Abgeordnetenhaus BERLIN

19. Wahlperiode

Plenar- und Ausschussdienst

Wortprotokoll

Öffentliche Sitzung

Ausschuss für Digitalisierung und Datenschutz

77. Sitzung
7. September 2026

Beginn: 14.06 Uhr
Schluss: 17.28 Uhr
Vorsitz: Johannes Kraft (CDU)

Vor Eintritt in die Tagesordnung

Siehe Beschlussprotokoll.

Punkt 1 der Tagesordnung

Aktuelle Viertelstunde

Siehe Inhaltsprotokoll.

Punkt 2 der Tagesordnung

Bericht aus der Senatskanzlei

Siehe Inhaltsprotokoll.

Redaktion: Swenja Schum, Tel. 2325-1463 bzw. quer 99407-1463

Vorsitzender Johannes Kraft: Wir kommen zu

Punkt 3 der Tagesordnung

a) Besprechung gemäß § 21 Abs. 3 GO Abghs — 0170 DiDat
IT-Sicherheitsvorfall im Landesnetz: Was ist bekannt und wie können wir uns endlich besser schützen?
(auf Antrag der Fraktion Bündnis 90/Die Grünen)

b) Besprechung gemäß § 21 Abs. 3 GO Abghs — 0171 DiDat
Cyberangriff auf das Berliner Landesnetz: Bilanz und Folgen für die IT-Sicherheitsarchitektur
(auf Antrag der Fraktion der CDU und der Fraktion der SPD)

Besteht der Wunsch, die Besprechungspunkte zu begründen? – Das ist der Fall. Herr Ziller, dann wären Sie als Erster dran. – Bitte schön!

Stefan Ziller (GRÜNE): Ich glaube, es ist schon noch mal begründungswürdig, was wir hier besprechen wollen. Ich glaube, uns eint das gemeinsame Ziel, möglichst Klarheit zu schaffen. Jetzt gab es am Wochenende wieder Pressemitteilungen und Veröffentlichungen, die in meinen Augen mehr Fragen aufgeworfen haben, als sie vielleicht beantwortet haben. Wir hatten nun eine Zeitlang das Gefühl, dass der Senat die Krise und auch die Informationslage ein bisschen im Griff hat, aber im Moment scheint es dann doch wieder auszufleddern.

Insofern sollten wir heute über verschiedene Komplexe reden. Wir sollten zum einen über den Opferschutz reden: Was ist jetzt wirklich passiert? Wie viele Personen sind identifiziert? Wie viele sind gewarnt? – Das ist mir alles zu vage. Bisher haben wir vor allem von den Kriminellen Informationen über die Anzahl der Betroffenen, über die Anzahl der Daten. Wir brauchen eigene Informationen. Wenn der Senat sie nicht hat, brauchen wir dringend die Klärung, wie der Stand ist. Wir müssen über akute IT-Sicherheitsprobleme reden. Nach dem, was man liest, bin ich der Überzeugung, dass in der Berliner Verwaltung sicherlich nicht nur eine Datei passwort.docx heißen wird. Auch darüber, was der Senat akut tut, damit solche Dateien verschwinden und andere Lösungen gefunden werden, müssen wir reden.

Wir haben im letzten Hauptausschuss mal nachgefragt, ob der Senat substanziell etwas ändern will. Die Finanzverwaltung hat sehr zurückhaltend agiert und gesagt: Na ja, wir warten jetzt mal ab. Das macht die Senatskanzlei. Wir brauchen uns um unsere IT gar nicht zu kümmern. – Auch da scheinen noch nicht alle die Dimension des Vorfalls verstanden zu haben, und die IT-Sicherheitsexperten, von denen man so liest, machen das hier auch sehr deutlich. Insofern, glaube ich, brauchen wir die Sitzung und den Besprechungspunkt, um gemeinsam noch mal ein Verständnis dafür zu bekommen, was jetzt vor uns steht und was jetzt dringend passieren muss. – Herr Hauer, ich nehme Ihnen ab, dass Sie das verstanden haben, aber viele andere, die sich äußern, haben es scheinbar noch nicht verstanden. Insofern trägt diese Sitzung hoffentlich dazu bei, mehr Leuten die Augen zu öffnen.

Vorsitzender Johannes Kraft: Vielen Dank! – Dann spricht zur Begründung des Tagesordnungspunktes 3 b der Kollege Förster. – Bitte!

Christopher Förster (CDU): Vielen Dank, Herr Vorsitzender! – Auch wir von der Koalition haben natürlich ein großes Interesse daran, dass wir heute noch deutlich mehr Licht in die Lage bringen. Es ist in den letzten Tagen viel spekuliert und geschrieben worden. Man muss leider festhalten, dass diejenigen, die diese Daten abgegriffen haben, ihre Warnungen und Drohungen wahr gemacht und am Freitag mehr als 5 Terabyte Daten im Darknet veröffentlicht haben. Ich denke, jeder von Ihnen hat in den vergangenen Tagen die unterschiedlichsten Interpretationen und Informationen zu angeblichen Dateien, die dort veröffentlicht worden sind, mit verfolgt. Uns geht es heute auch darum, dass uns einfach mal erklärt wird: Was wissen Sie vonseiten der Verwaltung überhaupt? Wie schlimm ist es? Wie und wohin können sich vor allem betroffene Bürger, aber auch Mitarbeiter der Verwaltung in Zukunft wenden? Wo gibt es Unterstützungsmöglichkeiten? – Darüber würden wir uns heute sehr freuen.

Vorsitzender Johannes Kraft: Dann ergänzt der Kollege Herr Dr. Kollatz. – Bitte!

Dr. Matthias Kollatz (SPD): Danke schön, Herr Vorsitzender! – Wir haben in unserem Antrag zur Tagesordnung ganz bewusst das Wort Bilanz gebraucht. Das heißt, wir glauben, dass es an der Zeit ist, eine Bilanz zu ziehen – vielleicht nicht eine Abschlussbilanz, aber schon so etwas wie eine Zwischenbilanz, denn die Diskussion, die gegenwärtig stattfindet, ist nicht nützlich. Jeder glaubt, etwas Besonderes zu wissen und etwas Besonderes zu sagen und so weiter. Zu einer Bilanz gehört zum einen ein hohes Maß an Transparenz, dazu gehört aber auch, dass im Prinzip klar wird, wo wir stehen: Was ist passiert? Was wird jetzt in den nächsten Tagen und Wochen passieren? – Ich glaube, dass das wichtig ist. Wir werden dann nach dem, was Sie darstellen, auch noch Gelegenheit haben nachzufragen, aber, wie gesagt, dieses Thema Bilanz ist für uns der wichtige Punkt, zu dem wir den Senat und natürlich die anderen Beteiligten um einen Bericht bitten, der diesen Bilanzversuch unternimmt. – Danke!

Vorsitzender Johannes Kraft: Vielen Dank! – Dann darf ich zu diesem Punkt herzlich den Landesbevollmächtigten für Informationssicherheit, Herrn Dr. Kroll-Peters, der bei uns ist, sowie Frau Gieseler aus dem Bereich IKT-Sicherheit begrüßen. – [Zuruf] – Sie ist noch nicht da. Außerdem darf ich Sie darauf hinweisen, dass Frau Plattner, ihres Zeichens Präsidentin des Bundesamtes für Sicherheit in der Informationstechnik, uns um 15 Uhr zugeschaltet sein wird. Das ist, finde ich, eine sehr gute Entwicklung. Ich habe bereits Herrn Staatssekretär Slotty und Herrn Werdin, Leiter des Referats Informationstechnik in der Stadtentwicklungsverwaltung, begrüßt. Aus der Senatsverwaltung für Mobilität, Verkehr, Klimaschutz und Umwelt begrüße ich Herrn Staatssekretär Herz. Außerdem ist Frau Dr. Borelli, Vorständin des ITDZ, heute bei uns. Insofern haben wir die gesammelte Kompetenz hier. Wie gesagt, um 15 Uhr würden wir dann das freundliche Angebot von Frau Plattner annehmen, sich digital zuzuschalten.

Ich darf fragen, ob eine einleitende Stellungnahme des Senats gewünscht ist. – Das ist der Fall. Dann, Herr Staatssekretär Hauer, haben Sie das Wort. – Bitte schön!

Staatssekretär Florian Hauer (Skzl): Sehr geehrter Herr Vorsitzender! Sehr geehrte Damen und Herren Abgeordnete! Ich würde in der Tat beginnen. Ich werde einen aktuellen Bericht geben. Der Bericht wird ein Statusbericht sein; eine Bilanz kann ich zum jetzigen Zeitpunkt noch nicht ziehen. Schön wäre es, wenn wir so weit wären, aber da muss ich leider die Erwartungen etwas einfangen.

Ich würde hier gerne über zwei Themenkomplexe berichten, die ein Stück weit auch zwei Handlungsstränge darstellen und vielleicht auch voneinander getrennt zu beraten sind. Der eine Handlungsstrang sind die Aktivitäten, die wir gerade entfalten, um das Landesnetz zu sichern, also die Wiederherstellung der Integrität des Landesnetzes. Das ist das eine, das vor allem bei uns, beim IKT-Notfallstab, seit Mitte August läuft. Der zweite Handlungsstrang und Themenkomplex, den ich separieren würde, ist das Thema Schadensumfang, Schadensbewertung und Schadensmanagement; das sind also der Datenabfluss, der Datendiebstahl und die Veröffentlichung dieser Daten. Das sind aus unserer Sicht – auch wenn es Überschneidungen gibt – überwiegend zwei separate Handlungsstränge, und deswegen würde ich das hier in meinem Bericht vielleicht so strukturieren.

Ich würde mal mit dem ersten Themenkomplex anfangen, der Sicherung des Netzes. Wir sind seit Mitte August, seitdem wir eine Infiltration des Netzes festgestellt haben, zum einen bemüht gewesen, die Tätergruppe aus dem Netz wieder herauszubekommen, und dann in der Folgezeit sicherzustellen, dass diese Infiltration nicht andauert, fortdauert und dass es nicht zu erneuten Angriffen gekommen ist.

Was haben wir – wir, das heißt, insbesondere der IKT-Notfallstab bei uns in der Senatskanzlei mithilfe der Kolleginnen und Kollegen aus den verschiedenen Behörden – dazu getan? – Wir haben uns zum einen im ersten Schritt selbstverständlich die kritischen Systeme angeschaut. Kritische Systeme sind in dem Sinne so zu verstehen, dass das die Systeme sind, die angesichts der beobachteten Angriffsvektoren als besonders kritisch erachtet wurden. Diese Systeme wurden als allererstes einer forensischen Analyse unterzogen. Damit ging dann eine Fokussierung auf die Wahlumgebung einher, die auch angesichts der Zeitplanung von uns als besonders kritisch erachtet wurde – im nächsten Schritt, nachdem diese Systeme so weit von der Forensik durchleuchtet wurden und auch sichergestellt ist, dass sie einer fortlaufenden Sensorik weiter unterliegen, um etwaige neue Angriffe oder Aktivitäten festzustellen, was aber seit Mitte August nicht der Fall war. Das will ich hier betonen: Seit Mitte August wurden keine weiteren Aktivitäten festgestellt. Seitdem geht es darum, die Forensik in alle Systeme auszurollen. Das ist das, was wir im Moment tun. In dieser Phase befinden wir uns.

Ich habe schon in der letzten Sitzung – oder war es im Innenausschuss vor zwei Wochen? – dargestellt, dass das auch quantitativ eine gewisse Herausforderung ist, weil es sehr viele Systeme sind, die zur Berliner IT-Landschaft gehören. Es ist aber der Anspruch, sie komplett auszurollen. Es sind selbstverständlich die Hauptverwaltung, die nachgeordneten Landesbehörden, aber auch die Bezirke, die dazugehören. Das ist also das Stadium, in dem wir uns gerade befinden. Sobald wir den Punkt erreicht haben, dass wir sagen können, es ist jetzt in alle IT-Systeme des Landes ausgerollt, wird es noch einige Tage dauern, bis die forensische Analyse hoffentlich so weit vorangeschritten ist, dass wir eine erste Zwischenbilanz ziehen können, zumindest mit Blick auf den erfolgten Angriff und die Frage, ob die Integrität des Landesnetzes, der Landes-IT wiederhergestellt ist.

Parallel dazu werden in diesem Handlungsstrang bereits Anstrengungen unternommen, um auch über die konkrete Gefahrenabwehr hinaus kurzfristig Maßnahmen zu ergreifen, die das System ein Stück weit härten sollen. Denn es ist auch klar, dass wir uns auch künftig mit solchen Szenarien auseinandersetzen müssen oder mit solchen Szenarien konfrontiert sein werden. Deswegen müssen wir uns diese Frage jetzt stellen und können das nicht auf die lange Bank schieben. Wir machen das jetzt direkt. Wie gesagt, in den nächsten Tagen und Wochen wird die forensische Sensorik fortlaufend die gesamten Aktivitäten dort überwachen, sodass wir davon ausgehen, dass wir es sofort detektieren und sehen würden, wenn es entweder zu neuen Angriffen kommt oder möglicherweise die Angreifer doch noch im System drin sind – bisher unbekannt, unerkannt und unentdeckt. – Das ist der eine Handlungsstrang.

Jetzt würde ich zum zweiten Themenkomplex kommen: Das ist der Datenabfluss, der leider stattgefunden hat, mit dem wir jetzt konfrontiert sind, den wir in irgendeiner Form managen müssen. Ich will gleich zu Beginn sagen: Ich werde in keinerlei Weise versuchen, den entstandenen Schaden irgendwie zu relativieren oder kleinzureden. Es ist rein zahlenmäßig eine immense Summe an Dateien, die abgeflossen ist. Es hat verschiedene Dimensionen. Es hat für betroffene Beschäftigte eine unmittelbare Wirkung, es hat für Bürgerinnen und Bürger und Unternehmen, die betroffen sind, ganz konkrete Auswirkungen. Jeder, der vielleicht selbst schon mal einen solchen Brief von irgendeinem Unternehmen oder von einem Dienstleister bekommen hat, bei dem es zu einem Datenabfluss gekommen ist, weiß aus eigener Erfahrung, wie schockiert man in dem Moment ist, wenn man einen solchen Brief bekommt und anfängt nachzudenken: Was heißt das denn jetzt eigentlich? Was muss ich in einer solchen Situation machen? – Die dritte Dimension ist die Frage der kritischen Infrastruktur und ähnlichem, von Behördenstellen bis hin zu Einrichtungen und Verfassungsorganen des Bundes, die, wie wir feststellen mussten, auch in irgendeiner Form betroffen sind.

Ich will vielleicht an der Stelle noch einmal kurz darstellen, was aus unserer Sicht in den letzten Tagen rein von der Chronologie her passiert ist und welche Fakten wir als gegeben ansehen: Wir hatten am 28. August das Ultimatum. Der Senat hat dann eine Entscheidung getroffen, auf diese Forderungen nicht einzugehen, und es war absehbar – leider –, dass dann eine Frist von sieben Tagen läuft. Diese Frist ist am Freitag um 15.35 Uhr ausgelaufen. Wir haben uns in den Tagen davor selbstverständlich mit den Szenarien auseinandergesetzt, auch zusammen mit den Sicherheitsbehörden. Wir sind Szenarien durchgegangen. Am Ende ist dieses Szenario, das jetzt eingetreten ist, die weitestgehende Komplettveröffentlichung der Daten, das, was als am wahrscheinlichsten angenommen wurde. So ist es dann auch gekommen. Wir kannten seit dem 28. August aufgrund der Indexierung der Inhaltsverzeichnisse, die die Tätergruppe selbst ins Darknet eingestellt hatte, zumindest die Spannbreite dessen, was betroffen sein könnte.

Ich wollte hier vielleicht auch noch einmal erwähnen, was wir bereits seit dem 28. August – oder schon zwei Tage länger – wussten, seitdem wir diesen zusätzlichen Datenabfluss festgestellt hatten: Wir wussten bis dahin durch unsere forensischen Untersuchungen, was bei den Behörden, in dem Fall SenMVKU und SenStadt, an Daten abgeflossen ist. Das konnten wir durch forensische Untersuchungen feststellen. Über die Zahlen habe ich Sie auch fortlaufend informiert; die gingen im Laufe der Tage nach oben. Man war am Anfang von 8 700 Dateien gesichert ausgegangen. Man ist dann relativ schnell leider zu dem Ergebnis gekommen, dass es wohl höchstwahrscheinlich 100 000, 115 000 und potenziell 215 000 Dateien sind. Das ist das, was wir aufgrund der eigenen forensischen Erkenntnisse in den eigenen Daten feststellen

konnten. Was tatsächlich abgeflossen ist, haben wir dann aber erst jetzt am Freitag um 15.35 Uhr festgestellt, als die Täter im Darknet angefangen haben, ihre Daten zu veröffentlichen. Das wissen wir erst seit Freitag um 15.35 Uhr. Zu den Zahlen, die mir vorliegen – ich kann jetzt nur das berichten, was das LKA mir berichtet hat: Am Freitag um 15.35 Uhr war von 755 000 Dateien die Rede. In der Nacht von Samstag auf Sonntag wurde dann noch ein weiteres Datenpaket freigegeben; das waren dann noch einmal 550 000 bis 560 000 Dateien. Das ist die Dimension, über die wir jetzt reden: 1,2 bis 1,3 Millionen Dateien.

Unsere Herangehensweise will ich jetzt hier vielleicht noch einmal erklären: Wir stehen jetzt vor der Aufgabe, dass wir feststellen müssen, was diese Dateien an Informationen enthalten. Dafür haben wir zwei Anknüpfungspunkte, ich habe es eben schon gesagt: Wir haben auf der einen Seite die Daten in den Verwaltungen, von denen wir wissen, dass sie kopiert worden sind. Das ist der eine Anknüpfungspunkt, um eine Analyse vorzunehmen. Der zweite Anknüpfungspunkt sind die Daten, die von der Tätergruppe veröffentlicht wurden. Das sind für uns zwei unterschiedliche Anknüpfungspunkte. Für das eine Paket, für das erste, von dem wir bereits seit dem 28. August wissen, ist es technisch gesehen relativ einfach, zumindest die Dateien zu identifizieren und zu durchsuchen. Für den zweiten Datenpool, also das, was seit Freitag veröffentlicht wurde, stellt sich das Ganze technisch schon etwas schwieriger dar.

Journalistinnen und Journalisten haben den Vorteil, dass sie willkürlich die Dateien durchgehen und das anklicken können, was aus ihrer Sicht interessant ist; dann können sie sich die Dateien anschauen und auch darüber berichten, was völlig legitim ist. Unser Anspruch muss sein, dass wir eine systematische Erfassung vornehmen. Eine systematische Erfassung geht nur dergestalt, dass wir zum einen diese Daten erst einmal sichern, was technisch gar nicht trivial ist, weil es bei den Sicherheitsbehörden aufgrund der schieren Größe und der langsamen Übertragungsbreite mehrere Tage dauert, diese Datenpakete herunterzuladen, dann die Daten zu sichern und auf einem separaten, gesicherten Server zur Verfügung zu stellen, damit wir diese Daten von dieser Seite aus systematisch analysieren können. Und was heißt dann analysieren? – Es ist Ihnen allen klar, dass es sehr aufwendig sein wird, jede Datei einzeln durchzugehen, wenn wir hier über mehr als 1 Million Dateien sprechen, die vielleicht sogar mehrere Dokumente enthalten. Aber um am Ende Betroffenheiten herauszufinden, Betroffene zu identifizieren, um auch Risiken einzuschätzen, werden wir um diese Aufgabe am Ende nicht herumkommen, dass wir all diese Dateien und Informationen einzelfallbezogen prüfen, bewerten und gegebenenfalls die notwendigen Maßnahmen ableiten.

Es ist klar, dass es in jedem Fall sehr lange dauern wird, wenn wir das Schritt für Schritt durchgehen. Deswegen ist unsere Herangehensweise jetzt, dass wir mithilfe von KI-Tools versuchen, diese Daten hinsichtlich ihrer Risikobezogenheit zu priorisieren: Die KI wird mit bestimmten Schlagwörtern gefüttert, und wir können durch die KI unter Priorisierungsgesichtspunkten eine Katalogisierung vornehmen, sodass wir am Ende die Dateien abgestuft nach Risikopotenzial angezeigt bekommen. Die Dateien, die als die am meisten risiko- und gefährdungsbehafteten erachtet werden, können dann prioritär geprüft werden. Prioritär zu prüfen heißt aber, dass vor allem die Kolleginnen und Kollegen aus den Fachverwaltungen, die das Fachwissen haben, sich erst einmal diese Dateien anschauen müssen. Hoffentlich können sie bei vielen Dateien schon im Rahmen einer summarischen Prüfung sagen: Diese sind völlig unproblematisch, das können wir beiseitelegen. – Wenn sie aber zu dem Ergebnis kommen, dass gewisse Dateien ein gewisses Risiko haben und wir nicht ausschließen können, dass damit eine gewisse Gefahr verbunden ist, dann müssen wir uns das näher anschauen.

Bei diesem näheren Anschauen müssen selbstverständlich irgendwann die Sicherheitsbehörden mit eingebunden werden, entweder, weil sie betroffen sind oder weil es dann um Maßnahmen geht, die abgeleitet werden. Ich sage nur das Stichwort Objektschutz, Personenschutz et cetera. Als Beispiel – das sind jetzt aber fiktive Beispiele, die ich hier nenne: Wir suchen mit dem Schlagwort KRITIS. Wir finden einen Dateitreffer, der betrifft zum Beispiel ein Tanklager, bei dem man sagen kann, das ist Teil der kritischen Infrastruktur. Im Idealfall gucken dann die Kolleginnen und Kollegen rein, stellen fest, dass das Tanklager gar nicht mehr existiert, weil das eine Datei ist, die zehn Jahre alt ist. Das wäre der Idealfall und der einfachste Fall. Oder das sind Informationen, die man auch so im Internet findet. Wahrscheinlicher – oder zumindest möglich – wird es sein, dass dieses Tanklager sehr wohl noch existiert und diese Datei auch sensible Informationen enthält über den Standort, vielleicht über Ansprechpartner, Mitarbeiter bis hin zu Telefonnummern. Dann muss man da konkret reingehen, auch mit dem LKA zusammen, und muss überlegen: Was machen wir jetzt? Müssen wir an dem Standort den Objektschutz hochfahren? Müssen wir die Betroffenen warnen, dass sie ihre Nummern aktualisieren, dass sie aufmerksam sind? – Das ist die Aufgabe, vor der wir ganz konkret stehen. Ich will nur dieses Beispiel nennen, damit Sie sehen, vor welcher großen Herausforderung wir in den nächsten Wochen stehen werden, auch zahlen- und arbeitsmäßig. Aber wir müssen das tun, alles andere ist keine Option. Wir müssen diesen Weg gehen, und, wie gesagt, wir werden diesen Weg gehen, indem wir mithilfe von KI-Einsatz und Schlagworten eine risikobezogene Priorisierung vornehmen und dann diese Dinge so schnell wie möglich abarbeiten. Das wird aber Zeit in Anspruch nehmen. Das wird sehr viele Ressourcen binden. Ich kann Ihnen zusagen, dass wir die dafür notwendigen Ressourcen aufbringen und intern entsprechend priorisieren müssen und werden.

