zu verhindern. Wir haben zur Kenntnis nehmen können, dass es nach dem durch den Anschlag bedingten Ausfall zunächst am selben Tag noch möglich war, größere Teile des Versorgungsgebietes wieder zu versorgen, offensichtlich über andere Leitungen, die in denselben Bereich führen. Hätte, mal laienhaft ausgedrückt, ein stärkeres Durchziehen von Berlin mit weiteren 110-kV-Leitungen dazu beitragen können, sehr kurzfristig auch in den Bereichen, wo es zwei Tage gedauert hat, sie wieder an das Netz zu bekommen, den Strom wieder fließen zu lassen? Wenn diese Erkenntnis richtig ist, wie aufwendig wäre es, gegebenenfalls das Stromnetz in Berlin weiter anzupassen? Da reden wir wahrscheinlich über ziemlich erhebliche Investitionen, und schon sind wir wahrscheinlich auch in einer Form von Abwägung, inwieweit die gerechtfertigt oder möglich erscheinen. Vielleicht können Sie zu dem Bereich noch ein bisschen beitragen. – Danke schön!

Vorsitzender Florian Dörstelmann: Vielen Dank, Herr Abgeordneter Matz! – Jetzt geht mein Blick mal in Richtung des Senats. – Frau Senatorin, Sie haben das Wort!

Senatorin Iris Spranger (SenInnSport): Herzlichen Dank! – Ich darf die ersten Fragen beantworten und Klarstellungen vornehmen, und dann würde ich wieder die Senatskanzlei, die für die IT-Infrastruktur und für das ITDZ verantwortlich ist, noch mal bitten, weitere Ausführungen zu machen.

Vielleicht darf ich mit dem beginnen, was ich vorhin schon gesagt habe; ich wiederhole es aber gern. Wir haben die Fachaufsicht und die Verantwortung im Sinne des Katastrophenschutzes; für den jeweiligen KRITIS-Betreiber muss aber und ist auch die Katastrophenschutzbehörde das jeweilige Ressort. Frau Ahmadi, Sie haben es angesprochen: Warum spricht die Wirtschaftsverwaltung? – Ich kann es Ihnen ganz einfach sagen: weil die Katastrophenschutzbehörde für Stromnetz Berlin selbstverständlich Wirtschaft ist, weil Stromnetz Wirtschaft untersteht, völlig klar. Anderes Beispiel, auch heute genannt: Krankenhäuser – Gesundheitsverwaltung. Deshalb hat die Gesundheitsverwaltung, was KRITIS betrifft, selbstverständlich ihre Ausführungen gemacht. Wenn Sie das in den letzten Monaten verfolgt haben, hat die zuständige Senatorin sehr ausführlich gemeinsam mit den Krankenhäusern über ihre Struktur gerade dort gesprochen. Wenn Sie über den Justizvollzug sprechen: Dafür ist die Justiz verantwortlich. Die Justiz ist dann die Katastrophenschutzbehörde. Deshalb habe ich das vorhin sehr deutlich gesagt. Alle Senatsverwaltungen sind für die nachgeordneten Einrichtungen Katastrophenschutzbehörden, genau so, das wurde hier auch schon gesagt, wie die Bezirke wiederum Katastrophenschutzbehörden sind mit ihren entsprechenden Leuchttürmen. Auch das haben wir gesagt.

Die Meldeketten haben in Köpenick funktioniert, das wurde hier schon angemerkt, weil – wie soll ich das sagen? – die Koordinierung nicht nur über uns gelaufen ist, sondern weil das über die entsprechende Katastrophenschutzbehörde, das war damals der Bezirk, geklappt hat, ebenfalls wie die Stromnetz GmbH. Das darf ich hier noch mal sagen.

Der BER liegt in Brandenburg, das ist Ihnen bekannt. Das heißt, das müsste mit dem BER in Brandenburg besprochen werden. Was ich glaube, was Sie machen sollten: Wir sprechen hier über Cybersicherheit, aber, Sie haben es schon selbst gemerkt, viele Fragestellungen gehen in einen Ausschuss, wo der eine oder andere von Ihnen vielleicht auch Ausschussmitglied ist. Das ist der IT-Ausschuss. Dort sollte es noch mal aufgerufen werden. Mir untersteht das LKA, und Herr Steiof hat sehr ausführlich über die Polizei – ich habe es angedeutet, wir haben ein eigenes System – gesprochen, über das LKA. Wir sind gut aufgestellt. Das war mein allererster Satz, den ich vorhin gesagt habe. Wir haben die Koordinierung, und diese Koordinierung nehmen wir nicht nur sehr ernst, sondern wir beraten auch in den einzelnen Stellen. Ich habe das vorhin ausgeführt, das möchte ich nicht alles noch mal machen. Deshalb müssen diese Fragen den entsprechenden Behörden gestellt werden. Herr Schrader, das geht in die gleiche Richtung: Auch hier kann ich nur anraten, noch mal den IT-Ausschuss zu benennen.

Herr Weiß, Sie haben das LKA haben Sie gelobt. Danke schön! Das untersteht mir. Sie haben mich benannt, dass ich auf dem linken Auge blind bin. Das bin ich nicht. – [Thorsten Weiß (AfD): Das habe ich nicht gesagt!] – Na gut, dann habe ich Sie falsch verstanden. – [Reinhard Naumann (SPD): Es klang aber so!] – Es klang sehr danach. Schon als wir den Ausfall in Treptow-Köpenick hatten, habe ich mich sehr deutlich dazu positioniert. Im Übrigen gibt es seit 2017 eine behördenweite Gesamtstrategie der Politisch motivierten Kriminalität -links- beim LKA. Wir haben dieses Dezernat beauftragt. Das wird dort gemacht. Das heißt, wir behandeln alle Phänomenbereiche, nicht nur -rechts-, sondern alle. Sie unterstellen uns das immer gern. Das wird uns von allen Seiten unterstellt. Es ist aber nicht der Fall. Wir haben alle Phänomenbereiche. – [Kurt Wansner (CDU): Das machen die Linken auch!] – Deshalb sage ich ja, dass uns das von allen unterstellt wird.

Ansonsten würde ich jetzt sehr gern noch mal an die Senatskanzlei weitergeben zu den Fragen, die das ITDZ betreffen. Im Übrigen arbeiten wir als Verwaltung ebenfalls mit dem ITDZ zusammen. Herr Steiof hat das auch schon gesagt. Insofern wissen wir, dass es dort sehr gute Mitarbeiterinnen und Mitarbeiter gibt, die das dort entsprechend behandeln, und wir stehen im ständigen Austausch. Insofern würde ich jetzt Frau Gieseler, mit Ihrer Genehmigung, Herr Vorsitzender, noch mal bitten, das Wort zu ergreifen.