Vielleicht beschreibe ich an der Stelle auch noch einmal, was wir bereits in organisatorischer und institutioneller Hinsicht getan haben: Wir haben in der letzten Woche, als uns klar war, dass dieses Szenario eintreten wird oder mit diesem Szenario zu rechnen ist, dass es zu einer weitgehenden Komplettveröffentlichung kommt, dafür organisatorische Vorkehrungen getroffen. Das BKA hat eine eigene BAO eingerichtet. Die Senatsverwaltung für Verkehr und Umwelt hat eine eigene BAO eingerichtet. Die beiden Senatsverwaltungen haben eine Taskforce eingerichtet, und weil wir sehen, dass es dort übergreifende Aspekte und eine gewisse Steuerungs- und Koordinierungsnotwendigkeit gibt, zusätzlich zum IKT-Notfallstab, der seit Mitte August tagt, haben wir eine zentrale Steuerungseinheit bei uns in der Senatskanzlei eingerichtet, um diese Prozesse zu unterstützen.

Vielleicht ein letzter Aspekt in diesem Zusammenhang: Die Betroffenheit beschränkt sich nicht auf Berlin, sondern es sind wahrscheinlich auch Bundesbehörden betroffen. Sie haben die Presseartikel gelesen. Ich habe seit Freitag viele Telefonate geführt, auch viele Telefonate von besorgten Kolleginnen und Kollegen von der Bundesseite erhalten. Ich kann aber sagen, dass die Bundesbehörden schon sehr frühzeitig, eigentlich von Anfang an, eingebunden waren, das BSI sowieso. Ich bin dankbar, dass die BSI-Präsidentin hier gleich mit uns in den Austausch kommen wird. Das BSI unterstützt uns seit Anbeginn sehr gut. Dafür bin ich ausdrücklich dankbar. Auch mit anderen Sicherheitsbehörden des Bundes sind wir im engen Austausch. Aber auch da wird es darum gehen, einen Prozess durchzuführen, wie ich ihn eben beschrieben habe. Auch die Bundesbehörden werden für ihren Bereich Schlagwortlisten erstellen, die es uns ermöglichen, eine risikobezogene Priorisierung durchzuführen, dass wir unter Risiko- und Gefährdungsgesichtspunkten wissen, welche Dateien wir uns als Erstes anschauen müssen, um dann eine solche einzelfallbezogene Analyse durchzuführen.

- schu/kr -

Ich habe eingangs gesagt, ich möchte nichts relativieren. Ich bin mir der Dimension in qualitativer und quantitativer Hinsicht absolut bewusst. Ich habe jetzt wenig über die Bürgerinnen und Bürger und Unternehmen, sondern vor allem über die kollektive Sicherheit gesprochen, aber wir sind uns auch dieser Dimension bewusst. Ich bin sehr dankbar, dass Frau Kamp uns beratend an der Stelle sehr gut unterstützt. Wir müssen jetzt einen Weg finden, wie wir die betroffenen Bürgerinnen und Bürger so schnell wie möglich identifizieren, aber da stellt sich die gleiche Herausforderung wie bei den Behörden, die ich eben genannt habe. Auch da wird es darum gehen, die Menschen so schnell wie möglich zu informieren, nicht nur, weil wir es in der Sache für geboten halten, sondern weil wir dazu auch gesetzlich verpflichtet sind, vor allem die datenführenden Behörden. Es gibt in den Datenschutzgesetzen und auch in der DSGVO klare Vorschriften, was bei Datenschutzvorfällen zu passieren hat. Dem müssen wir so schnell wie möglich nachkommen. Im Moment sind uns einfach nur faktische Grenzen gesetzt, die das Ganze erschweren.

Ich wollte noch einen Satz sagen, weil am Wochenende viel zu lesen war von, ich will nicht sagen, dramatischen Nachrichten, was das Schadenspotenzial angeht. Noch einmal: Ich will nichts relativieren, und wir sind bei der Risikobewertung der abgeflossenen Dokumente erst am Beginn, aber bisher haben wir keine Erkenntnisse dahingehend, dass die nationale Sicherheit – nationale Sicherheit wiederum in Bezug oder im Sinne von Verteidigungsfähigkeit der Bundesrepublik Deutschland, also auch mit Bezug auf die Bundeswehr – tatsächlich bedroht wäre, dass solche sensiblen Daten abgeflossen sind. Dass die nationale Verteidigungsfähigkeit bedroht wäre, dazu haben wir bisher zum Glück keine Erkenntnisse. Aber noch einmal: Wir befinden uns erst am Beginn des Untersuchungs- und Analyseprozesses, und ich habe eben schon gesagt, diese Fragen gehören zu den Themenkomplexen, die wir prioritär prüfen und analysieren werden. – Das von meiner Seite einleitend. Dann würde ich, Herr Vorsitzender – meine Kollegen aus den beiden betroffenen Senatsverwaltung sind ja noch hier –, gegebenenfalls ihnen noch das Wort geben, wenn es gewünscht ist.

Vorsitzender Johannes Kraft: Vielen Dank! – Beide, sowohl Staatssekretär Herz als auch Staatssekretär Slotty, haben angekündigt, dass sie ergänzen möchten. – Herr Staatssekretär Slotty, bitte! Sie haben das Wort.

Staatssekretär Alexander Slotty (SenStadt): Vielen Dank, Herr Vorsitzender! – Sehr geehrte Damen und Herren Abgeordnete! Ich möchte meinen Kollegen ergänzen, will vielleicht aber noch voranstellen, dass wir seit etwas mehr als drei Wochen in dieser Lage sind und ich mich bei den Kolleginnen und Kollegen sehr herzlich für die Zusammenarbeit bedanken möchte. Sie können sich vorstellen, dass wir alle seit dem Freitag vor drei Wochen in permanentem Austausch miteinander stehen. Ich will es deswegen an dieser Stelle nicht unerwähnt lassen, denn wir sind vielleicht ein Stück weit die Gesichter, die hier die Informationen transportieren, aber neben mir sitzt der Leiter unserer IT und hinter ihm steht ein weiteres Team. Die Kolleginnen und Kollegen sind im Prinzip seit dreieinhalb Wochen jeden Tag, ich will eigentlich sagen, Tag und Nacht, auch am Wochenende, im Dienst und im Einsatz, um eine Sicherheit zu gewährleisten, die wir jetzt brauchen, und hier die Aufklärung mit uns gemeinsam voranzutreiben. Ich vermute, dass Sie sich alle diesem Dank anschließen.

Worüber sehr viel spekuliert wird, ist der Punkt, an dem die Infiltration im Landesnetz stattgefunden hat. Da muss man am heutigen Tage sagen: Wir können das auch heute immer noch nicht mit aller Sicherheit beantworten. Das liegt vor allem daran, dass diese Frage Gegenstand

der Ermittlungen der Strafverfolgungsbehörden ist und die IT-Infrastruktur, die in diesem Zusammenhang steht oder stehen könnte, vom LKA frühzeitig beschlagnahmt wurde, um die Ermittlungen führen zu können. Das hat uns aber an der Stelle die Möglichkeit genommen, mit unserer eigenen Forensik zu ermitteln. Insofern kann das, was im öffentlichen Raum diskutiert wird oder was man in der Presse gelesen hat, stimmen, es muss aber nicht stimmen.

Man weiß über die Hackergruppe – das ist uns durch das Briefing, das wir durch BSI, BKA und BfV seinerzeit erhalten haben, bekannt –, dass die Gruppe oft mit Phishing-E-Mails agiert, in denen man als Teil einer Institution, als Mensch etwas herunterladen muss, etwas anklicken muss und so die Möglichkeit eröffnet, Schadsoftware oder Ähnliches in ein System einzuspielen. Insofern muss man sagen: Das ist das untere Level der Sicherheitsarchitektur in so einer IT, nämlich der Mensch. Der Mensch ist der Letzte, der mit seinem Finger auf der Tastatur oder der Maus entscheidet, ob er ein Sicherheitsrisiko eingeht oder nicht. In diesem Fall gibt es natürlich noch Sicherheitslevel darüber. Darüber ist die IT-Stelle der Senatsverwaltung für Stadtentwicklung, Bauen und Wohnen, die das aus einer gewissen Historie und wegen des Umfangs an IT-Fachverfahren, die bei uns in den beiden Häusern, SenMVKU und SenStadt liegen, selbst macht. Darüber gibt es noch das ITDZ als Sicherheitslevel. Das heißt, es gibt unterschiedliche Szenarien, die hier eingetreten sein können, bei denen auch unterschiedliche Sicherheitslevel passiert werden mussten, damit sich so eine Lage am Ende ergibt.

Ich will, ohne jetzt zu viel zu wiederholen, noch ein paar Punkte heute hier in der Öffentlichkeit sagen. Wir haben in der letzten Ausschusssitzung sehr umfangreich in einem nichtöffentlichen Teil tagen müssen. Die Situation hat sich nach der Veröffentlichung der Daten ein Stück weit verändert. Ich hoffe, dass trotzdem alle mit mir übereinstimmen, wenn ich sage, dass wir auch hier in vertraulichen Sprecherrunden versucht haben, so viele Informationen wie möglich weiterzugeben, um trotz der sensiblen Lage dem Informationsbegehren des Parlamentes nachzukommen. Insofern will ich auch erklären – und das wird sicherlich irgendwann noch einmal Gegenstand vertiefter Untersuchungen werden: Meine eigene erste Frage an meine IT-Stelle war, als die Krise begann, wie es mit dem Status unserer Hardware aussieht. Was ist mit der Software? – Die Kolleginnen und Kollegen haben mir mehrfach versichert: Unsere Hardware ist auf dem aktuellen Stand. Unsere Virenscanner, unsere Firewall, all diese Systeme, die man braucht, um Sicherheit für IT herzustellen, waren auf dem aktuellen Stand der Technik, waren alle aktuell geuptdatet. Das heißt, diese Punkte, die wir natürlich verpflichtend einzuhalten haben, haben wir auch eingehalten. Die Systeme sind entsprechend der Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik konfiguriert. Insofern sind wir, was die Frage angeht, wo genau das Ganze ausgelöst wurde, wo das passiert ist, genauso gespannt wie alle anderen auch.

Ich will auch noch sagen: Wir haben schon vor etwas über zwei Jahren ein sehr umfangreiches Schulungssystem für unsere Mitarbeiterinnen und Mitarbeiter in den beiden Verwaltungen eingeführt. Sowohl die Leitung in der SenMVKU als auch ich für die SenStadt haben seinerzeit entschieden, dass die Teilnahme an diesen IT-Sicherheitsschulungen – das System heißt SoSafe – für alle verpflichtend erfolgen muss. Das heißt, ich werde als Mitarbeiterin, als Mitarbeiter dieser beiden Verwaltungen regelmäßig geschult, und zwar immer wieder mit aktuellen Schulungen. Diese Schulungen hören auch nie auf. Wenn ich ein Modul abgeschlossen habe, wird dieses Modul aktualisiert und ein halbes Jahr oder ein Jahr später wieder neu eingespielt. Das heißt, ich bin permanent in einer Schulungssituation. Wir haben natürlich

auch das entsprechende Modul, das hier aufgrund der aktuellen Erkenntnisse besonders wichtig geworden ist, wieder entsprechend aktualisiert. Insofern sind wir, was das Thema IT-Sicherheit betrifft, mit Blick auf die Mitarbeiterinnen und Mitarbeiter, glaube ich, schon sehr gut aufgestellt, auch wenn man am Ende immer noch mehr tun kann.

Es gibt an dieser Situation wirklich nichts schönzureden, das ist so. Trotzdem gibt es natürlich auch gute Nachrichten, und da geht es mir wie dem Kollegen Hauer: Ich will hier überhaupt nichts relativieren oder schönreden, aber auch ich habe mich die letzten dreieinhalb Wochen sehr intensiv mit dem Agieren dieser Hackergruppe auseinandergesetzt, weil man sich natürlich sofort dafür interessiert, wenn man Opfer einer solchen schweren Straftat geworden ist, wie so etwas eigentlich abläuft. Diese Hackergruppe ist bekannt dafür, dass sie normalerweise Daten aus Systemen für sich generiert, das heißt sie kopiert, löscht oder verschlüsselt. Die gute Nachricht ist, dass unsere IT-Sicherheit auch dahingehend so gut funktioniert hat, dass wir zwar nicht sofort, aber wenigstens nach ein paar Tagen erkannt haben, dass in den IT-Systemen Unregelmäßigkeiten bestehen, und mit geeigneten Maßnahmen entgegengewirkt haben. Insofern kann ich Ihnen heute von der Größenordnung her einen Eindruck vermitteln: Es sind 1 Prozent der Daten, die sich auf den Servern der SenStadt befinden, abgeflossen, nicht mehr, aber natürlich auch nicht weniger. 1 Prozent können trotzdem über 1 Million Daten sein, und natürlich ist das erschlagend, aber es sind eben auch nicht mehr. Es sind auch keine Systeme in unseren Häusern verschlüsselt worden, wie es oftmals der Fall ist, die dann für die Organisationen, die diese Systeme betreiben, möglicherweise für immer zerstört werden oder eben verloren gehen. Das heißt, die Maßnahmen haben zumindest an der Stelle Schlimmeres verhindert.

Ich hatte bereits gesagt, dass die Aufklärung durch die Ermittlungsbehörden läuft. Das führt allerdings auch dazu, dass unsere eigene interne Aufklärung ein Stück weit erschwert ist, wie ich eingangs schon sagte, insbesondere in der Frage, wo genau der Punkt war, an dem die Hacker auf das System getroffen sind und man ihnen die Tür geöffnet hat oder sie eine offene Tür gefunden haben, wie auch immer.

Wir waren in den letzten zehn Tagen mit vielen weiteren Fragen befasst. Durch die erste Veröffentlichung am Freitag vor einer Woche haben wir Kenntnis davon erlangt, dass es sein könnte, dass sogenannte Zertifikate kopiert worden sind. Die Zertifikate sind unter anderem das, was ich benötige, um als Mitarbeiter aus dem Homeoffice oder als Bezirk aus der Entfernung auf unsere IT-Fachverfahren zuzugreifen. Das ist das, was ich beispielsweise benötige, um über Citrix auf die Server in der SenStadt zu kommen. Da wir nicht ausschließen konnten, dass diese Dateien auch kopiert worden sind, haben wir uns Freitag vor einer Woche noch sehr spät abends, es war fast nachts, entschieden, das ITDZ zu bitten, diese Zertifikate zu deaktivieren, damit mit all diesen Zertifikaten nicht mehr gearbeitet werden kann. Das heißt, wir haben zwischen der Veröffentlichung um etwa 15.35 Uhr bis abends um 22 Uhr diese Maßnahme ergriffen. Herr Werdin wird sicherlich heute auf Ihre Fragen antwortend noch detaillierter darauf eingehen. Das heißt, dass wir es an dieser Stelle verhindert haben, dass Zugriffe von außen auf die teilweise sehr teuren IT-Fachverfahren, die unsere Verwaltungen benötigen, um ihre Arbeit zu erledigen, weiter erfolgen können.

Es hat sich mittlerweile durch die Datenveröffentlichung herausgestellt, dass sich die Hacker nicht einfach nur den Zugang zu den Daten verschafft und die kopiert haben, sondern dass sie auch sehr intensiv ihre Spuren verwischt haben. Das hat es uns natürlich noch mal erschwert,

gleich zu Beginn dieser Krise zu erkennen: Womit haben wir es zu tun? Was genau ist passiert? – Das heißt, die sogenannten Logdateien, die entstehen, wenn ich einen Kopiervorgang starte, sind eigentlich alle nicht da, mit wenigen Ausnahmen. Da sind der Forensik, der Aufklärung, einige Steine in den Weg gelegt worden, und auch das führt dazu, dass wir deutlich langsamer sind, als das nachvollziehbarerweise von uns erwartet wird.

Es fiel schon das Stichwort Opferschutz. Ich hätte das auch meinerseits hier angesprochen. Die Sicherheit der Bürgerinnen und Bürger und natürlich auch der Mitarbeiterinnen und Mitarbeiter unserer Häuser steht absolut im Vordergrund. Wir müssen mit dieser Situation umgehen, wie sie ist und können nur für alle das einrichten, was sie brauchen. Wir haben beispielsweise bei uns im Haus – der Kollege wird das sicherlich gleich für seine Verwaltung sagen – unmittelbar am ersten Wochenende, nachdem wir Kenntnis erlangt haben, hausintern einen Krisenstab aktiviert. Dieser Krisenstab tagt nach wie vor täglich, und wir haben darüber hinaus weitere Maßnahmen ergriffen. Wir haben beispielsweise eine zentrale Ansprechstelle bei uns im Hause geschaffen, damit Kolleginnen und Kollegen persönliche Fragen und Anliegen im Zusammenhang mit dem Cyberangriff loswerden können. Wir haben alle noch einmal auf unser Angebot der Sozialberatung hingewiesen, wenn die aktuelle Situation zu Verunsicherung oder Sorgen führt. Wir haben gemeinsam mit der SenMVKU – oder besser gesagt, auf Initiative der SenMVKU – eine auf IT und Datenschutz spezialisierte Rechtsanwaltskanzlei als externe Beratungsstelle für unsere Beschäftigten eingerichtet. Wir haben die jeweiligen Beauftragten für Informationssicherheit, Datenschutz und Geheimschutz für Fragen noch einmal hausintern benannt, und wir haben für die Fälle, dass Kolleginnen und Kollegen durch kompromittierende Informationen beispielsweise von außen kontaktiert werden, erpresst werden oder Ähnliches darauf hingewiesen, dass die Internetwache, die örtlichen Dienststellen der Polizei zur Erstattung von Strafanzeigen zur Verfügung stehen und haben auch alle ermutigt, sich für den Fall, insbesondere von Erpressungsversuchen, sofort bei ihren Dienststellen zu melden, damit hier entsprechende Unterstützung gewährleistet sein kann. Das ist das, was wir als Sofortmaßnahmen erst mal möglich gemacht haben. Wie es der Kollege Hauer schon sagte: Wir stehen hier natürlich in der Pflicht, alle Bürgerinnen und Bürger, alle Kolleginnen und Kollegen unsererseits zu kontaktieren und über den Abfluss von personenbezogenen Daten zu informieren. Das werden wir auch tun. Sobald diese Auswertung entsprechend fortgeschritten ist, wird das nach und nach erfolgen. – Herzlichen Dank!

Vorsitzender Johannes Kraft: Vielen Dank, Herr Staatssekretär! – Dann hätte jetzt Arne Herz als Staatssekretär bei der Senatsverwaltung für Mobilität, Verkehr, Umwelt und Klimaschutz das Wort. Ich will mal darauf hinweisen, dass wir um 15 Uhr Frau Plattner per Schalte erwarten – nur, dass wir das alle im Hinterkopf haben. – Bitte schön, Staatssekretär Herz!

Staatssekretär Arne Herz (SenMVKU): Herzlichen Dank, Herr Vorsitzender! Das kriege ich hin. Ich will insofern nur ergänzen: Wir haben uns in der Woche, in der bekannt wurde, dass jenseits der öffentlich zugänglichen Daten auch weitere abgeflossen sind, gleich zu Beginn insofern Verstärkung an Bord geholt, dass wir eine große Anwaltskanzlei, die darauf spezialisiert ist, gebunden haben. Wir haben in der Folge insbesondere die Prozesse aufgelegt, die wir brauchten, um eine erste Möglichkeit zu haben, in die Dateien hineinzugucken. Das dauert ein paar Tage, wie Staatssekretär Hauer schon dargestellt hat. Ich will sagen: In der Zweiteilung der Aufklärung über den Abfluss und die IT-Sicherheit, die der CDO, glaube ich, schon sehr gründlich beleuchtet hat und das im Zweifelsfall heute noch weiterhin tun wird, kann ich mich dem Kollegen Slotty nur anschließen.

Wir haben nicht nur für Dritte außerhalb der Senatsverwaltung, sondern genauso für unsere Beschäftigten eine Verantwortung, deren Daten abgeflossen sind. Deswegen haben wir noch in der Woche, in der bekannt wurde, dass ein Datenabfluss jenseits der öffentlich zugänglichen Daten erfolgt ist, einerseits eine Ansprechstelle für IT-Sicherheitsfragen innerhalb der Verwaltung eingerichtet und den Kolleginnen und Kollegen als erste Maßnahme Verhaltensregeln mit an die Hand gegeben. In der Folgewoche haben wir in der Gemeinsamkeit mit der Senatsverwaltung für Stadtentwicklung nicht nur noch einmal auf die Sozialberatung hingewiesen, weil natürlich so etwas mit einem Menschen etwas macht, wenn er davon erfährt, dass persönliche Daten abgeflossen sein können, sondern gleichzeitig auf die Kanzlei, die über uns gebunden wurde als externe Beratungsstelle, um auch einen Vertrauensanwalt zu haben, der außerhalb der Behörde sitzt. Diese Kanzlei wird da, wo es relevant ist, selbstverständlich mit uns im Austausch stehen, damit wir Kenntnis von bestimmten Dingen erlangen, die wir untersuchen können sollten – nicht in Bezug auf den Beschäftigten, sondern in Bezug auf die Daten –, aber ansonsten besteht für die Beschäftigten auch die Möglichkeit, ganz bewusst eine solche Anlaufstelle zu haben, die erst mal nur für sie da ist. Der Kollege Hauer wird sicherlich darstellen, wie das in der Folge auch für betroffene Dritte gemeinsam mit unseren drei Verwaltungen organisiert wird. Deswegen würde ich mich jetzt erst mal darauf beschränken.

Ich will nur eines sagen: Wir haben dafür keine Blaupause. Deswegen sind wir, glaube ich, alle in der Verantwortung, das uns Mögliche und auch darüber Hinausgehende zu tun, um mit einer Situation umzugehen, in der wir schlicht schnell aufklären wollen und werden. Das tun wir in den ganzen Wochen schon, aber insbesondere seit dem Freitag sind wir auch darauf angewiesen, dass wir sämtliche Dateien in der Indexierung zugeliefert bekommen.

Vorsitzender Johannes Kraft: Vielen Dank! – Dann darf ich die Technik fragen, ob Frau Plattner schon zugeschaltet ist. – Sie ist noch nicht da. Gut. Wie wollen wir dann verfahren? Ich hätte jetzt schon vier Kollegen auf der Redeliste. – Moment, völlig richtiger Hinweis: Wir würden natürlich fragen, ob sich Frau Kamp und Frau Dr. Borelli noch ergänzend einlassen möchten. Das können Sie zu einem anderen Zeitpunkt auch machen, es muss nicht jetzt sein. – Dann sehr gerne, Frau Kamp!

Meike Kamp (Berliner Beauftragte für Datenschutz und Informationsfreiheit): Ich kann mich ja so lange einlassen, bis Frau Plattner am Telefon ist. – Ich würde gern zwei Sachen sagen. Einmal ist es so, dass ich mich als Berliner Beauftragte für Datenschutz und Informationsfreiheit entschlossen habe, jetzt auch aktiv in die Beratung einzusteigen und an der gegründeten Steuerungseinheit, über die Herr Hauer möglicherweise noch sprechen wird – ich möchte ihm jetzt nicht vorgreifen –, regelmäßig teilnehmen und unsere Aufgabe beratend gegenüber dem Senat wahrnehmen werde. Wir sind natürlich Kontroll- und Aufsichtsbehörde, das ist klar, und in der Regel wahrt man als Aufsichtsbehörde in der Funktion meiner Unabhängigkeit natürlich eine gewisse Distanz, weil man kontrollieren soll. Hier in dieser Situation möchten wir aber unsere Aufgabe vor allen Dingen wahrnehmen, den Senat zu beraten und dort insbesondere die Perspektive der Datenschutzanforderungen der weiteren Maßnahmen, die ergriffen werden, sowie die Perspektive der Transparenzherstellung in diese Beratungen mit einzubringen. Es ist aus unserer Sicht der wesentliche Punkt momentan, dass ein Informationsangebot und Transparenz geschaffen werden, dass Verfahren entwickelt werden, wie die Betroffenen benachrichtigt oder beauskunftet werden können.