Vorsitzender Florian Dörstelmann: Vielen Dank, Frau Senatorin! – Genauso machen wir das auch. – Dann für die Senatskanzlei noch einmal Frau Gieseler, und dann kommen wir natürlich auch zur Antwortrunde für unsere Anzuhörenden. – Frau Gieseler, bitte, Sie haben das Wort!

Sonja Gieseler (Skzl): Ich würde jetzt auf Ihre Fragen eingehen, die, sage ich mal, sehr stark durchmischt sind. Bei der Informationssicherheit – ich rede nicht immer nur von der IT-Sicherheit, das ist mir zu klein gefasst, sondern wir reden hier von der Informationssicherheit – ist es so, dass wir im Land Berlin bei der Zusammenarbeit für die Leitlinie schon jetzt eigentlich jahrzehntelang ein sogenanntes Informationssicherheitsteam haben. Das sind alle Informationssicherheitsbeauftragten sowohl der Senatsverwaltungen als auch der Bezirke. Die treffen sich mindestens alle drei Monate mit einer entsprechenden Agenda, und da werden auch genau diese Sachen, was vorbereitet ist, zur Diskussion gegeben, auch wirklich beurteilt, sie können ihre Kommentierung geben. Es gibt dann immer wieder weitere Fassungen, und die Erkenntnisse, die wir aus diesem Gremium ziehen, melden wir dem IT-Planungsrat. Also da ist wirklich ein sehr reger Austausch, und dadurch, dass sowohl Herr Dr. Kroll-Peters als auch ich daran teilnehmen, können wir sogar in Person sicherstellen, dass diese Informationsaustausche stattfinden. Sie werden sowohl vom Bundesamt für Sicherheit als auch vom IT-Planungsrat sehr positiv wahrgenommen, sie sind bisher auf alle unsere Änderungsvorschläge oder Ergänzungsvorschläge – sei es zu technischen Richtlinien des Bundesamtes für Sicherheit –, komplett eingegangen und haben sie sogar zu 100 Prozent umgesetzt. Das finde ich sehr angenehm in der Zusammenarbeit, und das macht es uns natürlich dann, gerade wenn es um Schnittstellen für eine gemeinsame Nutzung geht, wie beim Netz des Bundes, sehr einfach. Da haben wir deutliche Verbesserungen auch in Richtung Cybersicherheit wahrgenommen.

Zur Cyberstrategie: Natürlich ist es immer eine Ist-Darstellung, aber es sind auch sogenannte KPIs angekündigt worden, auch übrigens im Sicherheitsbericht; den gibt es ja jedes Jahr, den Lagebericht zur Informationssicherheit. Da wird es jetzt auch verstärkte KPI-Varianten geben, um genau diese Forderungen, die ja auch aus dem Festsetzungsschreiben zu NIS2 kommen, umzusetzen. Wie soll ich denn sicherstellen, dass wirklich alle Maßnahmen zur Umsetzung im Land Berlin gewährleistet werden? – Das kann ich ja nur mit entsprechender Überprüfung.

Das hat das ITDZ genauso, die ungefähr 25 000 Arbeitsplätze des Landes Berlin verantworten. Ich bitte, auch das dabei zu berücksichtigen. Wir reden hier aber ungefähr über 100 000 Endgeräte, die zu betreuen sind, Tendenz stark steigend. Von daher wird auch die landesweite PKI im nächsten Jahr eingeführt, das Projekt wird gerade erfolgreich umgesetzt beziehungsweise gerade beendet. Ich kann Ihnen das bestätigen, weil ich da die Projektleiterin bin. Es ist so, dass diese Varianten natürlich auch gerade bei Zertifizierungsstellen sehr hilfreich werden. Sie werden also nicht mehr die Nachrichten bekommen, dass diese Zertifikat niemand kennt, das ist genau nämlich die Umsetzung auch, die Maschinenzertifikate können jetzt alle auch signiert zur Verfügung gestellt werden. Das ist wirklich ein sehr großer Schritt auch zur Automatisierung, was dann auch wieder zum Schutzniveau beiträgt, weil auch der Mensch ein Unsicherheitsfaktor ist, schon allein, wenn man irgendwie bei einer Infrastruktur mal vergisst, ein magisches Kreuz zu machen.

Weiterhin zur Unterstützung mit den Leitlinien ist es auch so, dass wir unseren Kollegen, den Informationssicherheitsmanagern jetzt auch entsprechende Standardkonzeptionen zur Verfü-

gung stellen. Wir haben Sicherheitskonzepte entwickelt, die dann als Vordrucke zur Verfügung stehen. Die entsprechen alle den notwendigen BSI-Standards. Das heißt, wir haben auch entsprechende einheitliche Regelwerke, die wir dann auch überführen können, und es ist auch so, dass diese Konzeptionen den Landesbevollmächtigten zur Verfügung gestellt werden. Das heißt, wir erlangen auch immer mehr Übersicht über Infrastrukturen, die jetzt nicht unbedingt zum Exchange-Verbund des Landes gehören und dergleichen mehr. Also die Erkenntniswerte sind sehr enorm. Wir haben natürlich ein stetiges Optimierungspotenzial, das ist einfach so, weil ja auch die Bedrohungslage, wie Sie schon zu Recht mitgeteilt haben, immer komplexer wird. Das macht auch die Herausforderungen bei den Sicherheitskonzeptionen natürlich immer mehr.

Wir haben auch die Qualifizierung sehr ins Auge gefasst, um genau diese Kollegen immer mehr in die Lage zu versetzen, entsprechende Rahmenverträge mit Spezialisten zu nutzen, um diese Sicherheitsniveaus beziehungsweise Fragestellungen besser beantworten zu können. Ich kann Ihnen aufgrund meiner langjährigen Erfahrung nur sagen: Sowohl im ITDZ, wo ich auch beratend tätig war, als auch in der Landesverwaltung generell, wird dieses Angebot sehr stark genutzt. Man kann also nicht sagen, dass jeder gerne in seiner kleinen Kammer sitzt, sondern genau diese Sachen laufen auch unter kollegialer Beratung, sodass man nicht immer denkt, man ist allein. Es ist sehr offenkundig, dass sich auch die Bedrohungslagen bemerkbar machen. Eine hundertprozentige Sicherheit können wir nicht gewährleisten, dann müssten Sie einen Stecker ziehen und wieder Brieftauben fliegen lassen, das möchte kein Mensch. Aber es ist so, dass die Herausforderungen immer mehr steigen, und da ist es natürlich auch wichtig, dass Notfallübungen landesweit durchgeführt werden; übrigens jährlich, und viele Verwaltungen nehmen daran teil. Die Zahl der Verwaltungen, die daran teilnehmen möchten, steigt stetig.