Wir selbst haben am Samstagmorgen noch einmal aktualisierte FAQs auf unsere Webseite gesetzt, wo wir ein Informationsangebot für die Betroffenen geschaffen haben. Wir haben im bisherigen Austausch mit dem Senat, mit allen Senatsverwaltungen und mit dem CDO betont, dass wir davon ausgehen, dass senatsseitig ein eigenes Informationsangebot auch für Externe geschaffen wird, das noch mal auf bestimmte Punkte hinweist und auch Ansprechstellen schafft, die dann zur Verfügung stehen, wenn Betroffene ihre Auskunfts- oder Benachrichtigungsrechte geltend machen wollen. – Vielen Dank!

Vorsitzender Johannes Kraft: Vielen Dank, Frau Kamp – eine Punktlandung! Mir wurde gerade signalisiert, dass Frau Plattner jetzt so freundlich ist, uns per Video zugeschaltet zu sein. Ich sehe sie noch nicht.

Claudia Plattner (Bundesamt für Sicherheit in der Informationstechnik; Präsidentin) [zugeschaltet]: Ich wäre da! Hören Sie mich?

Vorsitzender Johannes Kraft: Hallo, Frau Plattner! Herzlich willkommen hier im Ausschuss für Digitalisierung und Datenschutz! – Sie wissen, dass diese Sitzung übertragen und auch aufgezeichnet wird und später abrufbar ist. Wir befinden uns in einem öffentlichen Teil, das heißt, wir haben hier auch die Presse zugegen, die Aufnahmen anfertigen darf. – Ich begrüße Sie herzlich, bedanke mich im Namen des Ausschusses, dass Sie sich als Präsidentin des Bundesamtes für Sicherheit in der Informationstechnik die Zeit für uns nehmen, und vielleicht, wenn Sie möchten, uns einleitend Ihren Blick auf die Geschehnisse in den vergangenen Wochen in Berlin zukommen lassen!

Claudia Plattner (BSI) [zugeschaltet]: Das mache ich sehr gerne! – Zunächst einmal herzlichen Dank für die Einladung und für die Möglichkeit, hier auch ein paar Worte zu sagen! Ich weiß das zu schätzen, und ich weiß vor allen Dingen die Bemühungen der Kolleginnen und Kollegen dort vor Ort zu schätzen, die sich jetzt um dieses Thema kümmern und hier den Schaden so klein wie möglich halten.

Ich glaube, was grundsätzlich geschehen ist, ist inzwischen verstanden: Ein Angreifer einer Cybercrime-Gruppe hat sich Zugriff auf die Daten verschafft, hat dort aus diesen Senatsverwaltungen dann doch eine relativ große Menge Daten entwendet. Dabei ist es dann aber doch gelungen, das rechtzeitig zu bemerken, bevor eine Verschlüsselung stattfinden konnte. Das ist, wenn man so will, Glück im Unglück, ändert aber nichts an der Tatsache, dass eine große Menge Daten, über 5 Terabyte, abgeflossen ist und dort auch Daten enthalten sind, die man nicht verlieren wollte. Das ist, glaube ich, unumstritten, und dass das alles andere als ein guter Zustand ist, ist, glaube ich, auch allen Beteiligten bewusst. Das ist nichts, was wir akzeptieren können, und das ist auch nichts, was uns zufriedenstellen kann.

Es ist aber jetzt nichtsdestotrotz Tatsache, und mit der müssen wir umgehen. Das ist auch das, was ich letzte Woche mit den Kolleginnen und Kollegen, hier auch insbesondere mit dem CDO, Florian Hauer, in seiner Gegenwart besprochen habe und auch mit Ihrem CISO entsprechend vor Ort. Ganz wichtig ist, zum jetzigen Zeitpunkt dafür zu sorgen, dass wir möglichst professionell, möglichst gut und konstruktiv mit dieser aktuellen Krise umgehen.

Wir gehen davon aus, dass die Krise noch einige Zeit dauern wird, einfach deshalb, weil die Daten jetzt öffentlich sind. Es ist aber nach wie vor nicht sehr leicht, sie herunterzuladen. Das heißt, es werden Stück für Stück auch mehr Informationen nach draußen gelangen, öffentlich werden, und wir gehen davon aus, dass sich dieser Prozess auch durchaus noch einen Moment hinziehen kann, bis dann alles flächendeckend bekannt ist. Wir wünschten zwar, wir könnten das überhaupt erst mal verhindern, das ist aber nicht der Fall. Die Daten sind jetzt in der Welt, und damit müssen wir auch umgehen. Bis sie aber dann entsprechend die Verbreitung finden, das wird sich jetzt noch eine ganze Weile hinziehen.

Was für uns jetzt wichtig ist, ist das, was ich gerade schon gesagt hatte: Wir müssen damit so gut wie möglich und so konstruktiv wie möglich umgehen. Das ist der entscheidende Punkt. Das heißt, es geht in erster Linie darum, die Daten bei all dem, was wir wissen, Stück für Stück auf ihre Kritikalität zu prüfen und entsprechend auch Maßnahmen vorzunehmen. Ich gebe Ihnen ein paar Beispiele, dass man es ein bisschen einordnen kann: Wenn sich Passwörter darin finden, müssen Passwörter ausgetauscht werden. Wenn sich Zertifikate darin finden, müssen Zertifikate ausgetauscht werden. Wenn Informationen über kritische Infrastrukturen dabei sind, dann geht es darum, hier entsprechende Vorkehrungen zu treffen, sei es, indem man sie besonders schützt oder sei es, indem man Pläne entsprechend ändert, die diese Liegenschaften, diese Institutionen dann auch schützen. Wir haben bis jetzt noch nichts von wirklich maximaler Kritikalität finden können, aber das ist einfach nicht auszuschließen, da sind die Analysen auch noch nicht abgeschlossen.

Der entscheidende Punkt für mich ist der, dass es uns gelingt, hierbei möglichst gut und möglichst professionell vorzugehen. Wir haben hier auch eine starke Unterstützung von Bundesseite für die Kolleginnen und Kollegen in Berlin zur Verfügung gestellt. Nach bisherigem Feedback wird das auch sehr dankbar angenommen, und es freut mich auch, dass wir da gut zusammenarbeiten. Das ist jetzt das mit Abstand Wichtigste, was wir in diesem Moment tun müssen. Ich kann es immer wieder betonen: Krise bedeutet, dass alle an einem Strang ziehen und miteinander arbeiten müssen, um da möglichst gut durchzukommen.

Für die Bundesregierung selber haben wir natürlich auch entsprechende Vorkehrungen getroffen. Das heißt, wir koordinieren uns hier auch entsprechend mit den anderen Sicherheitsbehörden und sorgen auch auf unserer Seite dafür, dass auf der Bundesseite alles getan wird, um möglichst gut durch die Krise zu kommen. Wir haben bei uns auch personelle Vorkehrungen getroffen, um hier auch über längere Zeiträume vernünftig zur Verfügung stehen zu können. Es ist mir ganz wichtig, dass auch Berlin weiß, Sie sind da nicht allein.

Zu guter Letzt würde ich noch ein paar Worte dazu sagen – ich hatte das auch in der letzten Sitzung, in der ich dabei sein durfte, erwähnt –: Lassen Sie uns versuchen, damit so konstruktiv wie möglich umzugehen. Wir haben keine Zeit und auch keine Energie, uns jetzt um Schuldige zu kümmern. Wir müssen uns darum kümmern, dass wir diejenigen stützen, die uns jetzt helfen können, um hier wirklich miteinander zu sehen, dass wir das gut meistern. Das bedeutet vor allen Dingen – das hatte ich das letzte Mal auch angegeben –, dass wir es schaffen, gut zu informieren. Das heißt, dass wir entsprechende Hilfemöglichkeiten für betroffene Bürgerinnen und Bürger, aber auch für betroffene Mitarbeitende bereitstellen, sodass die wissen, wohin sie sich wenden können, je nachdem, welche Daten abgeflossen sind. Wenn wir mit Szenarien umgehen müssen, in denen auch sehr sensitive persönliche Daten abgeflossen sind, sollten wir auch ernsthaft in Erwägung ziehen, dass wir Beratungsstellen dort aufsetzen,

an die Menschen sich wenden können, wenn sie Hilfe brauchen, zum Beispiel, wenn Angreifer persönliche Daten verwenden, um weitere Angriffe zu fahren, die dann persönlicher Natur sind, zum Beispiel mit sehr stark personalisiertem Phishing versuchen anzugreifen. Hier müssen wir sicherstellen, dass die Menschen wissen, dass sie Hilfe bekommen und dass wir es wissen, dass sie dort in Not sind und wir entsprechend auch unterstützen und helfen. Ich sage ganz bewusst wir, weil das keine Frage vom Senat Berlin oder Bezirksverwaltungen ist, auch nicht allein vom Bund, sondern das ist eine Frage von uns allen, das betrifft uns alle, das betrifft das ganze Land. Insofern haben wir auch alle unseren Beitrag dazu zu leisten, dass das möglichst gut funktioniert.

Wichtig ist mir, wirklich genau jetzt an dieser Stelle ein starkes Augenmerk darauf zu setzen, dass wir – Stück für Stück, nachdem wir die Daten auch besser analysiert haben und mehr darüber wissen – herausfinden, welche Schutzmaßnahmen für kritische Infrastrukturen, für angeschlossene Institutionen zu treffen sind. Das ist ganz wichtig, um diese Gefährdung dort kleinzuhalten. Das Nächste ist natürlich jetzt auch, das ganze Thema Ihrer IT-Absicherung voranzutreiben. Da versuchen wir, auch entsprechend zu beraten. Da weiß ich aber auch, dass Sie sich entsprechend Hilfe geholt haben. Ganz wichtig ist – hier auch wirklich die Bitte an alle – da mitzumachen! Wenn wir Passwörter brauchen, wenn wir Analysemöglichkeiten brauchen, wenn wir Sensorik brauchen, dann machen wir das garantiert nicht, um irgendwen zu ärgern, sondern es geht tatsächlich hier darum, das Thema Sicherheit jetzt schnell in den Vordergrund zu stellen, um da Schlimmeres zu verhindern.

Mir ist außerdem wichtig, dass wir auch noch einmal klar kommunizieren, dass wir uns beim Thema Wahlen in höchstem Maße engagieren und da im Moment auch keine Schwierigkeiten sehen. Das heißt, wir haben viel Erfahrung damit, die Wahlsysteme gut abzusichern, und da helfen wir auch aus Bundessicht entsprechend mit, wenn Hilfe gewünscht ist. Das ist überhaupt kein Thema. Ich weiß, dass die Kolleginnen und Kollegen dort auch im Austausch sind. Das ist auch etwas, was die Bevölkerung wissen muss, dass sich hier gekümmert wird und dass wir dort im Moment auch gut aufgestellt sind, um da wirklich höchste Sicherheit garantieren zu können. Auch das ist etwas, von dem ich mir wünsche, dass wir das klar kommunizieren und an die Menschen da draußen geben: Wir sind hier gut aufgestellt.

Was eine Weile dauern wird – das ist uns auch allen bewusst –, ist wirklich das Thema Abarbeitung der Anforderungen im Datenschutz. Das ist keine gute Situation, aber das müssen wir uns klarmachen, und dann müssen wir an dieser Stelle auch dafür sorgen, dass wir da gut durchkommen. Ich bekomme auch sehr viele Anfragen von Journalistinnen und Journalisten; es sind jetzt unter Umständen auch hier einige zugeschaltet. Mir ist bewusst, dass das Headlines sind, die sich gut verkaufen. Das verstehe ich alles. Das ist auch die Natur der Dinge. Auch das verstehe ich. Bitte verzeihen Sie, wenn ich in die Empörung nicht allzu laut einstimme. Mir ist jetzt wichtig, an dieser Stelle bei einem guten Krisenmanagement mitzuhelfen, und da lege ich im Moment meinen Schwerpunkt und den Schwerpunkt der Arbeit des BSI hin.

Uns geht es jetzt also darum, gut vorwärtszukommen, gut abzusichern, gut zu informieren und insbesondere alle notwendigen Schritte zu machen, je nachdem, welche Informationen jetzt auch Stück für Stück nach draußen kommen. – Damit würde ich es jetzt erst mal bewenden lassen und stehe Ihnen für Fragen auf jeden Fall zur Verfügung – je nachdem, wie Sie die weiteren Minuten gestalten wollen. Ich stehe Ihnen zur Verfügung und höre gerne zu!

- schu/sch -

Vorsitzender Johannes Kraft: Ganz herzlichen Dank, Frau Plattner! – Wir haben tatsächlich schon eine ganz gut gefüllte Redeliste. Mein Vorschlag wäre – wenn das für Sie, verehrte Kollegen, in Ordnung ist –, dass wir zunächst einmal die Fragen sammeln, die sich an Frau Plattner richten, weil Frau Plattner hat, glaube ich, wie viele hier im Raum, sehr viel zu tun, aber sie ist ja sozusagen heute dankenswerterweise da und Gast. Insofern, wenn Sie nichts dagegen haben, starten wir mal mit dem Fragenkomplex an Frau Plattner und würden dann anschließend an die anderen hier Anwesenden die Fragen stellen. – Ich habe jetzt Herrn Schulze und gesehen, die in Richtung Frau Plattner fragen möchten. Vor Ihnen stehen auf der Redeliste Herr Vallendar, Herr Ziller, Frau Ahmadi. Haben Sie jeweils auch Fragen an Frau Plattner? – [Zuruf] – Okay! – Dann schauen wir mal. Meine Bitte wäre, dass wir auch ein bisschen auf die wertvolle Zeit von Frau Plattner Rücksicht nehmen. Dann verfahren wir nach der Redeliste, und es beginnt Herr Vallendar. – Bitte!

Marc Vallendar (AfD): Vielen Dank, Herr Vorsitzender! – Meine Damen und Herren! Am 24. August 2026 hat der Staatssekretär in diesem Ausschuss erklärt, es seien nur öffentlich zugängliche Geodaten abgeflossen; das schließe sensible Daten logisch aus. Zwei Tage später meldete dann die Senatskanzlei weitere Datenabflüsse und vier Tage später eine Erpressung, und seit Freitag liegen 1,4 Millionen Dateien im Netz: Personalakten, Atteste, Passwörter, Notfallpläne für die Wasserversorgung, eingestufte Unterlagen zur zivilen Verteidigung. Dieser Ausschuss ist am 24. August also falsch informiert worden, vielleicht auch mangels Kenntnis zu dem Zeitpunkt. Am selben Tag hieß es aber, die ersten Unstimmigkeiten seien Ende Juli aufgetreten und die Forensiker damals schon beauftragt gewesen. Der Datenabfluss lief dann vom 7. bis zum 12. August. Das Netz wurde am 14. August getrennt. Über diese Zeit reden wir heute und nicht über die Professionalität der Täter.

Ich habe natürlich ein paar Fragen an den Senat. Wann genau hat die Senatskanzlei konkret von dem Abfluss Kenntnis erlangt? Warum dauerte es dann noch zwei Tage, bis das Netz getrennt wurde? Hatten die Fernzugänge einen zweiten Faktor? Wer hat Verschlusssachen in einem Netz abgelegt, von dem die Beamten im Februar schriftlich festhielten, dass sie es nicht schützen können? Wie viele Beschäftigte wurden denn jetzt schon konkret benachrichtigt, dass von ihnen konkrete Daten im Netz gelandet sind? – So, wie ich Sie jetzt verstanden habe, ist das bisher noch niemand. Was hat der Vorfall bis zum 31. August gekostet, und aus welchem Titel werden die Kosten getragen? – Ich will hier noch mal kurz einen Vergleich anführen: Der Märkische Kreis hat seinen Angriff von 2023 mit 2,8 Millionen Euro beziffert. Die British Library in London, die von derselben Gruppe angegriffen wurde, bezifferte diesen Angriff mit bis zu 7 Millionen Pfund. Berlin nennt bisher noch keine Zahl.

Da käme ich dann auch zu den Forderungen meiner Fraktion, was ich finde, was der Senat jetzt in den nächsten Wochen und Tagen erledigen sollte: Das eine ist, dass wir einen schriftlichen Lagebericht haben wollen, der eine Chronologie des Ganzen zusammenfasst, nach Möglichkeit bis zum 18. September, sowie einen Kostenbericht, der dann auch an den Hauptausschuss überwiesen wird. Ich halte es auch für wichtig, dass wir über die heutige Sitzung ein Wortprotokoll anfertigen. Es ist richtig, dass wir auch nach der Wahl noch eine Sondersitzung des Ausschusses bekommen sollten, denn dieses Thema wird uns weiter beschäftigen.

Ich habe auch noch ein paar weitere Punkte anzumerken: Es wäre aus meiner Sicht notwendig, dass wir auch hinsichtlich der Wahlen – das wurde schon angesprochen – eine schriftliche Bestätigung des Landeswahlleiters erhalten, dass das Wählerverzeichnis, die

Wahlscheinverfahren und die Adressprüfung, insbesondere durch das qualifizierte Straßennetz, integritätsgeprüft sind. Weiterhin bräuchten wir in Bezugnahme auf den Geheimschutz eine landesweite Prüfung, wo eigentlich die Verschlusssachen digital abgelegt sind; in dem Bereich muss dann auch eine Sperrung erfolgen. Wir bräuchten auch eine unabhängige Ursachenanalyse vom BSI und dem Rechnungshof, die dann noch zusätzlich in einem Bericht veröffentlicht wird, denn aus unserer Sicht sollte sich die Senatskanzlei nicht selber prüfen.

Ich möchte noch ein paar Fragen stellen. In den veröffentlichten Daten liegen – nach dem, was bisher in der Presse vorhanden ist – zum Beispiel Atteste, PCR-Testergebnisse, Impfkorrespondenz und Schwerbehindertenausweise vor. Die waren ja dann wohl auf den Dateiservern der Verwaltung, und da frage ich mich natürlich: Welche Löschfristen gelten denn für solche personenbezogenen Daten, und wurden die überhaupt eingehalten? Wenn sie nicht eingehalten wurden, woran liegt das? Warum sind so viele Dateien auf den Servern der Verwaltung, die eigentlich gelöscht werden müssten?

Ich hätte noch die Frage nach der groben Fahrlässigkeit: Es ist angesprochen worden, dass die Täter ja nun nicht von alleine ins Netz gekommen sind, sondern möglicherweise sozusagen durch Fahrlässigkeit ins Netz gelangen konnten. Da stellt sich natürlich zum einen die Frage nach den Kriminellen, die das Haus ausräumen, aber natürlich auch nach denjenigen, die die Tür offen lassen: Gibt es eigentlich Ermittlungsverfahren interner Natur, sowohl bezogen auf den armen Mitarbeiter, der dort möglicherweise einen Fehler begangen hat, aber auch intern in der Struktur? – Für die Fehler, die jetzt dazu geführt haben, dass diese Sicherheitslücken bestehen, gibt es natürlich auch auf Leitungsebene eine Verantwortung. Da stellt sich mir die Frage, ob es auch interne Ermittlungen disziplinarrechtlicher oder auch strafrechtlicher Natur gibt und wie da der Stand der Dinge ist. Oder wird im Moment nur vom LKA gegen dieses Hackerkollektiv ermittelt? – Das sollten erst mal meine ersten Fragen gewesen sein; eventuell stellen sich noch weitere Fragen.

Eines steht fest: Ich halte diesen ganzen Vorfall für gravierend. Der wird uns auch noch in der nächsten Legislatur beschäftigen. Die CDU hatte sich auf die Fahnen geschrieben, dass die Digitalisierung und eine funktionierende Verwaltung Berlins größter Auftrag sind. Aus meiner Sicht hat das Projekt jetzt kurz vor Ende der Legislaturperiode einen Kapitalschaden erlitten, denn dieser Schaden beim Datenabfluss und auch die möglicherweise fehlenden Schutzfunktionen des Landes Berlin in dem Zusammenhang zeichnen natürlich kein gutes Bild vom Land Berlin in Bezug auf die Sicherheit seiner Daten, die Daten seiner Bürger und auch seiner Beamten. Wir werden uns wahrscheinlich auch in der nächsten Legislatur noch im Rahmen eines Untersuchungsausschusses mit diesem Thema weiter beschäftigen müssen. – Das wäre es erst einmal von meiner Seite. Vielen herzlichen Dank!

Vorsitzender Johannes Kraft: Vielen Dank! – Dann hat jetzt der Kollege Ziller das Wort.

Stefan Ziller (GRÜNE): Vielen Dank für die umfassende Darstellung! – Ehrlicherweise fand ich jetzt das, was Sie heute gesagt haben, noch erschreckender als das, was in den letzten Sitzungen gesagt wurde. Ich will mal nachfragen oder die Informationen sozusagen noch mal zusammenstellen. – Das eine ist: Sie können bis heute nicht verlässlich den Angriffsvektor nachvollziehen, weil das LKA Ihnen den Laptop weggenommen hat und Sie deswegen die Phishingvariante nicht bestätigen können? Das heißt, Sie gehen aktuell davon aus, dass es auch noch einen anderen Weg geben könnte oder das Phishing nur vorgetäuscht ist und es ein

anderer Angriffsvektor ist? – Mit anderen Worten: Sie können nicht reproduzieren, wie der Angriff passiert ist; Sie können also auch nicht ausschließen, dass es in den nächsten Tagen oder Wochen noch mal passiert, und zwar, weil das LKA Ihnen den Rechner wegnimmt. Vielleicht können Sie dazu – auch aus BSI-Sicht – noch mal etwas sagen, ob das ein angemessenes Verfahren ist oder ob es nicht aus dem Gesamtinteresse heraus nötig wäre, zuerst den Angriffsvektor zu klären und das im Zweifel mit dem LKA oder dem BKA zusammen zu machen, weil das ja der erste Schritt ist, um das Netz wieder sicher zu machen. Wenn das durch Kompetenzgerangel unterbunden wird, dann finde ich das schwierig.

Aber wenn es so ist, dann wäre die zweite Frage: Wo sind die Daten genau abgeflossen? – Ich habe jetzt gelernt, dass die Logs gelöscht wurden. Es wird Ihnen also möglicherweise gar nicht gelingen, aus eigener Kenntnis herauszufinden, welche Daten abgeflossen sind, sondern nur aus dem, was die Kriminellen ins Netz stellen. Es ist gut, wenn man die Seite scannt, aber das heißt, dass wir zumindest in absehbarer Zeit gar keine Sicherheit darüber haben werden, ob da nicht vielleicht doch vertraulichere Sachen, die nicht veröffentlicht wurden, doch abgeflossen sind. Deswegen ist die Frage: Gibt es Dateien, die jetzt aufgetaucht sind außerhalb des Domainverbundes, der betroffen ist von den beiden Verwaltungen? Ist das sozusagen vielleicht nur eine Auswahl? Gibt es sozusagen Abflüsse in den veröffentlichten Dateien, die außerhalb sind? – Dann müsste man davon ausgehen, dass theoretisch alles weg sein kann.

Die zweite Frage: Befinden sich unter den veröffentlichten Daten nach heutigem Stand auch Daten aus Fachverfahren oder sozusagen nur Dateien von Fileservern, also Dateien, die da irgendwie abgelegt wurden? – Sekundärangriffe sind nicht auszuschließen, weil die Passwörter für die Fachverfahren da offengelegen haben. Die würde ich mal weglassen. Da wäre die Frage: Sind alle Fachverfahren, deren Passwörter jetzt öffentlich sind, technisch so ausgerüstet, dass sie logfähig sind, oder gibt es Fachverfahren, die gar nicht mitloggen, wer Zugriff hat, wo wir also auch nicht feststellen können, ob da abgegriffen wird?

Dann eine hoffentlich einfache Frage: Ist inzwischen geklärt, dass die gesamte Berliner IT kritische Infrastruktur ist, oder gibt es da noch Zweifel? – Richtung ITDZ würde ich nachher fragen.

Eine Frage – vielleicht auch in Richtung BSI – zu dieser Passwortdatei: Es ist ja leider menschlich, dass Leute Umgehungstatbestände machen, dass Mitarbeitende das einfach anlegen, ob das früher auf Zetteln war, mit Aufklebern oder jetzt mit diesen Dateien. Gibt es vom BSI eine Empfehlung, was Berlin jetzt machen sollte? – Meine These ist, dass die veröffentlichten Dateien nicht die einzigen im Landesnetz sind, die existieren; es wird weitere geben. Es wird auch Beschäftigte geben, die auch nach dem Vorfall sagen: Ist mir doch egal, ich behalte diese Datei weiter! – Was würden Sie dem Land empfehlen, um das Risiko zu minimieren, dass diese Daten abgegriffen werden?

Ich habe auch noch eine Frage zu den neuen Passwortregeln: Wir haben vermeintliche 12 000 IT-Systeme. Sind die alle in der Lage, die neuen Passwortregeln auch serverseitig einzuführen, oder gibt es Fachverfahren, die gar nicht in der Lage sind, die neuen Passwortregeln vorzuschreiben? – sprich, kann das dazu führen, dass Leute einfach trotzdem ihre Sonnenscheinpasswörter weiter benutzen, weil es gar keine Überprüfungsmöglichkeit gibt, ob die Leute die ändern, weil Sie ja nicht alle Passwörter im Klartext auslesen können? – Die Fragen richten sich vor allem und an erster Stelle auch an das BSI.

- schu/sch -

Vorsitzender Johannes Kraft: Vielen Dank! – Dann ist Frau Ahmadi die Nächste. – Bitte schön!

Gollaleh Ahmadi (GRÜNE): Auch von mir vielen Dank für die ausführlichen Darstellungen heute, und natürlich auch einen Riesendank an die ganzen Mitarbeiterinnen und Mitarbeiter, die gerade seit Wochen daran sitzen und versuchen, das Schlimmste zu verhindern und vor allem an Informationen zu kommen, die wir noch nicht haben! – Ich habe ein paar ganz konkrete Fragen in Richtung BSI, aber vielleicht können Sie das auch vom Senat einmal sagen: Erfüllt das Berliner Landesnetz die Anforderungen der Berliner Cybersicherheitsstrategie, die sich der Berliner Senat vor dem Vorfall selbst gegeben hat?

Sie haben gerade eben – aber auch heute Morgen im Innenausschuss – mehrfach betont, dass keine Daten, die für die nationale Sicherheit relevant wären, abgeflossen sind – Stand heute, also bis zur jetzigen Erkenntnis. Das heißt aber im Umkehrschluss: Sie können es auch nicht ausschließen. Ich betone, glaube ich, in jedem Ausschuss, in dem wir darüber sprechen, dass wir in zwei Wochen Wahlen in Berlin haben und Berlin die Bundeshauptstadt ist und eigentlich das gesamte Land Berlin die kritische Infrastruktur der Republik ist. Es ist eigentlich erschreckend, dass wir das gerade nicht ausschließen können, aber irgendwie damit leben müssen, dass da Informationen geflossen sind. Wir haben von Notfallplänen gehört. Wir haben von Informationen zur kritischen Infrastruktur gehört. Ich möchte hier auch einmal erwähnen, dass ich das ziemlich befremdlich finde, dass von der Innenverwaltung heute niemand dazu Stellung genommen und Fragen beantwortet hat, weder im Innenausschuss noch jetzt hier. Wir sprechen über sensible Daten, die abgeflossen sind. Wir sprechen über Datenschutzfragen von Bürgerinnen und Bürgern in Berlin, und es ist auch niemand von der Innenverwaltung da, der zum Thema Datenschutz, für den sie auch zuständig sind, heute Fragen beantworten kann.

Jetzt komme ich zu weiteren Fragen: Welche verbindlichen landesweiten Mindeststandards gelten derzeit für die IT-Sicherheit aller Berliner Behörden und Einrichtungen? Wie wird kontrolliert, ob diese Standards täglich eingehalten werden? Welche Behörden oder Einrichtungen erfüllen derzeit noch nicht vollständig die verbindlichen IT-Sicherheitsstandards des Landes? Welcher Nachholbedarf besteht hier? – Zudem würde ich gern wissen, welche Konsequenzen sich aus dem aktuellen Cyberangriff für die besonderen IT-Sicherheitsstandards und die landesweite Sicherheitsarchitektur sowie für die Berliner Cybersicherheitsstrategie, die Sie sich vor einem Jahr selbst im Kabinett gegeben haben, ergeben. Wurde die Berliner Beauftragte für Datenschutz und Informationsfreiheit bei der Darstellung des Wiederaufbauplans und der zusätzlichen Schutzmaßnahmen verbindlich eingebunden? – Sie haben ja vorhin schon etwas erzählt, dass Sie da eingebunden sind; das richtet sich jetzt also gerade auch auf die Zukunft: Wie wird das Ganze dann in Zukunft im Wiederaufbauplan eingebunden sein? Erfüllt das Berliner Landesnetz die selbstgesetzten Anforderungen von Ende Juli? – Hier geht es ganz konkret nicht um die Cybersicherheitsstrategie, die Sie sich vor einem Jahr gegeben haben, sondern ganz konkret die Anforderungen, die Ende Juli gegeben wurden. – Soweit erst mal von mir.

Vorsitzender Johannes Kraft: Vielen Dank! – Dann hat jetzt Kollege Schulze das Wort. – Bitte schön!

Tobias Schulze (LINKE): Danke schön auch von meiner Seite! – Ich möchte eine Vorbemerkung machen: Ich finde, dass wir an der einen oder anderen Stelle manchmal noch nicht so sprechen, dass wir die Dimension dieses Vorfalls in allen Größenordnungen abbilden. Es sind Daten von Mitarbeiterinnen und Mitarbeitern betroffen; das wissen wir mittlerweile. Es sind Daten von Bürgerinnen und Bürgern betroffen; das wissen wir auch. Es handelt sich aber eben auch um sensibelste Daten von kritischer Infrastruktur, mit denen schlimme Dinge angestellt werden können, wenn sie in die falschen Hände kommen. Es handelt sich um Kriseneinsatzpläne anderer Bundesländer. Es handelt sich um Schließpläne von sicherheitskritischen Gebäuden. Es handelt sich um Baupläne eines Gefängnisses. Wenn man sich das mal ausmalt, was da mit diesen Dingen passieren kann und in welche Richtung das gehen kann, dann, glaube ich, müssen wir aus meiner Sicht an dieser Stelle noch mal in einen anderen Krisenmodus kommen. Das ist jetzt kein Vorwurf gegen irgendjemanden persönlich, sondern es geht hier um das Mindset, mit dem wir an diesen Vorfall herangehen.

Ich will auch noch sagen, dass der Senat aus meiner Sicht – das wurde schon gesagt – alle Ressourcen darauf konzentrieren muss, die Folgen dieses Vorfalls jetzt zu minimieren, also wirklich alle Ressourcen. Es ist ein IT-Vorfall, wie wir ihn in diesem Ausmaß in der Bundesrepublik – zumindest nach meiner Erinnerung – in den letzten Jahren nicht hatten und wo einfach Dinge betroffen sind, die gesellschaftliche Schäden nach sich ziehen können, die wir uns heute noch gar nicht vorstellen können. Ich glaube, deswegen ist es so wichtig, dass wir jetzt ins Tun kommen – was Finanzen angeht, aber auch was organisatorische Ressourcen angeht.

Ich habe den Senat auch in der Presse aufgefordert, die Großschadenslage auszurufen. Vielleicht können Sie dazu noch mal etwas sagen, ob das noch ansteht. Der Landkreis Anhalt hat damals sogar den Katastrophenfall ausgerufen, und es wäre ja auch hier die Möglichkeit, über die Großschadenslage noch mal anders zu handeln, auch Amtshilfe in Anspruch zu nehmen, um beispielsweise auch gegenüber den Bezirken handlungsfähig zu sein. Vielleicht können Sie auch noch mal etwas dazu sagen, wie die Lage mit den Bezirken ist: Kooperieren jetzt alle nachgeordneten Behörden mit Ihnen? – Wir konnten in der Presse lesen, dass der Bezirk Lichtenberg wegen CrowdStrike keinen Zugriff auf seine Daten gibt, weil er nicht möchte, dass CrowdStrike auf seinen Servern läuft. Vielleicht können Sie noch mal sagen, ob alle Verwaltungen in Berlin bei der Aufklärung dieses Vorfalls kooperationsbereit sind.

An Frau Plattner habe ich die folgende Frage: Das BSI hat am Freitag einen Angriffsvektor veröffentlicht, TerminalFix. Ist das der richtige, den Sie konkret auf den Berliner Vorfall beziehen? – Vielleicht können Sie auch noch mal etwas dazu sagen, was Ihre Erkenntnisse sind: Wenn das der Angriffsvektor war, warum sind die Angreifer so tief in die Systeme reingekommen? – Da stelle ich auch die Frage an den Senat: Phishing-Mails waren schon ein Thema hier. Es passiert ja tausendfach am Tag, dass Mitarbeitende Phishing-Mails bekommen. Dann hat eine Mitarbeiterin, ein Mitarbeiter auf den Link geklickt, und dann hatten die Angreifer wochenlang Zeit, tief in dieses Thema einzudringen. Es war zwar nur ein Prozent der Daten, die abgeflossen sind, wie wir jetzt gehört haben, aber trotzdem hatten sie offenbar die Möglichkeit, in Systeme vorzudringen, in deren Nähe sie nicht einmal hätten kommen dürfen. Da wäre meine Frage: An welcher Stelle fehlten da die Brandmauern, um ein derzeit viel zitiertes Wort zu nutzen? An welcher Stelle hätte eine Sicherheitssperre greifen müssen?

Eine nächste Frage ist die nach den Betroffenen: Von Verwaltungsmitarbeitenden haben wir schon gehört. Dass die in großer Zahl betroffen sind, ist klar. Können Sie aber schon ungefähr abschätzen, wie viele Bürgerinnen und Bürger Berlins betroffen sind oder ob überhaupt Bürgerinnen und Bürger Berlins in größerer Zahl betroffen sind? – Vielleicht können Sie dazu mal etwas sagen, um welche Daten es da geht.

Dann hätte ich die Frage, ob der Senat eine Sicherungskopie der Daten gezogen hat, die im Netz stehen, denn es kann durchaus sein, dass die Gruppe weitere Spielchen mit den Daten spielt, sie auch wieder herausnimmt oder ähnliche Dinge. Sie haben gesagt, es dauert eine Weile, ehe die Daten überhaupt alle heruntergeladen werden können. Vielleicht können Sie sagen, wie Sie an der Stelle Beweismaterial sichern.

Zur Frage der Verschlüsselung frage ich noch mal Frau Plattner vom BSI: Sie haben gesagt, dass Sie froh sind, dass nichts verschlüsselt wurde. Das hat Herr Hauer auch gesagt. Lag das daran, dass so schnell reagiert wurde, oder lag das daran, dass das Ziel der Angreifergruppe gar nicht die Verschlüsselung der Server war? Gibt es dazu Erkenntnisse? – In der Regel ist die Gruppe ja dafür bekannt, dass sie irgendwann verschlüsselt. Vielleicht können Sie noch mal sagen, ob das hier in diesem Fall anders war und ob Sie hier anders vorgegangen sind.

Eine vorletzte Frage von meiner Seite betrifft das Thema Finanzierung: Im Innenausschuss hat Staatssekretär Hauer heute Morgen gesagt, dass für den Schutz der Daten und im Rahmen der Haushaltsverhandlungen für sicherheitsrelevante IT-Anwendungen und überhaupt für die Modernisierung unserer IT mehr Geld zur Verfügung gestellt werden muss. Das wussten wir auch schon in den laufenden Haushaltsberatungen. Die Stadtentwicklungsverwaltung hat auch in diesem Ausschuss in den Haushaltsberatungen ausgesagt, dass sie den Ersatz von Netzwerkkomponenten aufgrund von finanziellen Kürzungen aussetzen musste. Deswegen stelle ich hier auch noch mal meine Frage, auch an den CDO, ob bekannt ist, ob sich durch die Haushaltskürzungen im IT-Bereich betroffener Verwaltungen sicherheitsrelevante Modernisierungen verzögert haben oder ob Verwaltungen bei Ihnen angezeigt haben, dass sie Dinge aufgrund von Geldmangel nicht tun können, die sicherheitsrelevant sind. Vielleicht können Sie dazu auch noch mal etwas sagen, denn das spielt natürlich auch eine Rolle für die kommende Legislaturperiode, Stichwort Nachtragshaushalt. Da muss möglicherweise Geld reingeschossen werden, das in der Vergangenheit, in den letzten drei Jahren, aufgrund von Kürzungen nicht investiert worden ist.

Dann ist die Frage, auch von meiner Seite: Der Senat hat ja die Betroffenen aufgefordert, Anzeigen zu stellen. Haben Sie Kenntnis darüber, ob das schon passiert ist, und wenn ja, wie viele Anzeigen sind gestellt? – Ich hätte noch die Frage, ob Geld für den Schutz betroffener Bürgerinnen und Bürger eingestellt worden ist. Die Frage ist so ähnlich schon gestellt worden. Das eine ist, Passwörter zu ändern und entsprechende Softwarekomponenten abzuschotten, aber was ist eigentlich mit Schadensersatz? Wer haftet eigentlich dafür, wenn mit den erbeuteten Daten Schaden angerichtet wird, entweder bei den Betroffenen selbst oder an anderer Stelle? Steht das Land Berlin dann in der Haftung, oder steht jemand anderes in Haftung, und wenn das Land Berlin in Haftung steht, hat das Land Berlin dafür Vorsorge getroffen? – Danke schön!

Vorsitzender Johannes Kraft: Vielen Dank! – Dann Herr Dr. Kollatz, bitte!

Dr. Matthias Kollatz (SPD): Danke schön, Herr Vorsitzender! – Ich hatte beim letzten Mal schon gesagt, dass wir, wenn nicht heute ein abschließender Bericht kommen kann, auf außerordentliche Ausschusssitzungen zulaufen. Ich glaube, das ist offensichtlich. Das hat Herr Hauer einleitend auch gesagt. Wir sind nicht in der Situation, dass wir zum gegenwärtigen Zeitpunkt irgendetwas abschließen können. Also, bitte, richten Sie sich, richten wir uns alle auf Sondersitzungen ein. Es spricht vieles dafür, dass das Sinn macht.

Was ich ausdrücklich richtig finde, ist es, einen Fokus auf die Einbrecher und einen zweiten Fokus auf das Aufräumen zu legen. Das gerät bei einem Teil der Beiträge, die hier gerade gekommen sind, vielleicht ein bisschen in den Hintergrund, aber es spricht vieles dafür, dass das die richtigen Fokuspunkte sind, und da danke ich denen, die vorgetragen haben, dass sie das so gesagt haben.

Ich möchte mich ein bisschen an der Liste von Frau Plattner entlanghangeln: Passwörter und Zertifikate ändern kann man natürlich machen, ohne einen Beweis zu haben, dass die Passwörter und Zertifikate geklaut worden sind. Das heißt also, es ist offenkundig, dass da ein Schwachpunkt besteht, und das heißt, das kann und sollte insgesamt komplett geändert werden. Das kostet übrigens nicht so viel Geld. Deswegen habe ich dazu die Frage: Wann hat das begonnen, und wann wird das enden können?

Damit komme ich dann zum nächsten Punkt. Eine Zeitung berichtet, dass ein Bezirk gestern entschieden hat, Sie von der Landesseite und damit auch Sie vom BSI nicht auf seine IT zu lassen – Bürgermeister CDU, IT-Stadträtin Linkspartei –, und dort wurde gesagt: Die eigenen Leute haben sich das alles angeschaut, und es gibt kein Problem. Deswegen jetzt die Frage: Sind dort die Passwörter und Zertifikate alle geändert? Haben Sie darüber eine Gewissheit, oder, besser, haben Sie mittlerweile Zugang zu diesem System, obwohl das Gegenteil in der Zeitung stand? – Nicht alles, was in den Zeitungen steht, ist richtig. Gerüchteweise gab es fünf Bezirke, die Bedenken hatten, an dieser zentralen Aufräumaktion mitzuwirken, und da ist deswegen die Frage: Wie ist da der Stand?

Zu den Wahlsystemen hat Frau Plattner vom BSI gesagt, dass Sie da auch unterstützen können. Bedeutet das, dass seitens des BSI dafür Zugriffe auf die Systeme erforderlich sind, weil Sie natürlich auch mehr Angriffsmechanismen kennen als vielleicht wir in Berlin? – Das würde mich noch interessieren.

Der nächste Punkt ist das Thema Pläne. Dazu hatte Herr Schulze schon etwas gesagt. Es ist wichtig, sich das anzugucken, und da wollte ich um Transparenz bitten. Wenn das Angucken im Rahmen der Aufräumarbeiten ergibt, dass dort etwas zu ändern ist, ist es wichtig, dass wir hier in diesem Ausschuss davon erfahren. Der Ansatz mit den Beratungsdiensten ist richtig. Ich will das jetzt gar nicht groß kommentieren, würde aber vorschlagen – das kann auch in einer anonymisierten Form geschehen –, dass darüber auch in den zukünftigen Berichten berichtet wird, was dort geschieht, also über die Tätigkeiten, damit auch die Öffentlichkeit und wir im Ausschuss einen gewissen Überblick haben, was dort die Themen angeht. Es ist – nur, um ein Beispiel zu nennen – schon wichtig zu erfahren, auch hier im Ausschuss, ob es zum Beispiel individualisierte Erpressungsversuche gibt und so weiter. Deswegen bitte ich, das in Zukunft in die Berichte aufzunehmen. – Danke!

Vorsitzender Johannes Kraft: Vielen Dank, Herr Dr. Kollatz! – Bevor wir zur Beantwortung kommen, wurde angeregt, ein Wortprotokoll von diesem Tagesordnungspunkt anzufertigen. Gibt es da Widerspruch? – Das kann ich nicht erkennen. Dann herzlichen Glückwunsch, liebes Ausschussbüro! – Wir würden, wie besprochen, mit Frau Plattner beginnen. – Frau Plattner, Sie haben das Wort! Bitte!

Claudia Plattner (BSI): Wunderbar! Ich versuche gerne, etwas dazu zu sagen. Sie werden mir verzeihen müssen, dass ich nicht zu allen Punkten Stellung beziehen kann, denn das sind teilweise Interna, zu denen ich die Informationen gar nicht habe – und selbst wenn ich sie hätte, wäre ich auch nicht in der Rolle, sie ausplaudern zu können. Ich würde aber auf jeden Fall zu ein paar Punkten etwas sagen wollen. Es wurde am Anfang von Herrn Vallendar – ich hoffe, ich habe es richtig ausgesprochen, man möge mir verzeihen – die Chronologie aufgearbeitet, und insbesondere wurde auch gezeigt, dass Stück für Stück mehr Informationen nach draußen gekommen sind und damit dann bekannt wurden, auch Ihnen bekannt wurden. Ich kann das nicht anders betiteln, als dass es das Wesen einer Krise ist. Es ist nicht so, dass man von Anfang an immer grundsätzlich weiß, was denn das genaue Schadensausmaß ist. Das dauert. Da wird Forensik gemacht. Da werden Logfiles ausgewertet. Da wird geprüft, was vorhanden ist. Das ist erst mal nichts Ungewöhnliches. Ich weiß, dass das unangenehm ist. Ich kann das auch alles hundertprozentig verstehen. Ich habe das einfach nur schon sehr oft gemacht. Demzufolge kann ich an dieser Stelle sagen: Es ist das Wesen einer Krise, dass Dinge Stück für Stück ans Licht kommen, so unangenehm das auch sein mag. Es ist nicht so, dass man am Anfang immer schon genau weiß: Wie groß ist das Ausmaß? Was ist alles passiert? Wo haben die Täter angegriffen? Was werden die Folgen sein? – Das ist ein Stück weit genau das Wesen, dass man das nach und nach erst überreißt und dann auch entsprechend kommuniziert. Ich glaube, wir sind gut beraten, nicht von vornherein immer das Schlimmste anzunehmen, sondern darauf zu warten, dass Profis an dieser Stelle eine verlässliche Information geben können. Darauf dränge ich grundsätzlich, auch wenn es um den Bund geht, wo wir noch mal eine originäre Zuständigkeit haben: Die Menschen brauchen Zeit, um das vernünftig auswerten zu können. Insofern bitte ich um Verständnis, so unangenehm das auch sein mag.

Es wurden viele Sachen gefragt, die ich Ihnen nicht gut beantworten kann. Deswegen werde ich es lieber auch nicht versuchen. Ich kann aber zumindest Herrn Ziller ein paar Dinge beantworten. Zum Thema Angriffsvektoren, dass die nicht bekannt seien: Doch, wir haben eine ziemlich gute Vorstellung davon, was dort passiert ist. Wir sind da doch relativ sicher, dass wir da einen guten Überblick haben und auch weitere Vektoren ausschließen können, insbesondere durch die Detektionsmechanismen, die überall hochgefahren werden sollten. Ich weiß, hier wurden auch Ausnahmen genannt. Da habe ich leider nicht den allerneuesten Stand, wie das da jetzt aussieht, aber ich bin sicher, das wissen die Kollegen aus Berlin.

Sind auch Daten aus Fachverfahren abgeflossen? – Auf BSI-Seite haben wir dazu keine Informationen, die sagen würden, dass es so ist. Stand jetzt sehen wir das nicht. Wie ist hier die Mechanik dessen, was wir jetzt Stück für Stück tun? – Wir gucken uns die Indexdateien an und schauen jeweils, was da drin ist, und laden dann gezielt nach. Das machen wir gerade auch aus Bundessicht mit Betroffenen, das heißt, jeder, der sagt, das könnte auch etwas sein, was uns an der Stelle betrifft, kann sich aus dem Bund an uns wenden. Dann wird das entsprechend nachgeladen, um zu schauen: Wo gibt es Betroffenheiten, in die man noch mal tiefer reinschauen muss?

Warum machen wir das so? – Weil – das greift ein bisschen der Antwort auf eine spätere Frage vor – es nicht so ist, als könnte man auf einen Knopf drücken, dann kann man 5,7 Terabyte herunterladen und dann hat man sie eine Stunde später da. Tatsächlich ist die Datenbandbreite, die zur Verfügung steht, außerordentlich klein, was der Tatsache geschuldet ist, dass die Server, von denen man das herunterladen kann, natürlich gut versteckt sind. Es ist nicht so, als könnten wir sie bei Microsoft oder Amazon oder bei einer deutschen oder europäischen Firma einfach so herunterladen. Die stehen nicht einfach frei im Netz. Die stehen an Stellen, an denen sie gut versteckt sind. Das bedeutet auch, dass man dorthin eine sehr dünne Leitung hat, was wiederum bedeutet, dass es gerade jetzt, wo sehr viele versuchen, die Daten herunterzuladen, einige Zeit dauert. Das heißt, man muss selektiv vorgehen und schauen: Was sind Inhaltsverzeichnisse? Was ist da drin? Wo muss man gezielt noch mal reinschauen? Wo könnten entsprechende Betroffenheiten sein? – Genauso gehen wir auch vor, im Bund und meinem Verständnis nach auch in Berlin, und ich glaube, das ist vom Vorgehen her das Beste, was wir im Moment tun können. Ich sage es noch mal: Wichtig ist vor allen Dingen, dass wir die sicherheitskritischen Sachen zuerst analysieren, und das wird auch nur mithilfe derjenigen gehen, die im Zweifelsfall direkt betroffen sind, und deswegen ist dieses Vorgehen auch so gewählt. Zur Frage, ob mehr Daten abgeflossen sind als aktuell bekannt: Das ist theoretisch denkbar. Mein Verständnis ist aber, dass die Obergrenzen durchaus ganz gut erfasst sind, und insofern gehen wir im Moment davon auch nicht aus.