Wir haben dieses Jahr wieder eine Notfallübung sehr erfolgreich durchgeführt, wo zum Beispiel diesmal die Gerichtsbarkeiten teilgenommen haben, auch Vertreter der Polizei haben mitgemacht. Wir genießen sehr, dass das Interesse so groß ist, und der Mehrwert ist sowohl für uns als Verwaltung als auch umgekehrt für die Mitarbeiter im Land Berlin enorm. Allein schon für das nächste Jahr liegen uns 15 weitere Anmeldungen von Verwaltungen vor, die bei der nächsten Notfallübung, die wir ja immer gemeinsam konzipieren, teilnehmen wollen. Das ist ein enormer Schwung. Angefangen haben wir mal mit einer Verwaltung, und jetzt liegen wir, wie gesagt, nächstes Jahr schon bei 15; nur damit Sie das wissen. Es geht auch immer mehr um die kritische Infrastruktur bei diesen Notfallübungen, die sowohl im Großen, landesweit, aber auch in kleineren Sachen stattfinden. Es ist also nicht so, dass wir das nur einmal im Jahr haben, damit das erfüllt wird, sondern auch in kleinen Sachen finden immer wieder Austausche und Übungen statt. Ich kann nur aus meiner Erfahrung im ITDZ sagen, es finden sogar wirkliche Notfallübungen statt, in denen in Sandboxing-Systemen wirklich mal was kaputtgemacht und dann geguckt wird, ob alle Sachen wirklich funktionieren, die Server auch wirklich wieder wissen, dass sie Server sind.

Seien Sie mir nicht böse, ich kann nur allgemeine Informationen geben, denn wenn ich jetzt sehr ins Detail gehe, müsste ich jetzt eigentlich sagen, dass dürfte jetzt in der Öffentlichkeit nicht mehr gesagt werden, weil das dann so wie die Veröffentlichung im Intranet wäre. Das möchte ich nicht unbedingt. Also deswegen, seien Sie mir nicht böse, ich halte mich relativ allgemein, wenn das für Sie in Ordnung ist. Aber es hat eine unheimliche Entwicklung stattgefunden, und ich kann Ihnen nur sagen – ich bin allein in diesem Thema über acht Jahre un-

terwegs –, das ist schon wirklich von der Sensibilisierung oder auch vom Bewusstsein her, dass Beratung durch entsprechende Sicherheitsexperten schon am Anfang stattfinden sollte, und nicht erst, wenn das Kind schon in den Brunnen gefallen ist, ein vollkommene Wendung, die da stattgefunden hat.

Das ITDZ ist seit 2015 komplett BSI-zertifiziert, aber damals nur mit einem ganz übergreifenden Verfahren. Seit 2018 sind alle Basisdienste, die ja verbindlich nach dem E-Government-Gesetz genutzt werden, BSI-zertifiziert. Die BSI-Zertifizierung findet alle drei Jahre statt mit einer sogenannten Re-Zertifizierung, aber jedes Jahr findet ein Überwachungsaudit statt. Das heißt, da kommt ein unabhängiger BSI-Auditor, überprüft das alles, und die Überprüfung findet auch in den Systemen statt. Bitte stellen Sie sich nicht vor, diese Überprüfung finde nur on table statt, sondern der Auditor steht dann neben Ihnen, und wir müssen dann mal das Hochsicherheitsrechenzentrum aufschließen. Ich habe das jedes Jahr selbst erlebt, das ist wirklich eine komplette Überprüfung. Übrigens kommen auch Nachfragen während dieses Jahres, also Sie haben nicht nur an dem Tag oder in der Woche, wo der Auditor da ist, eine Überprüfung, sondern wir haben auch zum Beispiel mitten im Jahr entsprechende Prüfungen gehabt, wo Referenzdokumente übergeben wurden. – Ich glaube, Verschlüsselung findet alles statt, Ende zu Ende.

Mit dem Schutzniveau ist es so, durch die Leitlinie können wir jedes Jahr das Schutzniveau – – , und der Jahresbericht zeigt das Schutzniveau jedes Mal an. Ob das IT-Sicherheitsgesetz wirklich notwendig ist, dann müssten Sie sich bitte an die Gesetzgebung wenden! Bisher ist es so, dass wir diese Lücken durch entsprechende Ausführungsvorschriften jedes Jahr immer sehr gut schließen konnten.

Vorsitzender Michael Dietmann: Vielen Dank, Frau Gieseler! – Dann kommen wir jetzt zur Beantwortungsrunde unserer Anzuhörenden. Ich schlage die umgekehrte Reihenfolge des Aufrufes vorhin vor. – Herr Rütting, bitte, Sie haben das Wort!

Thomas Rütting (Stromnetz Berlin GmbH): Vielen Dank! – Ich würde gern die beiden Fragen von Herrn Dregger und von Herrn Schrader ein stückweit zusammenfassen, das ging ja in eine ähnliche Richtung.

Grundsätzlich muss man sagen, wenn man mal so zehn Jahre zurückschaut, hat man natürlich auch eine andere Situation. Sie, Herr Dregger, haben ja sehr gut dargelegt, welche Daten man überall im Internet findet und so weiter. Wir kommen ehrlicherweise auch aus einer ganz anderen Zeit, wo Openness, Partizipation extrem angesagt war, und aus dieser Zeit sind die Daten zum Teil noch; nicht ausschließlich, aber zum großen Teil. Ich will auch sagen, dass wir natürlich mittlerweile schon versucht haben, das Ganze wieder rückgängig zu machen – ich sehe schon, da wird gelächelt –, das scheitert aber an den gesetzlichen Möglichkeiten. Die Frage war ja, würden wir uns wünschen, dass diese Daten nicht mehr transparent sind im Sinne von Open Data auf der einen Seite, aber nicht für die kritische Infrastruktur? – Ein ganz klares Ja, das würden wir uns schon wünschen, und das wünschen wir uns sehr stark. Es gab diverse Aktivitäten, bisher leider ohne Erfolg.

Zum Thema Cyberattacken: Wir haben ja eine Trennung zwischen Office-IT und unserer OT, also der eigentlichen, womit wir unsere Betriebsmittel steuern und führen und da unterwegs sind. Wir hatten bisher zum Glück keine Ausfälle, weder in der Office-IT, aber schon gar

nicht in der OT, und das ist auch gut so. Allerdings bereiten wir uns – das war ja vorhin auch meinen Ausführungen zu entnehmen – schon intensiv darauf vor, wenn denn der Fall eintritt, damit wir darauf gut vorbereitet sind, Stichwort BCM, das treibt uns schon sehr stark um. – Das vielleicht zur Abrundung dieser beiden Fragen zu Open Data und Cyberattacken.

Jürgen Schunk (Stromnetz Berlin GmbH): Gut, dann würde ich an der Stelle weitermachen und da noch mal mit einem konkreten Beispiel anfangen. Das Telekommunikationsgesetz, das Ihnen sicherlich auch bekannt ist, sieht vor, dass wir Infrastrukturen dort offenlegen. Hintergrund ist, dass der Wettbewerb im Telekommunikationsbereich erhöht wird. Wir sind gesetzlich gezwungen, unsere freien Leerrohre oder auch Lichtwellenleiter, die wir besitzen, dort zu veröffentlichen. Wenn wir dort noch Unterstützung haben könnten, wäre das zum Beispiel auch noch ein Thema, wo wir sagen, dort letztendlich auch da im Gesetzgebungsveränderungsprozess uns zu unterstützen, damit diese Infrastrukturen dort nicht mehr bekanntgegeben werden müssen; das ganz konkret zu dem Thema, das Herr Rütting gerade auch nannte mit Cybersicherheit.

Herr Matz, Sie haben zwei sehr gute Fragen gestellt, vielleicht knüpfe ich da erst mal an. Aufgrund der Energiewende haben wir enorme Investitionen vor der Brust, wir verdoppeln die Netzkapazität in den nächsten zehn Jahren, investieren 5 Milliarden Euro, das sind 500 Millionen Euro im Jahr, und das ist natürlich auch eine Chance, weil wir nämlich jetzt nicht nur unser Netz erweitern, sondern können dabei auch Resilienzerhöhung im Netz mitdenken und es natürlich auch nutzen. Ein Beispiel ist der Rückbau der Freileitungen, den wir da ja auch vor der Brust haben; da werden wir natürlich auch – gerade im Nordosten von Berlin, wo wir im Wesentlichen noch diese Freileitungen haben – unser Netz umstrukturieren und mit der Investition, die wir jetzt für die Erweiterung durchführen, auch resilienter in unserem Netz werden.

Das Gleiche gilt in der Region Köpenick, da sind wir natürlich auch dabei, unser Hochspannungsnetz zu erweitern. Die Frage war: Gibt es kurzfristige Dinge? – Ja. Ich gehe jetzt erst mal auf das Hochspannungsnetz ein. Wir erweitern unser Hochspannungsnetz und werden mit den Maßnahmen, die wir dort jetzt schon seit Jahren durchführen, gerade in Köpenick nächstes Jahr fertig sein. Wenn der Anschlag danach erfolgt wäre, hätte er die Auswirkungen gar nicht gehabt. Daran sehen Sie, dass wir kontinuierlich daran arbeiten, die Resilienz in unserem Netz zu erhöhen, und natürlich hat das mit den Hochspannungsleitungen zu tun.

Sie haben darauf hingewiesen, dass wir bei der Störung in Johannisthal eine Teilversorgung durchführen konnten. Das ist richtig. Natürlich machen wir Havariekonzepte, die haben wir vorher schon gehabt, die erweitern wir aber auch immer wieder und gucken natürlich, wie wir über die Mittelspannungsebene in einem solchen Fall eine Versorgung sicherstellen können. Aber wir müssten nicht zwischen Hochspannung und Mittelspannung trennen, wenn die Leistungsübertragungen dieser Netze gleich wären. Das heißt, über ein Mittelspannungsnetz kann man immer nur eine geringere Leistung übertragen und damit auch nur eine Teilversorgung sicherstellen. Das denken wir aber mit, und wir haben natürlich, um kurzfristig zumindest einen Teil der Bevölkerung in einem solchen Fall abzusichern, dann auch diese Maßnahmen natürlich in petto.

Grundsätzlich noch mal zur Cybersicherheit, da will ich noch über die Infrastruktur kurz berichten: Wir haben ein eigenes Daten- und Telekommunikationsnetz, wir haben eigene Kup-

ferdoppeladern, wir haben eigene LBL-Leitungen, wir sind da nicht auf dritte, private Anbieter angewiesen. Wir betreiben dieses Netz komplett autark. Unsere IT, gerade im OT-Bereich, ist komplett nach außen abgesichert. Wir testen das auch; wir machen Krisenstabsübungen, wo wir wirklich komplett die Wand nach außen fallenlassen, und unsere IT-Systeme sind dann immer noch im Betrieb. Wir erreichen dann auch noch unsere Umspannwerke, um letztendlich auch da steuernd tätig zu werden. Wenn das trotzdem ausfallen sollte, gibt es immer noch Reserveinformationssysteme, die auf einer anderen Infrastruktur beruhen, mit denen wir dann auch noch unsere Infrastruktur erreichen, und wenn das alles scheitern sollte, was sehr unwahrscheinlich ist, haben wir immer noch die Möglichkeit, Umspannwerke auch wieder personell zu besetzen, wie es vor 50 Jahren war, und auch das würde dann funktionieren.

Vorsitzender Florian Dörstelmann: Vielen Dank! – Herr Holst, bitte, Sie haben das Wort!

Henrik Holst (IHK Berlin): Vielen Dank und danke für die Fragen! – Ich glaube, es gab eine Frage zu den Beteiligungsmöglichkeiten bei der Strategie oder allgemein beim Thema Cybersicherheit, und darauf würde ich gern noch einmal eingehen. Grundsätzlich kann ich, wenn es um Digitalstrategie geht, egal ob das jetzt das Thema Open Source ist oder eine Cybersicherheitsstrategie, nur wärmstens empfehlen, Wirtschaft und Wissenschaft wirklich ehrlich einzubinden. Das hat den Vorteil, dass Unternehmen, die vielleicht in anderen Bundesländern schon an verschiedenen Projekten beteiligt sind oder Erfahrungswerte gesammelt haben, ihr Wissen dann wirklich reingeben können. Das ist beim Thema Open Source besonders stark, da gibt es einfach andere Bundesländer, die schon weiter sind, und auch Berliner Unternehmen, die an verschiedenen Projekten beteiligt sind. Das ist auch beim Thema Cybersicherheit und KRITIS so.