Sind ganz Berlin und die gesamte Berliner IT eine kritische Infrastruktur? – Zunächst einmal liegt das im Bereich der Länder, das heißt, nicht im Bereich des Bundes und der kritischen Infrastrukturen dort. Nichtsdestotrotz gibt es entsprechend dort die Zusammenarbeitsthemen, und das wird jetzt an dieser Stelle auch zusammen behandelt.

Zu den Passwörtern wurde ich gefragt, ob wir eine Empfehlung haben. Die wichtigste Empfehlung, die wir haben, ist, mindestens einen Passwort-Safe zu verwenden. Das entlasten Ihre Mitarbeitenden davon, sich Passwörter merken zu müssen, was es deutlich leichter macht, sehr viele verschiedene und auch komplizierte Passwörter zu vergeben, was jetzt Pflicht ist. Insofern sind Passwort-Safes eine Best Practice, um überhaupt erst mal den ersten Schmerz zu lindern. Noch professioneller geht es dann natürlich mit Passkeys, wenn man moderne Infrastrukturen aufsetzt. Wir müssen aber auch ganz klar sagen: Es ist nicht so, als wäre das in allen Behörden Deutschlands, in allen anderen Bundesländern, in Kommunen, im Bund und auch in den Firmen überall schon ganz weit verbreitet, sodass man sagen kann, Berlin wäre hier unglaublich weit hintendran. Das ist nicht so. Wir haben keine starke Durchdringung mit Passkeys in den Institutionen und Organisationen in Deutschland – jedenfalls noch nicht, und wir dringen darauf, dass man entsprechend aufrüstet. Das halten wir für dringend geboten. Das gilt aber für alle.

Zu den Fragen von Frau Ahmadi: Ich schaue mal, was ich davon beantworten kann. Bei der Frage, ob alle Anforderungen des Berliner Senats erfüllt sind, kann ich natürlich nicht helfen. Kommen unter Umständen noch Daten zur nationalen Sicherheit, die unter Umständen dann den Bund und damit auch uns ganz originär betreffen? – Ich kann Ihnen versichern, dass wir mit Hochdruck daran arbeiten. Wir arbeiten mit Hochdruck auch mit den anderen Bundesbehörden daran. Das läuft bei uns im Cyberabwehrzentrum entsprechend zusammen. Dort wird die Arbeit koordiniert. Insofern ist das, was auch immer dort an Informationen gefunden wird, sofort an der richtigen Stelle, um sicherzustellen, dass das auch entsprechend behandelt wird. Das kann ich an der Stelle dazu sagen.

Zu Herrn Schulze und zum Thema Mindset: Das richtige Mindset an dieser Stelle ist, glaube ich, unerlässlich. Wir sind uns alle einig, dass das ein absolut gravierender Vorfall ist. Aus der Rolle des Krisenmanagements, die wir als BSI jetzt ein Stück weit miterfüllen und die sicherlich auch andere Kolleginnen und Kollegen aus Berlin miterfüllen, ist es das Wichtigste, dass wir ruhig sind und damit sehr konstruktiv umgehen. Das Schlimmste, was wir uns vorstellen können, ist ein hektischer Krisenmanager oder eine hektische Krisenmanagerin. Insofern ist es bei den Menschen, die wir in die Krisenstäbe geschickt haben, ganz wichtig, dass das Leute sind, die diese Aufgabe kennen, die diese Aufgabe verstehen und genau das und auch die entsprechende Erfahrung mitbringen, um hier – ganz egal, wie groß das Problem im Moment ist, und das ist groß, da sind wir uns alle einig – mit Ruhe und Professionalität an die Dinge heranzugehen.

Die Fragen zu dem Angriffsvektor kann ich so beantworten, dass das, was wir veröffentlicht haben, den Angriffsvektor mit dem Datum dann auch beschreibt. Das haben wir genau aus diesem Grund gemacht. Ich kann Ihnen versichern: In dem Moment, in dem bekannt wird, was wo passiert ist – und das betrifft nicht alleine Berlin, sondern ganz Deutschland –, geht eine Maschinerie los. Hier werden in einem CERT-Verbund von den Ländern, mit dem Bund, mit allen Beteiligten, teilweise auch mit weiterführenden Strukturen, auch Industriebeteiligung, sogenannte Indicators of Compromise geteilt, das heißt, hier wird sofort geguckt: Okay, woran kann man erkennen, dass der Angreifer sich unter Umständen im System befindet oder versucht anzugreifen? –, und das geht dann wirklich nach draußen. Diese Maschinerie läuft in dem Moment an, sodass alle anderen Bundesländer, Kommunen et cetera pp. in der Lage sind, auch bei sich auf Betroffenheit zu prüfen. Das ist immer so, und das ist auch die Art und Weise der Zusammenarbeit, und die funktioniert auch ganz hervorragend. Insofern kann ich an der Stelle sagen, dass das dann auch entsprechend verbreitet wurde.

Zum Thema Brandmauern hatten Sie gefragt: Wie kann es sein, dass man über einen Angriffsvektor dann doch relativ weit kommt? – Das ist das klassische Angriffsszenario, ein Angreifer verschafft sich Zugang. Wir dürfen auch nie vergessen: Das sind die Kriminellen hier. Die haben sich an dieser Stelle illegal Zugriff verschafft, und in dem Moment, in dem sie das geschafft haben, geht ein sogenanntes Lateral Movement, eine laterale Bewegung, eine Seitwärtsbewegung im Netzwerk weiter. Man schaut, wo man überall reinkommt und versucht mit weiteren Maßnahmen, sich noch erweiterte Rechte zu verschaffen. Das ist ein übliches Vorgehen. An dieser Stelle hat man es geschafft, an relativ viele Daten heranzukommen. Brandmauern an solchen Stellen – wie Netzwerksegmentierung, sehr strenges Identity- und Access-Management – sind normalerweise die Dinge, die dort helfen. Wir sehen auch hier, dass das in vielen Organisationen noch nicht auf dem Niveau ist, wie wir es brauchen. Wir müssen dort hin zu echten Zero-Trust-Architekturen, und auch das gilt für ganz Deutschland. Insofern hatten die Angreifer es hier immer noch zu leicht, und es ist ganz klar, dass die Größe der abgeflossenen Daten dafür auch Bände spricht. Hier sind in der Tat andere und mehr Schutzmechanismen aufzuziehen, und das gilt nicht nur für Berlin, sondern auch für viele andere Organisationen in der Industrie, aber auch im öffentlichen Sektor.

Die Downloads dauern relativ lange. Das hatte ich schon mal gesagt. Deswegen gehen wir davon aus, dass es noch einige Zeit dauern wird, einige Wochen, bis wir alle Daten dann auch wirklich gesichtet haben können, uns zwar von allen, die da draufschauen müssen.

- schu/ur -

Zum Thema Verschlüsselung: Es war in der Tat dem beherzten Handeln der Kolleginnen und Kollegen zu verdanken, dass es dazu nicht kommen ist. Jetzt kann man immer sagen, noch besser wäre gewesen, wenn man sofort gemerkt hätte, dass ein Angreifer im System ist, überhaupt keine Frage, aber zumindest ist es gelungen, es zu bemerken, bevor es zu einer Verschlüsselung gekommen ist. Dadurch konnte genau das unterbrochen werden; das ist jedenfalls unsere bisherige Annahme. Wir gehen davon aus, dass eine Verschlüsselung deshalb nicht stattgefunden hat, weil man es noch rechtzeitig bemerkt hat, dass sich ein Angreifer im System befindet und dann entsprechende Trennungsmechanismen greifen konnten.

Herrn Dr. Kollatz hatte ich noch notiert. Zum Thema Wahlsysteme kann ich sagen: Wir haben das für die Bundestagswahl auch schon mal gemacht, auch für die Europawahl. In beiden Fällen waren wir sehr erfolgreich. Sie haben das daran gemerkt, dass Sie nichts gemerkt haben. Das ist auch gut so. Da ist es nicht so, als bräuchten wir den Zugriff auf die Wahlsysteme, sondern es geht um die Frage: Wie werden die Wahlsysteme vor Ort von einem Backup gesichert? – Wir haben in Deutschland – ich nehme an, das wird in Berlin genauso sein, auch wenn ich dafür keine Expertin bin, das wissen Sie besser – Prozesse, bei denen papierbasiert vorgegangen wird. Nichtsdestotrotz ist es – gerade am Wahlabend, für die Übertragung der Ergebnisse oder für das, was dann an die Presse gegeben wird – absolut essenziell, dass die Integrität der Systeme gegeben ist, und da helfen wir auch gerne mit. Ich kann an dieser Stelle aber sagen, dass da Abkapselungen vorgenommen wurden. Das ist nicht dieselbe IT-Umgebung, so jedenfalls wurde mir an dieser Stelle versichert, und meine Kolleginnen und Kollegen helfen da auch mit.

Ob und wie man jetzt bei allen Systemen Passwörter und Zertifikate tauschen konnte, kann ich Ihnen an der Stelle nicht sagen. Wir sind normalerweise nicht diejenigen, die dann vor Ort auf die IT gehen, sondern das passiert hier durch die Organisation in Berlin. Wir stehen unterstützend zur Seite, aber es ist nicht so, als würden wir zentral auf die Systeme zugreifen. Das wollte ich an der Stelle auch noch mal kurz erläutern, dass es dazu auch Informationen gibt. – Das sind die Fragen, zu denen ich mich zumindest beim Mitschreiben in der Lage sah, etwas zu sagen. Wenn Sie das Gefühl haben, ich hätte auch noch zu etwas anderem etwas sagen können, melden Sie sich gerne noch mal. Das war von meiner Seite jedenfalls erst mal das, von dem ich glaubte, es gut beantworten zu können.

Vorsitzender Johannes Kraft: Ganz herzlichen Dank, Frau Plattner! – Gibt es noch Rückfragen an Frau Plattner? Sonst wäre der Vorschlag, dass wir uns sehr herzlich bedanken und Ihnen viel Erfolg bei Ihrer wichtigen Arbeit wünschen. Dann würden wir Sie nämlich nicht mehr länger aufhalten wollen. – Ich sehe keine weiteren Fragen an Sie. Dann haben Sie offensichtlich umfassend geantwortet. Ganz herzlichen Dank noch einmal für Ihre Zeit und für die Expertise und hoffentlich nicht bis schon bald wieder! – Wir hoffen, dass wir Sie nicht schon bald wieder brauchen werden. Ich danke Ihnen! Einen schönen restlichen Tag!

Claudia Plattner (BSI): Sehr gerne! Vielen herzlichen Dank an Sie und alles Gute!

Vorsitzender Johannes Kraft: Dann kämen wir jetzt zur Beantwortung der restlichen Fragen, die noch offen sich. Beginnen möchte Herr Staatssekretär Hauer. – Bitte schön, dann haben Sie das Wort!

Staatssekretär Florian Hauer (Skzl): Vielen Dank, Herr Vorsitzender! – Sehr geehrte Damen und Herren Abgeordnete! Vielen Dank für die Nachfragen! Ich hätte jetzt gerne auch noch einen persönlichen Dank an Frau Plattner gerichtet. Das hole ich dann im Nachgang bilateral nach. Ich habe es vorhin schon erwähnt, dass die Zusammenarbeit mit dem BSI auf allen Ebenen sehr gut ist und ich sehr dankbar bin für die Unterstützung, die wir dort aus Bonn und auch hier aus Berlin von den Kolleginnen und Kollegen des BSI bekommen.

Zu den Fragen: Ich würde der Reihenfolge nach vorgehen. Herr Vallendar! Sie hatten angefangen mit den ersten Fragen zur Informationspolitik. Ich will an der Stelle einfach noch mal wiederholen und noch mal ganz klar sagen: Wir, ich – aber ich glaube, das gilt für alle Kolleginnen und Kollegen senatsseitig – informieren immer nach bestem Wissen, und das Wissen sind dann Momentaufnahmen, die wir haben. Das ist hier auch so gewesen, gerade, was den Datenabfluss angeht und was auch die Erkenntnisse zum Datenabfluss angeht. Auch der Regierende Bürgermeister hat auf seiner Pressekonferenz im August gesagt: Nach seinem jetzigen Kenntnisstand seien keine sensiblen Daten abgeflossen. So habe ich es hier auch formuliert. Ich komme mir gelegentlich fast schon blöd vor, wenn ich in jedem Satz sage, dass die Angaben auf dem jetzigen Kenntnisstand beruhen. Es ist mir aber wichtig, damit genau solche Missverständnisse nicht entstehen.

Es ist hier eine sehr schwierige Lage, was den Überblick über die Lage und den Schaden angeht – anders als zum Beispiel am 3. Januar, wo ein Kabel abgebrannt war. Da kann man vor dem Kabel stehen und sieht: Hier sind fünf Meter Kabel abgebrannt, das ist der Schaden. – Das ist hier bei einem solchen Hackerangriff leider nicht so einfach, weil man große Mengen an Daten forensisch analysieren muss, um festzustellen, welche Daten tatsächlich abgeflossen sind et cetera und was der Schaden ist. Das ist die Situation, und das ist auch der Grund dafür, dass die Erkenntnislage dynamisch ist. Wir informieren aber wirklich immer und fortlaufend und schnell nach bestem Wissen. Wir hatten neben den Ausschusssitzungen immer wieder auch Gespräche mit den Fachsprecherinnen und Fachsprechern. An diesen Gesprächen waren auch Kollegen aus Ihrer Fraktion beteiligt. Ich habe diese Gespräche immer als sehr konstruktiv, produktiv und vertraulich empfunden und werde dieses Angebot und dieses Gespräch auch weiterhin suchen, weil es auch für uns sehr hilfreich gewesen ist, mit Ihnen diesen Austausch zu führen.

Sie fragten nach Ausgaben, die mit Blick auf die Forensik und ähnliche Dinge jetzt getätigt worden sind. Ich kann Ihnen an der Stelle keinen aktuellen Kontosollstand nennen, was das bisher konkret gekostet hat. Sie können aber davon ausgehen, dass wir Sie zu gegebener Zeit, wenn wir diese Informationen gesammelt haben, darüber informieren werden, was es genau gekostet hat. Diese Information ist im Übrigen auch deswegen wichtig, weil am Ende die Strafverfolgungsbehörden irgendwann an dem Punkt sind, wo sie einen Schaden festlegen und ermitteln müssen, um das Strafverfahren auf dieser Grundlage führen zu können. Alleine dafür benötigen wir es, aber ich gehe davon aus, dass wir auch in den zuständigen Gremien im Hauptausschuss darüber informieren werden. Wir werden Ihnen dann auch so schnell wie möglich die erbetene schriftliche Chronologie zukommen lassen. Ich bitte aber um Verständnis: Die letzten Tage haben es gezeigt, dass auch das sehr dynamisch ist, weil hier täglich und teilweise auch stündlich neue Informationen kommen und es für uns schon schwierig ist, die Lage fortlaufend zu managen.

Herr Ziller! Sie hatten nach den Angriffsvektoren gefragt, auch mit Blick auf die Frage, inwiefern wir das Netz, die IT absichern können und sicher sein können, dass wir sie abgesichert haben. – Frau Plattner hat dazu gerade einiges gesagt, und ich glaube, man muss an der Stelle vielleicht unterscheiden: Zunächst gibt es eine Sicherheit bezüglich der Angriffsvektoren in dem Sinne, dass sie strafrechtlich verwertbar sind, also sprich, dass Staatsanwaltschaft und LKA irgendwann an dem Punkt sind und für eine Klageerhebung sagen können: So ist es gewesen und nicht anders. – Das bedarf etwas mehr Belastbarkeit als das, was wir im Rahmen der Gefahrenabwehr benötigen. Das hat Frau Plattner eben auch noch mal erzählt. Ich glaube, da ist ausreichend klar, was die Angriffsvektoren waren und wo die entsprechenden Schwachstellen gelegen haben und wo – ich habe es eingangs auch schon gesagt – wir als Erstes mit der Forensik reingegangen sind, um sicherzustellen, dass zum einen keine Aktivitäten mehr zu beobachten sind und zum anderen sichergestellt ist, dass zumindest darüber kein weiterer Angriff mehr erfolgt. Aber um im strafrechtlichen Sinne klar sagen zu können, welcher Angriffsvektor initial war, also wo am Ende der Angriff erfolgt ist, der zu diesem Schaden geführt hat – das sind zwei unterschiedliche Dinge nach meinem Verständnis. Ich hatte aber das Gefühl, dass Frau Plattner das eben auch schon erklärt hat.

Zu den Kenntnissen über Datenabflüsse: Das ist das, was ich versucht habe, eingangs zu beschreiben, dass wir dafür zwei Bezugsquellen haben. Zum einen können wir durch unsere eigenen forensischen Erkenntnisse feststellen: Wo sind Daten kopiert worden, also entwendet worden? – Das ist das eine. Das andere ist, dass wir auf der Täterseite, also im Darknet, wo sie veröffentlicht werden, sehen: Welche Daten sind tatsächlich veröffentlicht? – Ganz offensichtlich gibt es dort ein Delta, und für dieses Delta gibt es verschiedene Erklärungsansätze und Erklärungsmöglichkeiten. Es kann auch sein, dass wir entweder in den forensischen Untersuchungen noch nichts gefunden haben oder dass Täter möglicherweise Spuren vernichtet haben bei uns im Datenbestand, und dass wir sie deswegen einfach nicht mehr finden. Dafür gibt es unterschiedliche Erklärungsansätze. Ich habe auch gesagt, dass wir gerade technisch vor der Herausforderung stehen, dass wir das, was dort abgeflossen ist, sichern müssen und dass allein dieser Kopiervorgang technisch nicht trivial ist, aber dass wir schon vor dem Freitag die entsprechenden Vorbereitungen und Vorkehrungen getroffen haben, sodass die zuständigen Behörden unmittelbar mit den Veröffentlichungen im Darknet mit der Sicherung um 15.35 Uhr begonnen haben – und das sind nicht nur Berliner Behörden, wir haben es gehört, sondern auch Bundesbehörden. – Zu den anderen technischen Dingen, was Sicherheit und Ähnliches angeht, hat Frau Plattner eben schon einiges gesagt. Dazu würde vielleicht Herr Dr. Kroll-Peters gleich noch etwas ergänzen können, auch was die Passwortregularien angeht. Zu der Frage, ob das bei allen Systemen anwendbar und umsetzbar ist – das war, glaube ich, Ihre Frage –, kann er sicherlich gleich noch etwas sagen.

Frau Abgeordnete Ahmadi, Sie haben nach den Mindeststandards in Berlin gefragt, und Sie hatten auch das Stichwort nationale Sicherheit genannt. Ich habe es eingangs gesagt, und Frau Plattner hat es eben auch noch mal genannt – ihre Wortwahl war: Es wurde noch nichts gefunden mit maximaler Kritikalität. – Das war ihre Aussage. Ich habe vorhin gesagt, dass wir zum jetzigen Zeitpunkt mit Blick auf nationale Sicherheit im Sinne von Verteidigungsfähigkeit davon ausgehen müssen und dürfen – wobei auch das vielleicht eine abstrakte Einschätzung ist –, dass bei SenMVKU und SenStadt bestimmte Informationen vielleicht oder hoffentlich gar nicht vorlagen – und wenn ja, dass sie dann, wenn sie eine bestimmte Einstufung hatten, nicht elektronisch abgelegt wurden. Elektronisch oder digital darf bis maximal VS-NfD abgelegt werden; Dinge darüber müssten eigentlich nur in Papierform vorliegen.

Wir gehen davon aus, dass es auch so gewesen ist. Aber, das hat Frau Plattner wiederholt, das habe ich auch gesagt: Wir sind am Beginn der Analysen. Ich habe eingangs versucht darzustellen, wie wir jetzt methodisch an die Risikoanalyse herangehen, vor welchen Herausforderungen wir stehen und was das auf der Zeitschiene bedeutet, dass es sehr aufwendig ist, bis wir wirklich sagen können, dass wir auch mit Blick auf die Qualität der abgeflossenen Daten Entwarnung geben können, auch mit Blick auf kritische Infrastruktur und Ähnliches.

Zu den Mindeststandards in Berlin: Wir haben über diese Frage beim letzten Mal, ich glaube, in der letzten Sitzung, gesprochen, auch über die Cyberabwehrstrategie. Ich habe die Frage damals schon beantwortet. Ich kann nur sagen, was ich vorhin schon erwähnt habe, dass es jetzt für den Moment vor allem darum geht, dass wir uns darauf konzentrieren, dass wir diesen akuten Angriff abwehren beziehungsweise den entstandenen Schaden so gut wie möglich managen, aber gleichzeitig, ohne dass wir die grundsätzliche strukturelle Analyse vorwegnehmen wollen, jetzt schon gucken und uns Maßnahmen anschauen und auch in die Wege leiten, die unmittelbar erforderlich sind, um das System zu härten.

Herr Abgeordneter Schulze, Sie haben verschiedene Dinge angesprochen. Ich fange mal mit dem letzten Punkt an, weil ich ihn mir am Ende hier oben notiert habe, Schadensersatz: Ich will das gar nicht ausschließen – ich kann es auch gar nicht –, dass am Ende möglicherweise solche Dinge geltend gemacht werden. Wie das dann rein juristisch zu bewerten wäre, was die Tatbestandsvoraussetzungen angeht, Fahrlässigkeit et cetera, die Beweisführung, wissen wir nicht. Das kann aber sein. Ich gebe aber zu, dass das im Moment für uns nicht Priorität hat. Es ist nicht so, dass wir jetzt schon haushälterisch dafür Vorkehrungen treffen würden, allein deswegen, weil wir es gar nicht quantifizieren können, aber dass so etwas kommen könnte, liegt in der Natur der Sache, dass so etwas denkbar ist.

Zur Großschadenslage, die Sie ansprachen: Ich sehe im Moment nicht, was diese Großschadenslage operativ an Vorteilen, an konkretem operativem Mehrwert für uns an der Stelle hätte. – Zwei Dinge: Mit Blick auf Bundesbehörden kann ich Ihnen sagen, dass wir maximale Unterstützung haben. Das läuft wirklich gut. Da würde eine solche Großschadenslage keinen Unterschied und Mehrwert darstellen. Ob es uns im Hinblick auf die Kooperationsbereitschaft des einen oder anderen Berliner Bezirks hilft? – Ich bin mir gar nicht sicher, ob da der richtige Weg die Ausrufung der Großschadenslage wäre – im juristischen Sinne, meinte ich jetzt –, oder ob wir über das LOG, die IKT-Steuerung den Hebel hätten. Ich werde am Ende noch etwas dazu sagen, weil Herr Dr. Kollatz auch danach gefragt hat und es mit den Bezirken leider etwas dynamisch ist. Darauf komme ich gleich noch mal zu sprechen, weil ich da ganz unterschiedliche Informationen bekomme und auch gerade vor wenigen Minuten wieder eine E-Mail von der zuständigen Stadträtin bekommen habe, die mich sehr irritiert. Dazu sage ich gleich noch etwas. – Sie hatten das Wort der Brandmauern genutzt. Dazu hat Frau Plattner gerade einiges gesagt, und dem habe ich nichts hinzuzufügen. Dazu hat sie eine Aussage getroffen, und ihre fachliche Expertise ist da über jeden Zweifel erhaben. Deswegen lasse ich das jetzt einfach mal so stehen, aber auch hier gilt: Wir gucken jetzt nach vorne.