Die aktuelle Cybersicherheitsstrategie wurde jetzt gerade schon einmal als Feigenblatt verschrien und einmal gesagt, das müssten wir machen, weil wenn es zwei machen – – Es gab in der vorherigen Koalition sogar einen Passus im Koalitionsvertrag, wo drinstand: Wir wollen eine umfassende IT-Sicherheitsstrategie machen. – Mein Problem mit der Strategie ist, wenn man sich nur damit befasst, den Status quo zu beschreiben, dann suggeriert das, dass wir schon relativ nah an den Idealstatus rankommen. Das ist ja nicht so. Wir müssen beschreiben, wo wir hinwollen, und wir müssen auch beschreiben, was wir dafür tun müssen, und das geht in dieser Strategie etwas abhanden.

Ein zweites Thema, und da würde ich gern das aufgreifen, was Senatorin Spranger gesagt hat: Es gibt viele Überschneidungen zum DiDat-Ausschuss und der Diskussion, die dort geführt wird. Es gibt ja aktuell auch die Diskussion, dass die Koalition ein Digitalgesetz plant, um mal zu überlegen, wie wir denn die Steuerung über das E-Government-Gesetz hinaus noch verbessern können. Einige Sachen, wie beispielweise: Wie kriegen wir wirklich eine einheitliche IT hin? Wie kriegen wir das Thema Vergabe so aufgestellt, dass wir auch das Thema IT-Sicherheit vielleicht bei Vergabeprozessen langfristig mitdenken, das Thema digitale Souveränität bei Vergabe langfristig mitdenken? – sind alles Themen, da gibt es einfach im Digitalbereich wahnsinnig viele Schnittmengen zwischen IT-Sicherheit und Digitalpolitik im Allgemeinen. Deshalb würde ich einfach appellieren, dass solche Aspekte in beiden Ausschüssen gleichermaßen diskutiert werden, nicht hin- und hergeschoben werden und aufeinander gezeigt wird, wer am Ende zuständig ist, sondern es betrifft beide Ausschüsse gleichermaßen, und die beiden Ausschüsse, sowohl die Abgeordneten, die in den Ausschüssen sitzen, als auch dann die Verwaltung, müssen sich entsprechend absprechen. – Vielen Dank!

Vorsitzender Florian Dörstelmann: Vielen Dank, Herr Holst! – Herr Dr. Herpig, bitte, Sie haben das Wort!

Dr. Sven Herpig (interface): Vielen Dank! – Ich würde mit einer kurzen Antwort auf die Frage der CDU zurückkommen zum Thema Veröffentlichung von Daten zu kritischen Infrastrukturen. Natürlich kann man das angehen, aber ganz ehrlich, das folgt so ein bisschen dem Konzept Security through Obscurity: Wir tun so, als ob wir die Daten runternehmen können und nicht darüber reden dürfen, und dann passiert schon nichts. – Die Infrastrukturen müssen abgesichert werden. Mir ist auch bewusst, dass viele von denen in der Öffentlichkeit zugänglich sind, die kann man eben nur bis zu einem bestimmten Punkt absichern, und dann muss man Redundanzen bauen, damit, wenn sie mutwillig kaputtgemacht werden, man dann eben auch Auswahlmöglichkeiten hat und so weiter. Im Endeffekt ist es so: Wogegen wollen Sie sich verteidigen? Gegen Einzeltäterinnen, die so etwas ab und zu mal kaputtmachen, oder reden wir hier von gut organisierten Gruppen, die zum Beispiel von ausländischen Staaten unterstützt werden? Die werden immer an diese Informationen herankommen, und damit ist es halt etwas, wo wir natürlich Ressourcen investieren könnten, aber ich glaube ganz ehrlich, das macht nicht viel Sinn. Im Sinne der Sicherheit und der Herstellung von Resilienz haben wir andere Maßnahmen, die wir ergreifen sollten.

Zur Frage aus der Fraktion Die Linke, Quellen-TKÜ und Onlinedurchsuchung: Man kann natürlich darüber reden, aber es ist kein Wundermittel. Ich zitiere hier mal das Bundesamt für Justiz:

> „Maßnahmen der Online-Durchsuchung gemäß § 100b StPO bleiben seltene Ausnahmen. Bundesweit wurden sie 2023 in acht Verfahren angeordnet und in sechs Verfahren auch durchgeführt.“

Die Frage ist, wie viele Ressourcen man dafür verwenden muss, wenn es in der bundesweiten Anwendung eigentlich überhaupt keine Rolle spielt. Die Beschaffung entsprechender Maßnahmen ist nicht günstig. Man macht sich abhängig von Herstellern, die erstens in Ländern beheimatet sind, mit denen wir vielleicht nicht zusammenarbeiten wollen, und die zweitens vor allem ihre Produkte und Dienstleistungen auch an Regime verkaufen, die Menschenrechte missachten. Ob wir das mit deutschen Steuergeldern finanzieren wollen, würde ich jetzt Ihnen überlassen.

Als letzten Antwortblock auf die Frage der Frau Abgeordneten Ahmadi: Was sollen wir denn jetzt tun? – Ich habe hier viereinhalb Punkte. Zuallererst, weil in den Antworten auf die kleinen Anfragen und jetzt auch wieder kam: Na ja, nein, das macht dann schon das BSI, und da sprechen wir mit jemandem vom BSI –: Als ehemaliger Mitarbeiter des BSI würde ich an dieser Stelle dringend anraten, Ihre Abhängigkeiten vom BSI zu prüfen. Denn wenn ich jetzt gemein wäre, würde ich sagen: Wenn Sie es nicht mal schaffen, eine Kooperationsvereinbarung mit dem BSI zu schließen, wie sehr können Sie sich dann auf die operative Kooperation des BSI im Vorfall verlassen? Aber ich bin ja nicht gemein, deswegen sage ich das nicht. Ich würde Ihnen aber zum Beispiel die Frage zurückgeben: Was glauben Sie denn, wie viele Nerds, wie viele mobile Vorfallsbearbeitungsteams das BSI gleichzeitig stellen kann? Wir haben 16 Bundesländer, wir haben Tausende kritische Infrastrukturen; die Mathematik würde ich jetzt Ihnen überlassen. Ich würde anraten, sich anzuschauen, was für skalierende technische IT-Sicherheitsmaßnahmen das BSI unterstützen kann, zum Beispiel das Schadsoft-

warekennungssystem oder das Schadsoftwarepräventionssystem, und sich da anzuschauen, wo man sich beim BSI sinnvoll technisch andocken kann, weil ich glaube, davon haben wir mehr, als auf solche Einzelpunkte zu setzen.

Der zweite Punkt ist: Niemand hier weiß wirklich, was operativ in der Cybersicherheit in diesem Bundesland vor sich geht. Sie haben kein operatives Lagebild. Das ist kein riesiges Problem, das haben die anderen Bundesländer auch nicht und der Bund sowieso nicht, aber vielleicht sollten Sie hier anfangen. Sie könnten es auch als Teilpuzzlestück bauen für ein gesamtes nationales Cyberlagebild, damit Sie operativ wissen, was bei Ihnen los ist. Auch da wieder der Verweis auf NIS2 und so weiter: Das sind kritische Infrastrukturen gemäß einer rechtlichen Definition von kritischen Infrastrukturen, aber nur, weil es ein kleines Krankenhaus ist, heißt das nicht, dass, wenn dort etwas ausfällt, da Leute nicht sterben.

Dritter Punkt: Fachkräftemodelle. Wir haben es gerade angesprochen, wir haben nicht genug Fachkräfte in diesem Bundesland; aber auch da kein Problem, denn das haben wir deutschlandweit und auch weltweit nicht. Aber Sie können etwas dagegen tun. Wir brauchen keine dreijährigen Ausbildungsberufe, wo am Ende jemand rauskommt, der mal 20 Stunden etwas zur IT-Sicherheit gemacht hat. Wir brauchen jemanden, der in sechs oder neun Monaten befähigt werden kann, Load Balancer einzustellen und Firewalls zu konfigurieren. Wir brauchen keine neue Professuren für Kryptografie, Blockchains und KI, wir brauchen die Leute, die das Doing machen, und die müssen dann entsprechend bezahlt werden, damit sie motiviert weiterhin beim ITDZ nett sind und gute Arbeit leisten können.

Der vierte Punkt, und das können Sie sehr schwer kontrollieren: Wir brauchen eine ehrliche operative Bestandsaufnahme in der Senatsverwaltung und -kanzlei bei Themen wie Assetmanagement, Schwachstellenmanagement: In welchen Softwarepaketen sind wir wie viele Patchstufen hinterher?, Ist das okay, ist das nicht okay?, Back-ups wirklich richtig prüfen. Ja, klar, wir haben alle drei Jahre eine Zertifizierung, jährlich ein Audit, aber es muss ja tagtäglich funktionieren. Das kann man nicht wirklich überprüfen, das muss intern alles funktionieren, und da muss man eben auf die Ehrlichkeit derjenigen setzen, die dort arbeiten, dass dieses auch vernünftig technisch dauerhaft jeden Tag umgesetzt wird und nicht nur auf dem Papier vorhanden ist. Ein Beispiel: Back-ups bei Colonial Pipeline in den USA, die hatten Back-up-Möglichkeiten, aber deren Leitungen und so weiter waren so langsam, dass die Wiederherstellung so viele Tage gedauert hätte, dass der Schaden die Firma ruiniert hätte. Da bringen auch keine funktionierenden Back-up-Fähigkeiten was, deswegen müssen sie eben real geprüft werden.

Letzter Punkt: Falls all diese Punkte nicht umgesetzt werden, dann sollte man vielleicht schauen, ob man das aus dem Jahr 2016 stammende E-Government-Gesetz noch mal anfasst und hier vielleicht verändert oder ein IT-Sicherheitsgesetz für Berlin verabschiedet. Ein Beispiel hier ist: Wenn wir kein operatives Lagebild hinbekommen, könnte man mit Meldepflichten arbeiten, die über die NIS2-Umsetzung hinausgehen und eben auch an das Land Berlin gemeldet werden, damit man im Land Berlin eine Ahnung hat, wie hier in der Cybersicherheit die Lage ist. – Vielen Dank!

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

Manuel Atug (AG KRITIS) [zugeschaltet]: Vielen lieben Dank! – Zur Frage, wie eine Beteiligung bei Herrn Kroll-Peters aussehen kann und ob das hilft: Erst mal zur Einleitung, wir finden es sehr toll, wie Stromnetz Berlin, die ISBs für Berlin und deren Teams und alle operativ umsetzenden Einheiten generell in Berlin wie auch beim ITDZ in so einer Lage handeln und die Versorgung weiterhin bestmöglich aufrechterhalten. Unsere Kritik richtet sich ja eher an die Verantwortungsdiffusion bei Entscheiderinnen und Entscheidern. Wir haben das Beispiel gehört, es gibt eine Koordinierungsstelle KRITIS, es gibt Fachaustausch, Wissensspeicher, Gespräche; alles richtig, aber insofern im Wesentlichen leider nichts Verbindliches zur Umsetzung von Maßnahmen. Durch Betroffenenstuhlkreise und vermeintliche Teillagebilder wird eben keine Resilienzmaßnahme umgesetzt, das hat ja Herr Dr. Herpig gerade auch ganz gut ausgeführt.

Insofern bieten wir als AG KRITIS immer gern unsere Beteiligung und Hilfe an, soweit wie wir es machen können. Wir können natürlich nicht die Wirtschaft und die Beratung da irgendwie ersetzen, und das wollen wir auch nicht. Wie gesagt, wir sind komplett unabhängig und machen das in der Freizeit. Aber wir beteiligen uns sehr gern. – Frau Gieseler, nehmen Sie das gern mit, nehmen Sie Kontakt zu uns oder direkt zu mir auf, und dann gucken wir, wieweit wir das können. Wir machen Stellungnahmen, wir machen Analysen, wir geben Hinweise, Tipps und Tricks; wenn es hilft, immer gern, soweit wir das schaffen, und dann kann man davon natürlich auch profitieren.