Zum Umfang der Betroffenheit und zum Stichwort Beweissicherung: Ich habe vorhin gesagt, wie schwierig es für uns ist, den Umfang der Betroffenheit festzustellen. Die Beweissicherung im rechtlichen Sinne, das ist klar, müssen LKA und Staatsanwaltschaft machen, weil die die Strafverfolgungsbehörden sind. Ich habe eingangs beschrieben, dass sie das getan und veranlasst haben. Aber wir nutzen diese Daten mit für unseren Bereich und zur Erfüllung unserer

Aufgabe, und unsere Aufgabe ist, den Schaden zu managen, sofern das möglich ist. Frau Plattner hat dazu gesagt, was jetzt erforderlich ist, wie wir da herangehen müssen. Ich habe vorhin in meinem Eingangsstatement dargestellt, was die Herausforderungen und die Schritte sind, die wir dazu veranlasst haben und die Schritte, die wir in den nächsten Tagen unternehmen müssen. Dafür ist es in der Tat wichtig, dass wir diese Daten sichern. Es ist aber auch veranlasst, dass das geschieht.

Zur Frage mit den Haushaltskürzungen, muss ich Ihnen ganz offen sagen, liegen mir jetzt keine belastbaren Erkenntnisse vor. Ich muss auch ganz offen sagen, dass das für mich gerade in der täglichen Arbeit nicht die Priorität hat, und ich kann Ihnen nicht sagen, ob Haushaltskürzungen – beziehungsweise, es sind ja keine Kürzungen, es sind von der Senatskanzlei angemeldete Haushaltsmittel, die vom Haushaltsgesetzgeber nicht gegeben, gewährt wurden – dazu geführt haben, dass einzelne Behörden, Senatsverwaltungen daraufhin gesagt haben, dass sie deswegen bestimmte Dinge nicht mehr tun können. Das ist mir jetzt nicht bekannt, und mir ist auch nicht bekannt, ob das in irgendeiner Form für die Szenarien, die wir jetzt haben, kausal wäre. Ich weiß es einfach nicht. Ich schließe das auch nicht aus, aber mir liegen dazu keine positiven Kenntnisse vor.

Der letzte Punkt in den Fragen an mich – Herr Dr. Kollatz ist gerade nicht da – war das Thema mit den Bezirksämtern. Im Moment ist es ein Bezirksamt, das laut unseres Wissens noch nicht im Status der vollen Kooperationsbereitschaft ist. Ich will es nicht namentlich nennen, weil ich sage, dass das Dinge des verwaltungsinternen Krisenmanagements sind. Darunter subsumiere ich das, und darüber will ich hier nicht öffentlich reden oder die Betroffenen nicht namentlich nennen. Ich kann nur sagen, dass ich das für extrem ärgerlich halte, weil ich es in dieser Situation für grob fahrlässig halte. Wir haben dargelegt, warum wir es als notwendig erachten, dass die forensische IT-Software in alle Bezirke, in alle Systeme ausgerollt wird. Wir haben datenschutzrechtlich dargelegt, warum das aus unserer Sicht rechtlich kein Problem darstellt. Wir haben versucht, die Argumente außer Kraft zu setzen. Es gab ein Hin und Her. Weil dort die örtlichen Kräfte, die politisch Verantwortlichen, nicht die Verantwortung übernehmen wollten, habe ich gesagt, ich übernehme alle Verantwortung für das, was da kommt, auch datenschutzrechtlich und Ähnliches. Daraufhin habe ich die Rückmeldung bekommen, es sei veranlasst, und der betroffene IT-Mitarbeiter sei angewiesen worden. Das war die Information vom Samstag. Die wurde Sonntagmorgen noch einmal bestätigt, und eben, vor wenigen Minuten, bekomme ich eine E-Mail von der zuständigen Stadträtin für IT, die mir schreibt: Kommando zurück, sie würden es erst morgen entscheiden. – Das ist eine total unglückliche Situation, und ich halte sie, wie gesagt, für grob fahrlässig, denn wir sind der festen Überzeugung, dass das dringend erforderlich ist, dass wir Gefahr im Verzug haben und wir so schnell wie möglich die Forensik auch auf die Bezirke ausrollen müssen. Wir werden uns im Nachgang kurz beraten, was wir daraus an Schlussfolgerungen ziehen, gegebenenfalls auch rechtlich. Ich kann nur an diejenigen appellieren, die vielleicht Zugänge zu der betroffenen Stadträtin haben. Ich habe gerade eben schon und werde auch noch einmal bilateral mit den Abgeordneten aus der betroffenen Partei in dem Fall sprechen und um Unterstützung für die Sensibilisierung bitten, dass das schnell kommt, denn ich muss sagen, meine Geduld ist am Ende. Es kostet unheimlich viel Kraft, sich mit solchen Widrigkeiten auseinandersetzen zu müssen, und ich halte das für nicht verantwortlich und verantwortbar, dass dort immer noch eine Blockade stattfindet und nicht mit uns kooperiert wird. – Ich hoffe, jetzt alle Fragen beantwortet zu haben. Gegebenenfalls haben wir noch eine weitere Runde. Danke!

Vorsitzender Johannes Kraft: Vielen Dank, Herr Hauer! – Dann hat sich Herr Staatssekretär Slotty gemeldet. – Bitte schön!

Staatssekretär Alexander Slotty (SenStadt): Danke, Herr Vorsitzender! – Ich will gleich bei dem letzten Punkt anschließen und den Kollegen dahingehend ergänzen, weil ich das auch heute Morgen bei der montäglich stattfindenden Staatssekretärskonferenz schon erklärt habe: Das ist eine unglaubliche Stresssituation für alle, und dass wir hier mit einem Bezirk, der Teil dieser Verwaltung ist, über solche Maßnahmen im Rahmen einer solchen Lage mehrere Tage diskutieren müssen, dafür fehlt mir ehrlicherweise jegliches Verständnis. Deswegen sage ich mal: Ich will jetzt kein Ultimatum setzen, aber ich habe heute Morgen schon bekannt gegeben, dass ich diesen Bezirk von allen IT-Fachverfahren unserer beiden Häuser trennen werde, wenn sich der Bezirk weiter verweigert, wenn er sich der Forensik, also der Aufklärung der Frage, ob sich auf dem dortigen System Schadsoftware befindet, und auch der Sicherheit, die durch diesen Dienstleister zusätzlich zu unseren IT-Sicherungsmaßnahmen hergestellt wird, verweigert. Diese Sicherheit ist dann nicht gegeben. Insofern bitte ich um Verständnis, dass wir jetzt mit Nachdruck versuchen werden, den Bezirk zum Einlenken zu bewegen.

Vielleicht noch mal zu den ergriffenen Maßnahmen: Da wird mich Herr Werdin als Leiter unserer IT gleich noch ergänzen. Wir haben natürlich das Sicherheitsniveau für die beiden Senatsverwaltungen durch eine stärkere Sensibilisierung der Systeme und der Mitarbeitenden erhöht. Wir haben verschärfte Passwortregeln durchgesetzt. Wir haben die Zertifikate für die Arbeit von außen erneuert. Wir haben unsere kritischen Systeme stärker abgeschottet, eine weitere Segmentierung von Kommunikationsnetzen vorgenommen und die Sensorik entsprechend hochgefahren. Herr Werdin wird gleich noch darauf eingehen, was auch noch auf der Ebene der Server jeweils unternommen wurde.

Ich will jetzt noch mal vorne anfangen, weil der Begriff Kompetenzgerangel vorhin gefallen ist. Ich glaube, wir haben in den letzten Jahren immer einen sehr fairen Umgang miteinander gehabt. Ich glaube, wir können in einer solchen Lage nicht von einem Kompetenzgerangel sprechen. Es gebührt doch der Respekt vor den Ermittlungen der Strafverfolgungsbehörden, dass wir nicht ein Bild erzeugen, bei dem das LKA uns irgendetwas wegnimmt und wir dadurch unsere Arbeit nicht mehr machen können. Frau Plattner hat ihrerseits als Präsidentin des BSI, die auch in die Aufarbeitung eingebunden ist, dem Grunde nach bestätigt, dass diese Phishing-Variante diejenige ist, von der gegenwärtig ausgegangen wird, das heißt, dass es einen Mitarbeiter gegeben hat, der aus einer E-Mail eine Datei heruntergeladen hat über einen Link oder Ähnliches. Ich glaube, jeder hier im Raum weiß – dafür muss man kein Experte sein –, das ist eben ein Weg. Das ist das letzte Level, die Mitarbeiterin und der Mitarbeiter, innerhalb dieser Sicherheitsarchitektur in der IT, auf die man auch angewiesen ist. Es hat aber zwischen dem LKA und uns keinerlei Gerangel gegeben, sondern für uns ist natürlich klar, dass die Ermittlungen vollumfänglich unterstützt werden und wir dann auch im Weiteren auf die Ermittlungserkenntnisse angewiesen sind. Aber ich habe natürlich größten Respekt davor, dass Staatsanwaltschaft und Landeskriminalamt uns nicht ihre aktuellen Erkenntnisse einfach mal so mitteilen, sondern natürlich abwägen müssen, welche Informationen sie mit dem Senat und dem politischen Raum teilen können.

Ich will nur zur Klarstellung sagen, damit wir den gleichen Kenntnisstand haben: Diese Logdateien, von denen ich vorhin gesprochen habe, über die wir auch Erkenntnisse darüber gewinnen, was an Daten abgeflossen ist, sind nicht alle gelöscht, aber da wir Informationen

haben über abgeflossene Dateien, zu denen es keine entsprechenden Logdateien auf unseren Systemen gibt, müssen wir davon ausgehen, dass Logdateien gelöscht wurden. Wir haben aber auch Logdateien gefunden. Wir wissen beispielsweise, dass auch verschlüsselte Dateien abgeflossen sind. Das heißt, das sind Dateien, bei denen wir uns erst einmal nicht so ganz große Sorgen machen. Ärgerlich sind natürlich die Dateien, die unverschlüsselt abgeflossen sind.

Es wurde vorhin auch die Frage gestellt, welche Konsequenzen das eigentlich am Ende hat. Gegenwärtig konzentrieren wir uns auf die Herstellung der IT-Sicherheit und auf die Aufklärung des Vorfalls. Selbstverständlich dringen wir dadurch auch in immer tiefere Ebenen vor. Es gab aber auch einen Bundestagsabgeordneten, der schon auf Bundesebene personelle Konsequenzen gefordert hat. All das wird beantwortet werden müssen. Es gibt auch bei mir in der Verwaltung Kolleginnen und Kollegen, die trotz der IT-Sicherheitsvorschriften, die schon gegolten haben und die alle kennen sollten – insbesondere die Administratoren von IT-Fachverfahren –, Zugangsdaten und Passwörter unverschlüsselt in Worddokumenten abgespeichert haben, die dann eben abgeflossen sind. Diese Erkenntnisse haben wir, wir kennen auch die Wege. Gegenwärtig ist das nicht das Wichtigste, aber wir werden das natürlich im Weiteren noch untersuchen und dann auch zu würdigen wissen.

Was die Fachverfahren selbst betrifft – ich muss das, wie der Kollege, immer wieder sagen: Nach heutigem Erkenntnisstand geht es ausschließlich um Dateien, die von Fileservern abgeflossen sind. Nach unserem Stand sind keine Daten aus Fachverfahren abgeflossen. Ich hoffe, dass es dabei bleiben wird. Wie gesagt, bis dato hat die Forensik hier keinerlei andere Erkenntnisse gewonnen. Frau Plattner hatte vorhin schon einmal beschrieben, wie das BSI jetzt damit umgeht, Daten aus dem Darknet, aus dem Tor-Netzwerk, herunterzuladen. Ich sehe es nicht als meine Zuständigkeit, einen Zugang in das Darknet herzustellen, um dort dann einfach mal das Datenpaket herunterzuladen, das angeboten wird, denn wir müssen gegenwärtig davon ausgehen, dass sich in diesen Daten, die dort angeboten werden, wiederum neue Schadsoftware befinden kann. Diese Risiken wollen wir auf gar keinen Fall eingehen. Deswegen liegt das in den Händen der Behörden, die in die Aufarbeitung und Ermittlungen eingebunden sind, das heißt, beim LKA und den entsprechenden Bundesbehörden, die hier unterstützen, dafür zu sorgen, dass hier keine weitere Schadsoftware durch ein wie auch immer geartetes Herunterladen in unsere Systeme einsickern kann.

Ansonsten kann ich heute auch noch sagen: Wir haben – zumindest, was die Systeme der SenStadt und der SenMVKU betrifft – inzwischen 95 Prozent der Daten und Systeme vollständig überprüft und können an dieser Stelle sagen, auf diesen Systemen ist nach unseren Erkenntnissen nicht mit weiteren kompromittierten Usern, mit Schadsoftware oder irgendwelchen anderen Schläferdateien oder was auch immer zu rechnen. Wir haben diesen Prozess also fast abgeschlossen. Wenn wir die 100 Prozent erreicht haben, heißt das aber nicht, dass wir einen Haken dranmachen und sagen, toll, haben wir gut gemacht, sondern natürlich wird das Ganze wiederholt werden. Die Forensik wird da weiterlaufen; das ist Teil der Sicherungsmaßnahmen, die wir ergriffen haben und die erst mal fortlaufend bestehen werden. – Da es thematisch passen würde, wäre es toll, wenn Herr Werdin jetzt kurz das Wort bekommen könnte, wenn es in Ordnung wäre.

Vorsitzender Johannes Kraft: Sehr gerne! – Bitte, Herr Werdin!

Christian Werdin (SenStadt; Referat Informationstechnik; Leitung): Vielen Dank! – Nur, weil die Frage nach den Passworten und Zertifikaten vorhin aufkam: Wann wurde was wie in der zeitlichen Abfolge zurückgenommen beziehungsweise neu ausgerollt? – Das war tatsächlich ein sequenzieller Prozess. Wir hatten in Abstimmung mit dem Landesinformationssicherheitsbeauftragten und auch unter Beratung mit dem BSI eine Maßnahmenliste erarbeitet: Was muss vor der Netzkopplung unbedingt umgesetzt werden? Was sind Maßnahmen, die danach in die Planungen einfließen müssen beziehungsweise vielleicht schon umgesetzt sind? – Da gab es eine entsprechende Punkteliste. Unter anderem war zum Beispiel der Passwortwechsel in der Domäne festgehalten, insbesondere von den Privilegierten, also Administrationskonten. Das musste schon vor dem Wiederanschluss geschehen.

Die weiteren Maßnahmen: Ich glaube, 17 Punkte sind auf der Liste. Wir haben den Internetzugang beschränkt und erst mal nur auf ganz dedizierte Ziele zugelassen; das haben Sie auch der Presse entnehmen können. Mit dem neuen Erkenntnisstand, der sich einerseits aus den Vorabveröffentlichungen, aber auch den Veröffentlichungen am Wochenende ergeben hat, haben sich natürlich weitere Maßnahmen angeschlossen. Wir haben viel Unterstützung – auch da noch mal ein Danke – von den Kollegen des ITDZ erhalten. Wir haben alle Kleinzertifikate zurückziehen lassen. Das war nach der ersten Veröffentlichung, als wir gesehen haben, dass Passworte tatsächlich in Klartext gespeichert werden. Wir haben Passwortwechsel dann erneut wiederholt, weil wir gesagt haben, wir wollen das Risiko ausschließen, und zwar flächendeckend, und haben zu dem Zeitpunkt schon gesagt, auch unsere anderen Systeme, die wir verwalten, müssen unbedingt einem Passwortwechsel unterzogen werden. Dann kam auch noch das Schreiben von CDO Hauer, dass das landesweit zu erfolgen hat, und insofern haben dann die Zahnräder so ineinander gegriffen.

Es kam, glaube ich, auch die Frage auf, ob jedes Fachverfahren diese Vorgabe technisch erzwingen kann. Ich weiß es nicht, aber ich würde vermuten, nein, das geht nicht bei jedem Fachverfahren. Sie wissen selbst, wie alt manche Fachverfahren sind. Da werden diese Regelungen wahrscheinlich technisch nicht erzwingbar sein. Da gilt es, zurückzumelden, wenn das nicht möglich ist – auch die Aufforderung kam ja, dazu wird Herr Kroll-Peters wahrscheinlich noch etwas sagen. Wir haben von zentraler Seite erst mal das versucht, was möglich ist, aber auch versucht, die Beschäftigten so zu sensibilisieren, dass sie selbst sehen, wenn manche Passworte vielleicht doppelt verwendet werden, auch im privaten Umfeld, auch dorthin zu schauen und entsprechende Hinweise zu geben, wie man überhaupt mit Passworten umgeht. Das Thema SoSafe ist angesprochen worden: Da haben wir eine neue Kampagne ganz explizit auf diesen Punkt gestartet, und in einem an diesem Wochenende stattfindenden Prozess mit dem ITDZ haben wir für bestimmte Fachverfahrensseiten – manche haben wir ohnehin noch nicht angeschlossen – noch einmal gesagt, wir müssen auch da sicher gehen, dass wir die Zertifikate getauscht haben. Das ist auch an die Bezirke gegangen. Dazu sind wir in Abstimmung mit dem ITDZ. Die sind dabei, diese Zertifikate neu auszustellen, wohl in dem Wissen, dass es auch wieder zu Einschränkungen kommen kann. Aber wir wollen nicht auf die Erkenntnisse dieser Veröffentlichung warten – denn, Sie haben es heute schon oft genug gehört, das kann dauern. Wir haben gesagt, zur Sicherheit ziehen wir alle zurück, selbst wenn sie nicht in diesem Bestand sind, um eine potenzielle Gefährdung, die wir vielleicht erst in zwei Wochen erkennen, an der Stelle auszuschließen. – Das wäre es von meiner Seite. Danke!

Vorsitzender Johannes Kraft: Vielen Dank! – Dann Staatssekretär Herz, bitte schön!

Staatssekretär Arne Herz (SenMVKU): Herzlichen Dank, Herr Vorsitzender! – Ich will das vorwegschieben, was auch die Präsidentin des BSI, Frau Plattner, gesagt hat, weil es zu mehreren Dingen in den Fragen passt und es auch notwendig ist, sich das zu verinnerlichen: Nur der Download der Dateien – so, wie sie von der Tätergruppe veröffentlicht wurden – gibt uns die Sicherheit, welche Dateien – nicht welche Verzeichnisse –, sondern welche Dateien im Einzelnen abgeflossen sind. Frau Plattner hat Ihnen erklärt, dass dieser Download dauert. Was wir kennen, sind die Verzeichnisse, und dementsprechend können wir mindestens in vielen Fällen etwas ahnen. Der Kollege Slotty hat eben schon beschrieben, wie sich die Erkenntnis mit den Logdateien verhält. Überall da, wo ich aus den eigenen Erkenntnissen sicher weiß, dass ich einen Abfluss habe, kann ich logischerweise in diese Verzeichnisse reinschauen, aber ohne dass ich das sicher weiß – und das werde ich erst mit einem kompletten Download und einer Bewertung der durch die Tätergruppe veröffentlichten Dateien durch die Sicherheitsbehörden wissen – bin ich begrenzt, zumindest in der Möglichkeit, jede Datei im Einzelnen bewerten zu können, die bei uns existiert, und zu erkennen, ob sie abgeflossen ist.

Konkret zu der Frage – und das hat damit zu tun, deswegen habe ich das an den Anfang gestellt –, wie viele Beschäftigte wir benachrichtigt haben: Wir haben alle rund 1 650 Beschäftigten benachrichtigt. Warum? – Weil wir mit der Erstveröffentlichung schon Kenntnis hatten, dass sogenannte Home-Laufwerke, also die persönlichen Laufwerke der Mitarbeiterinnen und Mitarbeiter, betroffen sind, ohne dass wir abschätzen konnten, wie viele das sind – auch da wieder aufgrund des Problems, das ich gerade beschrieben habe. Wir haben durch die Indexe vom vergangenen Freitag erfahren, dass aus der Abteilung Z, Zentrales – dort, wo der Personalbereich angesiedelt ist – mindestens erhebliche Dateiverzeichnisse abgeflossen sind. In dieser Kombination ist es sehr wahrscheinlich, dass mehr oder weniger jeder Mitarbeiter, jede Mitarbeiterin betroffen sein kann. Wenn es am Ende 2 Prozent nicht wären, dann habe ich lieber jeden Einzelnen jetzt informiert als zu einem späteren Zeitpunkt oder gar sukzessive. Deswegen haben wir uns zu diesem Schritt entschlossen, denn, ich habe das vorhin schon anklingen lassen, auch gegenüber unseren Beschäftigten – ich komme gleich noch zu der Frage nach Externen – haben wir eine Verantwortung. Wir müssen möglichst ab dem Zeitpunkt, wo wir zumindest eine relative Wahrscheinlichkeit haben, genau diese nicht nur datenschutzrechtlich gebotene Information teilen, sondern schlicht und einfach unser Wissen teilen, soweit das eben geht.

Das bringt mich zu der Frage des Abgeordneten Schatz nach der Anzahl der Betroffenen außerhalb der Verwaltung. Aus den bereits beschriebenen Gründen wäre es im Moment rein spekulativ, irgendeine Zahl zu nennen, denn erst mit der kompletten Analyse werde ich Ihnen irgendwann eine Zahl nennen können. Auch da gilt selbstverständlich, dass wir nicht nur die rechtlichen Gegebenheiten der Benachrichtigung einhalten werden nach Kenntnisnahme durch uns und dementsprechend wissen, wen wir überhaupt benachrichtigen müssen, sondern dass wir das immer da tun werden, wo wir irgendeine Ahnung haben. Ich bitte aber um Verständnis, dass ich gar nicht möchte, dass wir mit nicht gesicherten Erkenntnissen arbeiten. Für viele der Überlegungen, die im Raum stehen, seit Freitag und auch schon vorher, was da alles betroffen sein könnte, ist das für uns als Behörde noch spekulativ. Wenn Sie es so wollen, könnten Sie über jedes Themenfeld, das die SenMVKU bearbeitet, spekulieren, dass das abgeflossen ist, dass das einen potenziellen Schaden haben könnte, egal in welchem Bereich. Das darf jeder, weil in diesem Land Gott sei Dank eine Meinungsfreiheit herrscht. Aber Sie haben sicherlich genauso Verständnis, dass wir als Behörde nur von den gesicherten Erkennt-

nissen berichten und dementsprechend auch nur solche bestätigen werden und alles Weitere von unserer Seite aus nicht tun.

Ich will das, was der Kollege Slotty zum Stichwort Landeskriminalamt und Ermittlungsbehörden insgesamt gesagt hat, unterstreichen: Erstens kann ich vorwegstellen, dass die Zusammenarbeit insbesondere mit dem Landeskriminalamt, aber auch mit den Sicherheitsbehörden des Bundes, der Kollege Hauer hat es vorhin ganz allgemein angesprochen, aber auch im Konkreten, da, wo wir Erkenntnisse haben oder Anfragen der Behörden kommen, um die Fragen, die sie gerade stellen, in anderer Weise beantwortet zu bekommen, einfach hervorragend ist und auf einem sehr kurzen Dienstweg läuft.

Der Abgeordnete Schatz hatte sich zum Stichwort Mindset geäußert. – [Zuruf: Schulze!] – Entschuldigung! Schulze. Zumindest hatte ich es in der richtigen Fraktion verortet. Der Kollege Hauer hat es vorhin erwähnt: Wir haben eine Besondere Aufbauorganisation ins Leben gerufen, weil das die Aufgaben, die wir haben, das ganz normale Verwaltungshandeln, bei Weitem überschreitet. Deswegen wurden die Kräfte, die notwendig sind, zusammengezogen, aber es wird im Weiteren mit Sicherheit noch ausgeweitet werden. In eigener Zuständigkeit, aber auch und vor allem da, wo das LKA in deren Zuständigkeit wiederum Nachfragen hat, um eigene Einschätzungen vornehmen zu können, laufen wir zweigleisig und haben diese Fragen durch die Sicherheitsbehörden in dieser BAO gebündelt, um schnellstmöglich jeweils Auskünfte geben zu können, damit andere wiederum in ihrer Professionalität und Zuständigkeit Entscheidungen beziehungsweise Bewertungen treffen können und darauf aufbauend gegebenenfalls Entscheidungen treffen können. Insofern können Sie mir sicherlich glauben und zutrauen, dass das, was uns jetzt insbesondere seit anderthalb Wochen noch mal anders als vorher begleitet, in Strukturaufbau, in Strukturvollzug, aber vor allen Dingen im Inhalt dessen, das wir da bewerten und tun, ein Mindset voraussetzt, wie ich es nicht härter fassen oder formulieren würde, ein Engagement, das ich zwar in gewisser Weise für jeden, der im öffentlichen Dienst und damit für den Staat arbeitet, voraussetze, aber das – das wissen wir alle – in unterschiedlicher Form, mal so, mal so, ausgeprägt sein kann. Dieses Mindset ist im höchsten Maße vorhanden.

Es wird uns auch noch eine ganze Weile begleiten. Deswegen wird es Kraft kosten, aber diese Kraft wenden wir auf. Ich kann Ihnen sagen, dass die Mitarbeiter sehr schnell bereit sind und waren – insbesondere die, die ein absolutes Spezialwissen haben, um bestimmte Einschätzungen treffen zu können –, zu unterstützen und schlicht und einfach zur Verfügung standen. Das tun sie bis heute. Ich muss nicht die einzelnen Stellen, die sehr besonders gefordert sind, erwähnen. Es ist in gewisser Weise unsere Aufgabe, die nehmen wir ernst, und deswegen ist das Mindset in höchstem Maße vorhanden. Damit will ich gerne schließen.

Vorsitzender Johannes Kraft: Vielen Dank! – Möchten Sie ergänzen? – Selbstverständlich. Ich will nur mal, bevor Sie das Wort ergreifen, darauf hinweisen, dass wir noch eine halbe Stunde reguläre Sitzungszeit haben. Wir haben aktuell auf der Redeliste zwei Wortmeldungen. Vielleicht können wir uns, nachdem Herr Kroll-Peters geantwortet hat, auf ein Verfahren verständigen. – Bitte schön!

Dr. Olaf Kroll-Peters (Landes InfSiBe): Nachdem mein Chef mich schon angekündigt hat, ergreife ich natürlich gerne das Wort. Hallo! – Herr Ziller hat am Anfang die Frage gestellt – leider ist er gerade rausgerannt: Was müssen wir eigentlich weiter in Zukunft machen? – Da möchte ich als Landesbevollmächtigter für Informationssicherheit sagen oder Ihnen mitgeben: Wir sollten uns vielleicht ein bisschen von der konkreten Situation lösen und auf die generelle Problematik übergehen. Da haben Sie eigentlich ein ganz gutes Beispiel genannt: Passwörter. Wir haben in der konkreten Situation gesehen, das Passwörter abgeflossen sind, und wir haben versucht, möglichst schnell dafür eine Lösung zu finden, damit wir dieses Problem nicht mehr haben. Irgendjemand fragte auch: Ist das jetzt das Ende? – Nein, die nächste Passwortänderung wird demnächst kommen, weil wir jetzt abgewogen haben zwischen dem, was wir schnell schaffen, um da ein bisschen Sicherheit rein zu bekommen, und dem, was man eigentlich wirklich machen muss. Wenn Sie sich da die Vorschriften vom BSI angucken, sind sie noch deutlich umfangreicher als die paar Zeichen, die wir zurzeit haben. Jetzt überlegen Sie alle mal, wie viele Ihrer Mitarbeiter in letzter Zeit geflucht haben, weil sie ein Passwort eingeben mussten, das schon recht lang ist, aber eigentlich noch viel länger sein müsste. Das liegt daran, dass wir mittlerweile eigentlich viel weiter sind. Wir wissen, dass wir eine sogenannte Multi-Faktor-Authentifizierung brauchen, bei der wir uns nicht mehr so viel Kram, den sich ein Mensch sowieso nicht merken kann, merken müssen, und dafür etwas anderes haben.

Jetzt ist natürlich die Frage: Warum haben wir das nicht gleich gemacht? – Das kann ich Ihnen sagen: Schon diese 16 Zeichen – das hat Herr Ziller gerade auch gefragt – stoßen bei vielen unserer gut abgehangenen Fachverfahren auf Begeisterung und sind nicht umsetzbar. Was machen wir in dem Fall? – Wir haben überall gefragt: Wo haben wir denn ein Problem damit und müssen ergänzende Sicherheitsmaßnahmen einführen? – Das hat Frau Plattner gerade auch gesagt. Wir haben eine ganze Menge Absicherungsmaßnahmen, und es ist jetzt ein bisschen kurz gegriffen, dass wir sagen, wir machen Passwortänderungen, wir gucken uns die Firewalls an, wir machen Zero Trust. Bis Ende 2029 müssen wir Zero Trust umsetzen, aber auch Post-Quantum und IPv6 müssen wir umsetzen. Wir haben da eine ganze Menge vor, und dafür sind unsere Verfahren nicht wirklich geeignet, und da müssen wir auch an dieses Mindsetting ran, dass wir eine sichere Welt wollen, aber das Ganze irgendwo ändern müssen. Das würde ich gerne mitgeben.

Bei den Passwörtern ist es so, dass wir sie jetzt mal schnell geändert haben, damit wir ein bisschen auf der sicheren Seite sind. Es gab noch ein paar andere Maßnahmen; Herr Werdin hat, glaube ich, eine von denen genannt, weil wir gesehen haben, da sind manche Sachen abgeflossen. Dann gucken wir uns genau an: Welchen Angriffsvektor sehen wir, um da Gegenmaßnahmen zu machen? – Aber eigentlich müssen wir da noch einen Schritt weitergehen und die Basis darunter sicher machen. Wir brauchen eine Architektur, denn wenn ich jetzt mit meiner Sicherheitsarchitektur komme und sage, wir brauchen Multi-Faktor-Authentifizierung und die Architektur darunter es nicht hergibt, dann spielt die Sicherheitsarchitektur irgendwann keine Rolle mehr. – Vielen Dank! Ansonsten Fragen gerne an mich.

Es kam noch eine Frage zu den Sicherungskopien, die wir aus den Daten, die im Internet sind, ziehen könnten. Ganz ehrlich: Machen Sie das besser nicht, weil wir nicht wissen, welche Schmutzdaten da noch mitheruntergeladen werden, weil wir davon ausgehen, dass nicht nur die Wirkdaten heruntergeladen werden, sondern vielleicht noch ein paar Gimmicks, die dabei sind. Wir haben das LKA auf unserer Seite. Die laden gerade kräftig runter. Wir haben noch

zwei Forensikdienstleister, die kräftig herunterladen. Es dauert vermutlich noch eine ganze Weile. Wenn Sie Fragen haben, können wir die im Nachgang irgendwann besprechen, wenn die heruntergeladen sind, aber wenn Sie es selbst tun, machen Sie das vielleicht irgendwo in einer Umgebung, in der Sie sicher sind, dass da nichts passieren kann.

Vorsitzender Johannes Kraft: Vielen Dank für den praktischen Hinweis! – Ich habe noch zwei Kollegen auf der Redeliste. Das sind Herr Ziller und Herr Schatz. Ich gucke mal in die Runde, ob wir weitere Wortmeldungen haben. – Das ist nicht der Fall. Dann gucke ich noch mal in Richtung Frau Kamp und Frau Dr. Borelli: Gibt es aus Ihrer Sicht Dinge zu ergänzen? – Sie müssen nicht. Ich frage nur zur Sicherheit. Wenn Sie möchten, dann sehr gerne.

Dr. Maria Borelli (ITDZ): Ich würde gerne, aber vielleicht warte ich erst mal auf die Fragen, die kommen.

Vorsitzender Johannes Kraft: Okay, alles klar! – Dann hat sich jetzt noch Herr Vallendar gemeldet. Mein Vorschlag wäre, dass wir diese Runde noch machen, dann machen wir eine Antwortrunde, und dann haben wir vielleicht noch Organisatorisches zu besprechen. – Herr Kollege Ziller, bitte!

Stefan Ziller (GRÜNE): Vielen Dank! – Danke fürs Warten! Die Fragen an das ITDZ hatte ich zumindest noch zurückgestellt, denn wir wollten ein bisschen priorisieren. Vielleicht stelle ich, wenn das jetzt die letzte Runde ist, noch mal insgesamt die Frage an den Senat: Wie viele Personen oder Unternehmen wurden bereits identifiziert, und wie viele davon wurden schon gewarnt? – Ich stelle gar nicht infrage, dass Sie das nicht vollständig wissen, aber Sie werden den Prozess ja irgendwie begonnen haben müssen und eine Zählung der Geschädigten haben. Die wird im Laufe der Erkenntnisse immer höher werden. Dafür habe ich totales Verständnis, aber ich hätte gerne ein Gefühl dafür, wo wir da im Prozess stehen, auch angesichts der Informationen, die die Kriminellen veröffentlichen. Daran kann man sich ja ein bisschen orientieren. – Das wäre die erste Sache.

Die zweite Sache, zum Thema Angriffsvektor: Ich hatte vorhin nachgefragt, weil Herr Slotty gesagt hat, mit dem Phishing ist es nicht so richtig klar, der Rechner war weg, und deswegen wussten Sie es nicht. – Das BSI hat das jetzt zumindest aufgeklärt. Alles gut, dann sind Sie jetzt auch up to date, was die Infos angeht, und dann können wir das erst mal abhaken. Nach dieser Ausschusssitzung habe ich aber das Gefühl, wir sind mitten auf dem Ozean. Wir haben uns zwar jetzt an irgendeinen Holzstamm geklemmt, aber was die IT-Sicherheit angeht, ist die Lage doch weiter dramatisch. Meine Frage wäre jetzt aber, vielleicht ans ITDZ: Wie gehen Sie mit der Situation um? Welche Erkenntnisse haben Sie inzwischen zu den Defiziten der Architektur und auch in Sachen Netzsegmentierung? Was muss eigentlich gemacht werden? Funktioniert dieser Domainverbund? Braucht man zusätzliche Schutzmechanismen in absehbarer Zeit und nicht erst 2029/2030? – Ich teile auch die Einschätzung, dass nicht die ganze Verwaltung betroffen sein darf, wenn ein Mitarbeiter auf so einen Phishing-Link klickt. Ich hatte extra nachgefragt: Es kann nicht ausgeschlossen werden, dass über den Domainverbund SenStadt und SenMVKU hinaus andere Verwaltungen betroffen sind. Wie ist die Architektur des Netzes? Wie kann man sie machen, dass man das eher vermeidet? –, denn das halte ich für schwierig.

Wir wissen auch alle, dass wir veraltete Fachverfahren haben, für die zum Teil Sicherheitsstandards von Windows 11 und anderen Sachen gesenkt werden müssen, die zum Teil auch im ITDZ laufen nach meinem Kenntnisstand. Wie geht das ITDZ damit um? Gibt es da eine Liste von Fachverfahren, die man aus Sicherheitsgründen vielleicht doch vom Netz nehmen sollte, auch wenn sie eigentlich gebraucht werden, aber die das Landesnetz gefährden? Oder bauen Sie eine isolierte Umgebung für den ganzen alten Mist auf und nehmen den aus dem Landesnetz heraus und bauen ein isoliertes Netz? – Da wäre die Frage, was das ITDZ da sieht.

Dann zur Frage der Hardware: Teilt das ITDZ die These, dass der Abfluss vor allem von Fileservern eine gewisse Sicherheit gibt, dass Netzwerkkomponenten und andere Hardware nicht beschädigt oder kompromittiert sind, oder besteht nicht doch die Aufgabe über kurz oder lang, die Hardware auch im Netz auszutauschen? – Das kann im Zweifel auch risikobasiert, sozusagen auch mit regulärem Austausch passieren, aber ist unsere Hardware sicher?

Über Downloads haben wir gesprochen und gesagt, dass der kriminelle Server langsam angebunden ist. Irgendwann wird das Land Berlin oder eine Stelle die Daten aber mal haben. Kann das ITDZ dabei unterstützen, oder wie kann das ITDZ dabei unterstützen, diese Daten durchsuchbar zu machen, um die Identifikation besser zu machen? Wie ist überhaupt das ITDZ in das System eingebunden? Gibt es Behörden, Bezirke oder andere, die gesagt haben: Liebes ITDZ, ich will mit dir reden! Ich weiß, ich habe ein Problem, ihr müsst mir helfen! – Gibt es diese Prozesse schon? Hat das ITDZ den Auftrag, die Verantwortungs- oder Betriebsübernahme von kritischer IT anzugehen, mit einem Zeitplan, Maßnahmenplan, also sich auf den Weg zu machen? Oder ist es weiter so, wie wir in den Haushaltsberatungen gelesen haben: Jeder fragt nach, der Lust hat, und dann gucken wir mal, wann das passiert? Hat sich da nach dem Vorfall etwas geändert?

Der letzte Punkt, der vielleicht auch zum Nachdenken anregen sollte: Wir haben jetzt gehört, es sind Daten vor allem auf Fileservern betroffen. Fachverfahren speichern Daten anders ab. Deswegen macht die Unterscheidung total Sinn. Wir haben ein Fachverfahren, das eigentlich vielen zur Verfügung stehen sollte, die E-Akte. Wenn Daten in der E-Akte sind, ist die E-Akte so konstruiert, dass man mit einem Admin-Zugang nicht alles herunterladen kann, oder hat die E-Akte dasselbe Risiko wie offensichtlich die Fileserver bei StadtWohn oder dem Land Berlin? Macht es nicht auch Sinn, die E-Akte, wenn sie dann überall eingeführt ist, zu nutzen und Beschäftigte zu ermutigen, Dateien nicht einfach im Fileserver oder auf dem Desktop liegen zu lassen, sondern die Fachverfahren zu nutzen, damit sie vielleicht einen höheren Schutz bieten? Ist das etwas, wo das ITDZ die Beschäftigten und die Verwaltungen unterstützen kann, damit wir kurzfristig besser werden?

Eine Frage, die sich irgendwie schon noch stellt, in Richtung Senat: Manche sagen, die Frage des Mindsets haben wir verstanden. Bei manchen Äußerungen habe ich den Eindruck, vielleicht stimmt das auch doch nicht. Teilt der Senat die Einschätzung von IT-Experten, dass das Verwaltungshandeln in den letzten Jahren mutmaßlich grob fahrlässig ist und war, und dass wir sehenden Auges in diesen Prozess reingegangen sind? Oder würde der Senat immer noch sagen, dass wir Pech gehabt haben und nichts hätten verhindern können?

Vorsitzender Johannes Kraft: Vielen Dank, Herr Ziller! – Wenn wir eine Chance auf qualifizierte Antworten haben wollen, dann sollten wir uns vielleicht in der Zeit, die wir für Fragen in Anspruch nehmen, ein bisschen beschränken. – Herr Kollege Schatz, bitte!

Carsten Schatz (LINKE): Vielen Dank, Herr Vorsitzender! – Ich will gar nicht 15 einzelne Fragen stellen, sondern vielleicht noch mal eine Bitte äußern, die ich auch schon in der letzten Sitzung geäußert hatte und die jetzt hier parasitär aufgegriffen wurde: Das ist die Frage nach der Zeitleiste. – Herr Staatssekretär Hauer! Ich verstehe, dass das Arbeit macht, ich glaube aber, dass das für die Rekonstruktion der Abläufe und für das Lernen daraus für uns alle wichtig ist. Deshalb ist es aus meiner Sicht nicht sinnvoll, das ex post zu machen, weil – das sage ich jetzt als Historiker – ex post Dinge immer verklärt werden, also im Nachhinein. Wir müssen in dem Moment, in dem wir Informationen bekommen – und das wird die Verwaltung auch machen, es gilt das Schriftlichkeitsprinzip –, festhalten: Welche Informationen sind angekommen? An wen wurden sie weitergegeben? Wer hat welche Entscheidung getroffen, und welche Folgen hatten die? – Das muss, finde ich, sehr zeitnah aufgeschrieben werden, bevor neue Erkenntnisse den Stand überschreiben und man gar nicht mehr dazu kommt, feststellen zu können: Hat man an der Stelle vielleicht einen Fehler gemacht? – Ich will es mal deutlich sagen: Mir geht es gar nicht darum, wer welchen Fehler gemacht hat, sondern darum, einen Prozess anzuschauen und im Nachhinein zu prüfen, wie wir Prozesse besser organisieren können, damit andere Ergebnisse herauskommen.

Man muss hier einfach mal sagen: Es hat einen Angriff gegeben, der lange Zeit – und in der Digitalisierung sind sieben Tage eine lange Zeit – unbemerkt blieb. Man hat auch den Eindruck, dass die Strukturen des Landes nicht wirklich ausreichend darauf vorbereitet waren. Ich glaube, da muss man dem auch gerecht werden, was Frau Plattner sagte: Das Wesen einer Krise ist, dass man alle zwei, drei Tage neue Informationen bekommt, und, wie gesagt, eine Dokumentation muss immer auf dem Kenntnisstand passieren, den man aktuell hat. Vielleicht macht es Sinn, wenn Sie noch zwei, drei Kolleginnen oder Kollegen hinzuziehen, die sich nur dieser Aufgabe widmen und gar nichts weiter machen. Das ist bei den vielen Stäben, glaube ich, gar nicht mehr das Problem.

Dann würde ich gerne noch eine andere Sache aufgreifen, die auch Frau Plattner sagte, nämlich: Die Angreifer hatten es zu leicht. Das ist in der Tat ein Punkt, über den man politisch im Nachhinein noch mal reden muss. Herr Schulze hat darauf hingewiesen: Als wir hier den Nachtragshaushalt 2024 miteinander beredet haben, war das Thema, dass Sie damals 12 Millionen Euro aus dem Betrieb des Landesnetzes genommen haben und 2 Millionen Euro aus der Eindringungserkennung. Ich finde, darüber kann man doch jetzt nicht einfach hinweggehen. Ich finde, diesen Punkt muss man schon noch mal ansprechen, und wir müssen uns das auch angucken. Deshalb möchte ich die Fragen, die gestellt worden sind, auch beantwortet haben: Welche ursprünglich vorgesehenen Maßnahmen zur Eindringungs- und Anomalieerkennung wurden infolge dieser Haushaltsentscheidung verschoben, reduziert oder nicht umgesetzt? – Das möchte ich wissen. Welche wären wichtig gewesen für die frühere Erkennung des Angriffes? Kann der Senat ausschließen, dass diese Kürzungen die Fähigkeit zur frühzeitigen Erkennung beeinträchtigt haben? – Ich glaube, nein.

Zur Chronologie habe ich etwas gesagt, und ich glaube, die brauchen wir dringend. Ich habe auch gelernt, dass wir mittlerweile eine AO in der SenMVKU haben, oder wie auch immer sie jetzt heißt. Wir haben den IKT-Notfall-Krisenstab. Wir haben jetzt eine neue Steuerungs-

gruppe. Es gibt eine Koordinationsgruppe, von der Frau Plattner vom BSI gesprochen hat. Ich habe Angst, Herr Hauer, dass Sie nur in Runden sitzen. – [Zuruf] – Auch in Ausschüssen. Vielleicht können Sie uns dazu auch noch mal Auskunft geben, denn ich glaube, dass es nicht wichtig ist, sich am Ende zu Tode zu koordinieren, sondern zu gucken, dass Entscheidungen getroffen werden, und möglichst aus einer Hand. – Vor dem Hintergrund will ich mich vielleicht auch noch mal zu der Bemerkung hinreißen lassen: Ich glaube, dass das, was in einem Bezirk gerade gemacht wird, massive argumentative Grundlagen dafür legt, die Selbstverwaltung der Bezirke zu beschneiden. Daran sollte kein Bezirk ein Interesse haben und deshalb sehr schnell mit dem Land kooperieren, damit wir hier zu einer Lösung kommen. Das finde ich extrem unverantwortlich, was hier passiert.

Last but not least habe ich noch eine Frage, zu der hier schon mehrfach gesprochen wurde. – Ich habe den Kollegen Schulze übrigens, Herr Kroll-Peters, nicht so verstanden, dass er dazu aufrief, dass alle diese Daten herunterladen sollen. – Mich interessiert es auch datenschutzrechtlich; vielleicht kann Frau Kamp noch mal etwas dazu sagen: Wie ist denn jetzt, auch aus datenschutzrechtlicher Sicht, das Herunterladen dieser Daten? – Da sind ja enorm sensible Daten dabei, zumindest nach dem, was wir wissen. Wie kann das beispielsweise auch durch die Behörden ordnungsgemäß passieren, und auf welcher Rechtsgrundlage? – Vielen Dank!

Vorsitzender Johannes Kraft: Vielen Dank! – Das hat mit der Zeit jetzt nicht so super geklappt. – Herr Vallendar, bitte schön!

Marc Vallendar (AfD): Ich werde mich etwas kürzer fassen. Ich habe noch eine Nachfrage, beziehungsweise wurde die Frage nicht beantwortet, die sich auf die Löschfristen hinsichtlich Personal- und Gesundheitsdaten beim Senat bezog: Wie sind die geregelt, wie lange sind die gespeichert und warum waren Sachen wie PCR-Testergebnisse auf Ihren Servern gespeichert? – Corona ist ja nun schon eine Weile her. Wenn Sie das nicht beantworten können, würde ich in dem Zusammenhang gleichzeitig die Datenschutzbeauftragte des Landes Berlin fragen, ob ihre Behörde in den letzten fünf Jahren bei SenStadt oder SenMVKU die Löschkonzepte für Personal- und Gesundheitsdaten überprüft hat, und mit welchem Ergebnis.

Dann hätte ich noch eine Frage an Frau Dr. Borelli hinsichtlich der Migration von SenStadt und SenMVKU zum ITDZ: Wie lange wird die Migration in etwa dauern? Deckt der Nachtragswirtschaftsplan von 2026 die Kosten dafür vollständig ab, oder bräuchte es noch mehr finanzielle Mittel? – Vielen herzlichen Dank!

Vorsitzender Johannes Kraft: Vielen Dank! – Jetzt haben wir doch relativ viele Fragen gesammelt und auch relativ viele Adressaten wurden angesprochen. Meine Vermutung ist, dass wir das in den kommenden zehn Minuten nicht schaffen werden. Deshalb stelle ich schon mal vorsorglich die Frage: Besteht Widerspruch dagegen, dass wir um zehn Minuten verlängern? – Das ist nicht der Fall. Dann würden wir so verfahren und ich darf fragen, wer als Erster antworten möchte. – Herr Staatssekretär Hauer, bitte schön!