Dann gab es noch die Frage, wie andere Bundesländer tolle KRITIS-Verordnungen umgesetzt haben und wie eine gute aussähe. Das war vielleicht ein Missverständnis. Tatsächlich hat bisher kein Bundesland eine KRITIS-Verordnung erlassen. Unser Vorschlag war ja, dass man sich mal zusammensetzen müsste. Tatsächlich zeigen alle immer auf die anderen und sagen: Na, haben die eine? –, und dann heißt es: Nein, haben die auch nicht, wir befinden uns also in bester Gesellschaft, wir haben auch keine. – Wie eine gute KRITIS-Verordnung aussehen könnte: Man müsste tatsächlich eine gemeinsame sogenannte Musterverordnung besprechen und abstimmen, sodass alle 16 Bundesländer diese einheitlich so umsetzen. Dann hätten wir quasi die KRITIS-Verordnung auf Bundesebene und quasi das Gleiche auf den Landesebenen. Denn die Akteure im Netz, ob das Spionage, ob das staatliche Akteure wie Geheimdienste oder eben die Onlinekriminellen und alle anderen sind, von mir aus auch Sechzehnjährige aus Mittelhessen in Deutschland – haben wir ja auch öfter erlebt – fragen nicht nach einer gemeinsamen Verordnung oder machen an einer Verantwortungsgrenze halt, sondern sie wollen Systeme zerstören oder Daten abziehen. Insofern sähe es gut aus, wenn man sich zusammensetzt, auch da würden wir gern die Hilfe bereitstellen, dass man sagt, Staat und Verwaltung und Medien und Kultur reguliert man innerhalb der Bundesländer, und zwar einheitlich, damit man da auch ein gleiches Schutzmaß, Schutzniveau und Schutzverständnis hat. Das würde sicherlich guttun.

Zur Anmerkung zu flosm.org oder weiteren veröffentlichten Details zu Stromnetzen, Open Data versus KRITIS und dergleichen, da können wir nur sagen: Wir widersprechen, dass man aus Gründen der Sicherheit solche Veröffentlichungen grundsätzlich unterbieten sollte. Akteure, die gezielt Sabotage durchführen oder Ausfälle bewirken wollen, kommen insbesondere auch aus der Querdenkerszene, wie wir in der Pandemie und danach erlebt haben, als aufgrund der 5G-Chips, die uns mit den Impfungen eingespritzt werden, Mobilfunkmasten attackiert wurden. Das waren tatsächlich nicht oft Linksradikale, sondern eher Querdenker und auch von der rechten Szene beförderte Menschen, die diese Mobilfunkmasten angegriffen

haben; ironischerweise waren fast alle angegriffenen Mobilfunkmasten 4G-fähig, nicht 5G-fähig, also hätten sie gar nicht diese 5G-Chips steuern können. Auch diesen Schwachsinn aus diesen Szenen müssen wir natürlich als offene Gesellschaft ertragen können. Aber auch Security by Obscurity funktioniert nicht. Insofern sollte man immer zweimal abwägen, ob man Dinge heimlich hält. Es ist so, dass die Gutes bewirken können, nämlich transparent zu machen, wie Schutzmaßnahmen aussehen, wo wie Redundanzen sind, dass man das mal für sich recherchiert. Auch KRITIS-Betreiber, auch kleine Krankenhäuser, wie Herr Dr. Herpig gerade gesagt hat, können das dann in Anspruch nehmen, ohne groß Tamtam zu machen. Das würde tatsächlich helfen.

Schönes Gegenbeispiel ist, dass die Notbrunnen und die Notwasserversorgung in Deutschland geheim gehalten wird. Man kann in seiner eigenen Kommune nachfragen. Wenn man vehement genug ist, bekommt man die Antwort und die gesamte Liste; wenn man das als Akteur macht, hat man die genauso, das ist also Augenwischerei. Der Nachteil ist aber, wir haben nicht alle Notbrunnen in freien Systemen wie OpenStreetMaps klassifiziert.

Wir können also nicht einfach daraus Schutzmaßnahmen für die Bevölkerung ableiten, freie Software bauen, die diese Dinge abfragt, maschinenlesbar in öffentlichen Schnittstellen nutzt und für eine Verbesserung der Versorgungslage der Bevölkerung sorgt. Stattdessen haben wir das Problem, dass ungefähr die Hälfte der Notbrunnen defekt sind, weil sie nicht gewartet werden, weil die Kommunen kein Geld haben und der Bund auch unzureichend bereitstellt, und das passiert dann eben unter dem Deckmantel der Geheimhaltung, sodass nicht auffällt, dass wir da eine sehr desolate Lage haben. Ich würde also tunlichst von abraten, leichtfertig zu sagen: Wir halten diese Informationen geheim. – Das ist nicht der richtige Schritt.

In Ergänzung zu Dr. Herpig zuletzt noch: Dass die Polizei Staatstrojaner und Quellen-TKÜ erhalten soll, verwundert mich sehr. Es ist das Gegenteil von Cyberresilienz, Schwachstellen offen zu halten und ausnutzen zu wollen. Das ist ungefähr genauso eine schlechte Lösung für unsere Cybersicherheit wie Palantir einsetzen zu wollen.

Was wir brauchen, ist wirkliche Maßnahmenumsetzung. Da finde ich schön, dass Frau Gieseler mal sehr ausführlich dargelegt hat, was alles im Rahmen dessen getan wird, was genehmigt und zugelassen wird. Das ist wirklich super. Das beruhigt auch ein wenig. Es ist nicht so, dass es entspannt, wir haben viel zu tun, es sind noch viele Baustellen offen, aber es ist toll, dass viele angegangen wurden. Insofern ist das auch der Grund, warum wir als AG KRITIS erstens existieren und zweitens immer noch Hoffnung haben, denn Dinge können sich verbessern und können in eine andere Richtung gehen, auch wenn die Richtung derzeit oftmals gruselig aussieht. Das hatte ich ja auch schon vor zwei Jahren gesagt: Kurz und knapp gilt die Sicherheit in Berlin als gruselig und desolat wie in allen anderen Bundesländern und auch auf der Bundesebene. Wir sollten nicht mehr von Befugnissen, Palantir, KI, Gesichtserkennung, Quellen-TKÜ reden, stattdessen Cyberresilienz und Basissicherheitsmaßnahmen wirklich vorantreiben, und insofern kommen wir immer wieder auf diese Punkte, weil das die wirkliche Abwehr von Angriffen ist. Dann verpuffen die Angriffe und ihre Auswirkungen im Idealfall wirkungslos oder fabrizieren nur kleinere Störungen. Das ist genau das, was wir für Berlin, aber auch für die Bundesrepublik erreichen müssen. – Danke!

Vorsitzender Florian Dörstelmann: Vielen Dank, Herr Atug! – Dann habe ich jetzt eine Wortmeldung von Herrn Abgeordneten Mirzaie. – Sie haben das Wort!

Ario Ebrahimpour Mirzaie (GRÜNE): Vielen herzlichen Dank! – Ich finde die Debatte wirklich sehr spannend und sehr interessant. Sie knüpft ja auch in vielen Punkten an Diskussionen an, die wir schon vor einigen Wochen in den Anhörungen rund um ASOG, Quellen-TKÜ und so weiter hatten. Dazu komme ich aber gleich noch mal.

Zunächst einmal will ich noch an die Adresse der AfD richten, dass es schon etwas lächerlich ist, hier Antifaschismus kriminalisieren zu wollen und in Zusammenhang mit irgendwelchen Anschlägen zu stellen. Ich weiß nicht, wen Sie da vor Augen haben, ob die Omas gegen Rechts da jetzt in Ihren Augen hier irgendwie gegen die kritische Infrastruktur vorgehen. Das ist einfach lächerlich, und das möchte ich hier auch zurückweisen. Aber das ist ja gerade Teil Ihrer Strategie, dass Sie versuchen, nach der Hochstufung als rechtsextremistisch hier Strohfrauen, Strohmänner aufzubauen. Das geht ja völlig am Thema vorbei. Aber ich kann Ihnen sagen: Wissen Sie, wer mich beunruhigt? – Das sind die Mitglieder Ihrer Partei, die in sicherheitsrelevanten Berufen, eventuell auch in der Verwaltung Berlins, sitzen. Das ist die wahre Gefahr für unseren Staatsdienst, für die öffentliche Ordnung, und deswegen werden wir als

Grüne auch weiterhin daran arbeiten, dass eine systematische Überprüfung einer AfD-Mitgliedschaft für Beschäftigte im öffentlichen Dienst stattfindet, damit eben die Mitglieder Ihrer Partei nicht in kritischen Positionen sitzen und da für Putin oder andere Leute spionieren oder gar noch schlimmere Sachen machen. Das ist der Fokus, auf den wir uns konzentrieren werden, und nicht auf irgendwelche Nebelkerzen, die Sie uns hier, inspiriert durch Ihre Freunde von MAGA, Trump und Co, irgendwie in die Debatte einwerfen wollen.

Dann wollte ich noch mal auf den Punkt der Transparenz eingehen. Ich glaube, um da dem einen Experten zu widersprechen, nicht, dass wir jetzt aus einem Zeitalter rauskommen, in dem irgendwie Transparenz mal en vogue war, und sie jetzt nicht mehr en vogue ist. Vielleicht habe ich Sie da auch falsch verstanden. Aber ich würde davor warnen, hier so ein Bild zu zeichnen. Es gibt da doch dieses schöne Zitat: Es gibt nichts Schlimmeres, als aus Angst vor der Unfreiheit Freiheit selbst schon einzuschränken. – Ich finde, an der Stelle, wo es um Transparenz geht, kann das ja nicht bedeuten – und da bin ich vollkommen bei Herrn Atug und anderen, der das auch schon nach dem Anschlag in Treptow-Köpenick in der Presse gesagt hat –, dass es darum geht, hier irgendwie die Transparenz oder die Ausweisung bestimmter Stromtrassen und so zurückzufahren, sondern es geht darum, die Angriffe zu verhindern und zu wissen, was Resilienz in dem Zusammenhang bedeutet. Sorry, aber ich kann mir das auch praktisch gar nicht vorstellen. Will man dann Flecktarn über die Strommasten werfen oder hier Stromkästen im Stadtbild anmalen? Da fehlt mir auch so ein bisschen die praktische Umsetzung dessen, was man da jetzt irgendwie verschleiern möchte. Ich bin auch weiterhin ein großer Verfechter und Freund von Open Data, von Transparenz, und ich glaube, an der Stelle geht es nicht um irgendwelche Karten oder Google-Maps-Hinweise, sondern wirklich darum, gemeinsam zu gucken, wie wir die so wichtige kritische Infrastruktur hier in Berlin auch gemeinsam widerstandsfähiger und resilienter machen können.

Letzter Punkt: Was ich so ein bisschen auch für die Debatte wichtig fand, ist tatsächlich noch mal der Hinweis: Die technischen Anbieter auch diejenigen, die uns bestimmte Softwarelösungen anbieten – das hat Herr Dr. Herpig völlig zu Recht gesagt, und das hatten wir auch in der Anhörung zum ASOG mehrmals unterstrichen, da hatte ja der Senat gesagt: Wir machen jetzt erst mal die gesetzlichen Grundlagen und entscheiden dann, welche Software und welchen Anbieter wir dann heranziehen –, da will ich hier noch mal unterstreichen, dass das eine zentrale Frage ist und eben viele dieser Anbieter entweder in Ländern sind, die wir kritisch sehen, oder wirklich auch mit Regimen zusammenarbeiten, mit denen wir nichts zu tun haben wollen. – Vielen herzlichen Dank!

Vorsitzender Florian Dörstelmann: Vielen Dank, Herr Abgeordneter Mirzaie! – Weitere Wortmeldungen sehe ich jetzt nicht. Ist von Senatsseite noch etwas anzufügen? – Das ist nicht der Fall. – Vielen Dank! – Dann sind wir am Ende unserer Anhörung angelangt.

Ich danke Ihnen, den Anzuhörenden, ganz herzlich dafür, dass Sie sich heute die Zeit genommen haben, uns hier mit Ihrer Expertise zur Verfügung zu stehen! Danke Ihnen für die präzisen Antworten und natürlich auch alle übrigen Ergänzungen, die Sie uns hier gegeben haben, und den Überblick, den wir dadurch gewinnen konnten. Vielen Dank! Das wird sich vielleicht an anderer Stelle noch einmal ergeben. Wir freuen uns darauf und wünschen Ihnen eine erfolgreiche Woche!

Wir sind damit am Ende des Tagesordnungspunktes 2 angekommen. Ich frage die Fraktion Bündnis 90/Die Grünen, ob der Tagesordnungspunkt 2 a damit als abgeschlossen vermerkt werden darf. In der Praxis wird es keinen Unterschied machen, weil wir das andere natürlich noch mal aufrollen, sobald wir das Wortprotokoll vorliegen haben. – Gut, dann wird Punkt 2 a abgeschlossen und Punkt 2 b vertagt.

Punkt 3 der Tagesordnung

a)	Besprechung gemäß § 21 Abs. 3 GO Abghs **Korruptionsverdacht wegen gekaufter Personenschützer:** **Eigenleben beim LKA 6** (auf Antrag der Fraktion Die Linke)	0244 InnSichO
b)	Besprechung gemäß § 21 Abs. 3 GO Abghs **Mögliche private Schutzaufträge von LKA-Beamten für den Rapper Bushido – Aufklärung der Vorgänge, dienstrechtliche Konsequenzen und Maßnahmen zur Widerherstellung des Vertrauens in die Polizei Berlin.** (auf Antrag der AfD-Fraktion)	0245 InnSichO

Vertagt.

Punkt 4 der Tagesordnung

Verschiedenes

Siehe Beschlussprotokoll.

* * * * * *