Staatssekretär Florian Hauer (Skzl): Genau, ich würde anfangen und versuchen, so viele der Fragen wie möglich zu beantworten. Gerade habe ich noch eine Nachricht gelesen, die passt auch zum Thema heute im Kontext Lichtenberg. Ich fange aber mit der letzten Frage an, die ich relativ einfach beantworten kann und da vielleicht noch mal ein bisschen Aufklärung bringen kann in der Frage: Welche Daten sind überhaupt abgeflossen?

Herr Abgeordneter Vallendar! Sie fragten nach den Löschfristen und sprachen PCR-Tests und Ähnliches an. – Nach meinem Verständnis – und da können mich die Kollegen aus den betroffenen datenführenden Verwaltungen korrigieren, wenn ich da einen Denkfehler habe – sind diese Daten abgelegt gewesen und von den persönlichen Laufwerken der Mitarbeiter gestohlen worden. Die haben auf ihren Laufwerken Dinge abgelegt. Es spricht einiges dafür, dass sie ihre PCR-Tests sowie Geburtsurkunden ihrer Kinder abgelegt haben, dass sie dort ihre eigenen Bewerbungsunterlagen abgelegt haben, weil sie sich vielleicht woanders hin oder im Haus neu beworben haben. Es gibt zumindest eine gewisse Plausibilität, dass das so gewesen sein könnte. Dann würde sich die Frage nach den Löschfristen erübrigen, weil es dann nicht im Datenbestand der Personalabteilung gewesen wäre, sondern auf den persönlichen Laufwerken. Das ist ein Erklärungsversuch, ein Erklärungsansatz, der in meinen Augen eine gewisse Plausibilität hat, aber das können die datenführenden Behörden sicherlich bestätigen. Wenn es so wäre, würde es sich vielleicht erklären, warum die Daten nicht gelöscht sind, wenn es auf persönlichen Laufwerken abgelegt war.

Herr Ziller! Sie hatten auch noch mal nach den Ressourcen der BAO gefragt. – Herr Schatz! Sie fragten: Wie arbeiten die verschiedenen Strukturen und Stäbe nebeneinander, nicht, dass wir uns am Ende zu Tode koordinieren und dort Reibung haben? – Das ist eine berechtigte Frage. Deswegen würde ich, bevor ich die Frage von Herrn Ziller beantworte, die Frage von Herrn Schatz beantworten, wie jetzt die Strukturen sind. – Ich habe eingangs dargestellt, wie unsere Herangehensweise ist und wo unsere Anknüpfungspunkte sind, was die Daten angeht. Wir haben einmal die datenführenden Stellen, die ihre Daten gesichert und isoliert haben, von denen Sie wissen, dass sie abgeflossen und kopiert worden sind. Die haben allein mit Blick darauf eine BAO eingerichtet, weil damit ganz viele Fragen zusammenhängen, die Risikobewertung, aber auch die Frage: Wie gehen wir mit Beschäftigten um, die betroffenen sind? Wie werden sie informiert? Wie wird diesen Beschäftigten geholfen?

Ich gehe mal einen Punkt zurück, weil ich das in meinem Eingangsstatement gesagt hatte, zur Struktur: Der eine Strang bezieht sich auf die Sicherung des Landesnetzes. Das ist das, was seit Mitte August installiert ist. Das ist der IKT-Notfallstab unter Leitung des Landesbevollmächtigten für Informationssicherheit, der diese Aufgabe hat. Das ist seine Kernaufgabe. Das ist der eine Handlungsstrang. Daneben haben wir das Thema Schadensmanagement. Wie gehen wir mit den abgeflossenen Daten um? Wie können wir sie sortieren? Wie können wir sie so schnell wie möglich analysieren? Wie können wir Risikobewertungen vornehmen? Wie können wir Betroffene informieren? Das ist der zweite Handlungsstrang, den wir gerade haben. Da haben wir zum einen die besagte BAO bei SenMVKU. Wir haben die BAO, die ich genannt habe, beim LKA, die aber zusätzlich die Aufgabe hat, selbstverständlich auch als Strafermittlungsbehörde für die Staatsanwaltschaft zu fungieren. Das ist auch eine separate Aufgabe. Dann sind wir, als diese Datenmenge klar wurde, die auf uns zukommt, und auch diese technischen Herausforderungen, die ich eingangs beschrieben habe, dass es rein technisch und organisatorisch anspruchsvoll ist, zu dem Ergebnis gekommen, dass es sinnvoll ist, zusätzlich zu den beiden Einrichtungen eine koordinierende Steuerungseinheit einzurichten. Die kann nur in der Senatskanzlei sein, weil sie zentral aus der Mitte heraus koordiniert. Da geht es darum, dass wir all diese Dinge, die jetzt mit Blick auf Datenanalyse, Datenbewertung, Risikoabschätzung und vor allem Informations- und Kommunikationskanäle auf uns zukommen, irgendwo zentral bündeln, aussteuern und auch ein Controlling vorhalten müssen und Ähnliches. Das kann, wie gesagt, nur in der Senatskanzlei sein. Deswegen ist es bei uns unter meiner Führung und Verantwortung eingerichtet.

Das soll aber nicht die Arbeit des IKT-Notfallstabes ersetzen. Ich sehe da eine klare Abgrenzung, auch wenn es natürlich Überschneidungen gibt, auch personell. Diese Steuerungseinheit hat die Aufgabe, diesen Prozess zu managen und zu forcieren, den ich eingangs beschrieben habe, dass wir die Daten so schnell wie möglich identifizieren, analysieren, eine Risikobewertung vornehmen, die notwendigen Maßnahmen ergreifen und die Betroffenen informieren und beraten. Das muss getan und koordiniert werden, weil es verschiedene Stellen betrifft, insbesondere die beiden Senatsverwaltungen als datenführende Behörden, die am Ende diejenigen sind, die in den meisten Fällen nur eine erste inhaltliche Prüfung durchführen können. Wir brauchen an einem bestimmten Punkt aber auch das LKA, um zu gucken, ob Personen und Objekte gesondert und besonders geschützt werden müssen. Wir haben die Anfragen der Bundesbehörden. Das hatte vorhin Frau Plattner auch gesagt, was die Bundesbehörden tun. Die sind wiederum auf Informationen und Zulieferungen von uns angewiesen, und an einer Stelle müssen die Informationen zusammenfließen. Das kann nur in der Senatskanzlei sein. Wir haben entschieden, dass das in der Senatskanzlei sein soll und dass wir das machen, um dort die notwendigen Informationsflüsse zu gewährleisten. Das ist die Idee. Das haben wir veranlasst, und das muss jetzt mit Hochdruck betrieben werden.

Zu der Frage, was bei SenMVKU und SenStadt an Personal eingesetzt wird, können die Kollegen selbst etwas sagen, zumindest für diese besonderen Einrichtungsstäbe wie BAO und die Taskforce. Ich habe eingangs beschrieben, was auf uns zukommt, und wenn wir am Ende all diese Informationen und Dateien sichten und bewerten müssen, deswegen kann ich Ihre Frage nicht beantworten, gehe ich davon aus, dass es am Ende nur mithilfe aller Kolleginnen und Kollegen in den betroffenen Verwaltungen funktioniert, zumindest all denen, die in den zuständigen betroffenen Fachreferaten, Sachgebieten und Abteilungen arbeiten. Die müssen sich dort alle einbringen – Herr Herz hat es gerade beschrieben, Stichwort Mindset –, und das werden sie auch, und das wird uns allen viel abverlangen, aber das muss jetzt geleistet und geliefert werden. – Deswegen, Herr Schatz, kann es zu Überschneidungen führen, und es wird auch Koordinierungsbedarf zwischen den Stäben und Abgrenzungsschwierigkeiten geben. Es ist wie immer bei solchen Stäben. Ich glaube aber, dass wir das so eng definiert und die unterschiedlichen Aufgaben und Handlungsstränge auch voneinander abgegrenzt haben, dass sich das in Grenzen hält beziehungsweise handhabbar ist.

Zur Frage zum Haushalt, die Sie gestellt haben: Ich bitte da um Verständnis. Ich kann Ihnen diese Zahlen gegenwärtig nicht nennen. Ich weiß sie einfach nicht. Zu dieser konkreten Frage, die Sie gestellt haben – was das für die IT in den einzelnen Ressorts zahlenmäßig bedeutet hat, ob es dahingehend kausal war, dass bestimmte Investitionen und Vorkehrungen nicht getroffen werden konnten, ob wiederum dieses Unterlassen kausal war für den jetzt stattgefundenen Angriff –, kann ich Ihnen heute nichts sagen. Ich glaube, dafür brauchen wir am Ende keine Historiker – das ist sicherlich auch hilfreich –, aber das können wir erst ex post dann beantworten.

Zu Ihrer Frage zur Zeitleiste und so weiter: Ich habe eben auch wieder das beschrieben, was wir jetzt tun. Wir brauchen dafür wirklich alle Ressourcen. Es ist nicht so, dass wir drei, vier Kolleginnen und Kollegen haben, die das mal eben nebenher leisten können. Es ist bei uns schon schwierig, dass wir solche Gremiensitzungen wie heute vorbereiten – beziehungsweise bereiten wir sie am Ende kaum vor, weil wir die Ressourcen dafür nicht haben. Unser Fokus liegt im Moment auf dem akuten Krisenmanagement.

Gleichwohl werden wir versuchen, Ihnen diese Zeitleisten und Informationen so schnell wie möglich zukommen zu lassen. Ich habe gesagt, das ist ein evolutionäres Dokument, was die Sache nicht einfacher macht, weil es so dynamisch ist. Ich verstehe aber Ihr Bedürfnis nach laufender Information. Das ist auch mein Anspruch. Ich hoffe, das konnten wir zeigen, dass wir das fortlaufend tun. Es ist völlig berechtigt, und wir versuchen, Sie dort bestmöglich in die Lage zu versetzen, dass Sie das hier parlamentarisch begleiten und kontrollieren können. Ich habe auch gesagt, dass auch für mich der Austausch sehr sinnvoll ist, gerade auch diese Gespräche, die wir führen, wenn wir mit den Sprecherinnen und Sprechern sprechen. Das ist für mich auch eine wichtige Erkenntnisquelle. Das hilft ja auch.

Noch einmal – das ist auch das, was Frau Plattner eingangs sagte: Wir Repräsentanten Berlins sitzen im Moment alle in einem Boot, und wir kommen auch nur gemeinsam aus dieser Krise wieder heraus. Alleine auch in diesem Sinne haben wir den Anspruch, Sie bestmöglich informiert zu halten. – Vielen Dank!

Vorsitzender Johannes Kraft: Vielen Dank! – Dann möchte Staatssekretär Slotty ergänzen. – Bitte schön!

Staatssekretär Alexander Slotty (SenStadt): Danke, Herr Vorsitzender! – Ich möchte vielleicht noch mal an den letzten Punkt hier anknüpfen: Heute sind ganz viele Fragen gestellt worden, die ich selber auch habe. Die sind nach so kurzer Zeit einfach noch nicht vollumfänglich beantwortbar. Es bringt, glaube ich, auch nichts, wenn man jetzt bei allem anfängt zu mutmaßen. Wir sollten den Weg, den wir im Rahmen der Aufklärung eingeschlagen haben, konsequent gehen und die Kräfte darauf konzentrieren.

Ich will mit dem Blick auf die Frage, ob im Rahmen von Haushaltsaufstellungen oder Haushaltsplanbeschlüssen so viel gespart worden ist, dass die Infrastruktur am Ende darunter gelitten hat, sagen: Ich bin schon seit Beginn der Legislaturperiode dabei. Schon im Dezember 2021, noch in der anderen Koalition, war ich auch damit konfrontiert, in dreistelligem Millionenumfang – seinerzeit als Staatssekretär für Bildung – einsparen zu müssen. Deswegen wage ich jetzt mal die Aussage heute: Wahrscheinlich lässt sich der Zustand einer IT-Infrastruktur in einem Bundesland nicht nur auf die letzten 24 oder 36 Monate zurückberechnen, zurückführen, sondern ich glaube, bei einer IT-Infrastruktur, die hier in Berlin über zwei Jahrzehnte hinweg entsprechend gewachsen ist, gab es sicher in der Vergangenheit durchaus auch Fehlentscheidungen, die dazu geführt haben, dass man heute dort steht, wo man steht.

Für mich war es mit Beginn dieser Krise wichtig, erst einmal zu erfahren, wie es um unsere Hardware und Software steht. Zu dieser Aussage stehe ich auch, weil ich mich auf das Wort meiner Kolleginnen und Kollegen absolut verlassen kann: Unsere Hardware und Software waren auf dem aktuellen Stand, alles war geupdatet, und wir haben auch die Vorgaben des BSI berücksichtigt und eingehalten. Insofern haben wir mit Blick auf dieses IT-Sicherheitslevel, glaube ich, das eingehalten, was natürlich mindestens einzuhalten ist.

Ich glaube im Übrigen, der besagte IT-Sicherheitsexperte, der sich nach zwei Beratungen in den zurückliegenden Jahren im Land Berlin geäußert hat, hat nicht von fahrlässigem Verhalten mit Blick auf die IT-Infrastruktur in Berlin gesprochen, sondern ausschließlich mit Blick auf das Speichern von KRITIS-Informationen, so habe ich das verstanden. Dazu will ich vielleicht auch noch mal sagen: Wir wissen aktuell noch nicht vollumfänglich, was für

Daten, die möglicherweise den Bund betreffen, abgeflossen sind. Ich kann Ihnen aber zum Beispiel aus der Welt der Baupläne sagen: Wenn eine Bundesbehörde beziehungsweise das BBR oder die BImA, die für den Bund bauen, bei der Senatsverwaltung für Stadtentwicklung, Bauen und Wohnen eine Baugenehmigung beantragen, dann muss der Bund Unterlagen entsprechend klassifizieren. Das heißt, der Bund sagt, ob diese Unterlage nicht klassifiziert ist, ob sie VS-NfD-klassifiziert, Geheim oder anders klassifiziert ist. Beispielsweise sind jetzt in der Öffentlichkeit schon Unterlagen erwähnt worden, irgendwelche Baupläne, bei denen es sich gar nicht um Baupläne handelt, die zum Beispiel im Rahmen von Genehmigungsverfahren bearbeitet wurden, die auch gar keine Baupläne im eigentlichen Sinne sind, durch die sich gar keine Rückschlüsse auf die Beschaffenheit oder Konstruktion des Gebäudes zwingend ziehen lassen. Das können manchmal auch Darstellungen von Plangebieten aus Bebauungsplänen und ähnlichem sein. Diese Dokumente sind zum Beispiel nie klassifiziert, nie eingestuft worden, insofern war das bei denen in Ordnung, falls sie auf Laufwerken lagen.

Ich kann Ihnen auch sagen, weil die Frage schon vor geraumer Zeit aufgetaucht ist: Schon lange vor dieser Krise haben beispielsweise die Bauunterlagen für den Neubau des Bundesnachrichtendienstes bei uns nie elektronisch vorgelegen. Diese Unterlagen haben sich immer in 24 Stunden bewachten Baubaracken auf dem Gelände befunden. Nachdem die Unterlagen von den Bearbeitern schlussendlich gestempelt wurden und die Baugenehmigung erteilt wurde, sind diese Unterlagen beispielsweise wieder vollständig zurück an den Nachrichtendienst gegangen. Das haben wir gar nicht erst in Berlin gespeichert. Alle anderen Bauunterlagen, die beispielsweise die Bundesbehörden betreffen, werden gar nicht elektronisch gespeichert, sondern werden, wenn sie nicht zurückgegeben werden, an vertraulichen, Ihnen jetzt auch nicht bekannten Orten in Berlin physisch abgesichert. Insofern mache ich mir jetzt erst mal, was diesen Bereich Baugenehmigungsverfahren für Dienstgebäude des Bundes betrifft, ehrlicherweise keine großen Sorgen.

Aus der ersten Fragerunde hatte ich vergessen, eine Frage zu beantworten, die wahrscheinlich an den Kollegen Herz und mich gleichermaßen gestellt worden ist. Das eine wissen wir wahrscheinlich alle nicht, nämlich, wie viele Strafanzeigen zwischenzeitlich eingegangen sind. Das wird Ihnen nur das LKA beantworten können. Ich kann Ihnen aber sagen: Bei uns im Hause haben sich bei der eingerichteten Ansprechstelle für Kolleginnen und Kollegen bis zum Wochenende zehn Kolleginnen und Kollegen mit 26 Fragen gemeldet. Es hat sich ein ehemaliger Mitarbeiter unseres Hauses persönlich an mich gewandt, und auch heute hat sich im Laufe des Tages eine Kollegin persönlich an mich gewandt, weil ich den Kolleginnen und Kollegen auch diesen Weg der Kommunikation angeboten habe, dass sie mich auch persönlich kontaktieren können, damit ich mich dann in solchen Fällen darum kümmern kann.

Was die Frage betrifft, wo die Daten abgeflossen sind – gerade die, die der Kollege Hauer gerade noch mal genannt hat, Zeugniskopien, Geburtsurkunden und so weiter, auch Dateien mit personenbezogenen Informationen –: Die müssen nicht zwingend aus unserem Referat, das für das Personalwesen zuständig ist, abgeflossen sein. Wir wissen mittlerweile – unter anderem auch durch die Dateien mit den Klarpasswörtern in unverschlüsselten Worddokumenten –, dass die auf Homelaufwerken lagen, also auf den persönlichen Laufwerken von Mitarbeiterinnen und Mitarbeitern. Es ist also nicht auszuschließen, dass diese Dateien auch an dieser Stelle abgeflossen sind. Das heißt auch, dass für das Speichern dieser Dateien die Dienststelle gar keine Verantwortung hat und über die Speicherung dieser Daten natürlich gar nichts wusste. Das wird sich jetzt aber nach und nach – und, ich gehe auch davon aus,

sehr zeitnah – durch unsere Dienstleister herausstellen, denn wir haben sogenannte Indexdateien beauftragt. Über diese Indexdateien kann dann ermittelt werden: Was ist eigentlich der genaue Ursprung dieser Datei, die jetzt veröffentlicht ist? – Darüber können wir feststellen, von welchem Server, von welchem Laufwerk diese Datei abgeflossen ist, und dann kennen wir auch den genauen Ursprung. Wenn jetzt, wenn wir bei diesem Beispiel bleiben, eine Krankmeldung oder eine Geburtsurkunde von Mitarbeiter XY öffentlich geworden ist, können wir nach diesen Indexdateien feststellen: Hat er das selber auf seinem Laufwerk abgespeichert, oder ist das im Zugriffsbereich des Personalreferats abgeflossen? – Alle diese Fragen, die Sie haben, habe ich auch. Wir sind an der Aufklärung. – Vielen Dank!

Vorsitzender Johannes Kraft: Vielen Dank, Herr Staatssekretär Slotty! – Die von uns vereinbarten zehn Minuten Verlängerung der Sitzungszeit wären jetzt um. Die Frage wäre, wie wir verfahren wollen. Ich würde tatsächlich die Antwortrunde noch fertigmachen, denn es gab auch dezidiert Fragen an Frau Dr. Borelli und Frau Kamp. – Es soll überhaupt nicht unhöflich klingen, aber vielleicht könnten Sie sich wirklich auf die wesentlichen Punkte beschränken, auch weil ich davon ausgehe – das war schon angekündigt –, dass dies nicht die letzte Sitzung zu diesem Thema in dieser Wahlperiode war. Ich gucke noch mal in Richtung der Kollegen. Dann geben wir uns jetzt noch mal zehn Minuten, dann sollten wir aber so langsam zum Ende kommen. – Frau Dr. Borelli, bitte!

Dr. Maria Borelli (ITDZ): Danke schön! – Ich versuche, mich kurzzufassen. Zu der Frage von Herrn Ziller, wie das ITDZ mit dem Thema, vor allem mit diesem Architekturthema umgeht: Das ITDZ Berlin wird jedes Jahr vom BSI zertifiziert. Wir haben alle zwei Jahre eine vollständige Zertifizierung und dazwischen immer eine Zwischenzertifizierung. Seit zehn Jahren machen wir das schon. Wir halten uns sehr konsequent an die Empfehlungen der Auditoren, die uns zertifizieren. Bis jetzt wurden wir immer zertifiziert, immer mit relativ kleinen Findings. Dort, wo die Auditoren ein Finding haben, setzen wir die empfohlenen Maßnahmen um, sodass wir uns sicher sein können, dass unsere Schutzmechanismen alle up to date und State of the Art sind.

Nichtsdestotrotz haben wir noch eine kleine Zahl veralteter Fachverfahren bei uns, End of Life. Dazu müssen Sie wissen: Wir haben seit 2024 ein Projekt zur Eliminierung der End-of-Life-Fachverfahren laufen. Das läuft relativ erfolgreich in Zusammenarbeit mit den Kunden, sodass ich sagen kann: Die Anzahl der wirklich hoffnungslos veralteten Fachverfahren ist relativ gering. Da gehen wir wie folgt vor: Wir bieten den Kunden eine Lösung an, wenn das Verfahren unbedingt noch aufrechterhalten sein muss, sodass das Verfahren komplett auf dezidierten Systemen und isoliert von den anderen Systemen betrieben werden kann, damit im Falle eines erfolgreichen Angriffs die anderen Verfahren nicht in Mitleidenschaft gezogen werden können. Das hört sich gut an, ist aber sehr kostspielig, und das ist die Stelle, an der wir regelmäßig in den Dissens mit unseren Kunden geraten, wer diese Kosten finanzieren soll. Aber das ist aktuell unsere Herangehensweise. Was ich ansonsten machen kann, ist, dann den Vertrag zu kündigen, was nicht weniger dramatisch wirkt.

Zu der Frage, ob die Hardware sicher ist: Das Finding, dass jetzt nur aus Filesystemen heruntergeladen wurde, legt nahe, dass die Hardware nicht betroffen ist, ausschließen kann man das aber natürlich nie. Fakt ist: Wir konnten bis jetzt nichts feststellen.

Zu der Frage, wie das ITDZ unterstützen kann und wie das ITDZ eingebunden ist: Das ITDZ Berlin ist von Anfang an dabei gewesen, schon bei den ersten präventiven Untersuchungen, die letztendlich dazu geführt haben, dass wir das Datenleck entdeckt haben. Wir konnten für die Systeme, die in unserer Betreuung sind, also für unsere eigenen Systeme und für die Systeme unserer Kunden, die bei uns in Betrieb sind, relativ schnell diese forensische Software installieren und die Scans durchlaufen lassen. Ich glaube, die Maßnahme wurde am 17. August angeordnet, und wir waren am 19. August schon mit 90 Prozent fertig. Die restlichen 10 Prozent wurden später gemacht, aus zwei Gründen: Zum einen betraf das Verfahren, die relevant waren, und für solche Verfahren gibt es mit der Innenverwaltung ein gesondertes Freigabeverfahren für Änderungen in diesen Systemen. Daran haben wir uns gehalten, und deswegen hat sich die Installation der forensischen Software dort ein bisschen verzögert. Zum anderen ging es um ein ITDZ-Verfahren, das dazu dient, Datenaustausch über das Internet zu ermöglichen. Es liegt in der Natur der Sache, dass wir genau bei diesen Verfahren länger geschaut und intensiver untersucht haben. Ansonsten waren wir mit diesen Maßnahmen relativ schnell fertig. Der Grund dafür ist, wie ich gesagt habe, dass wir BSI-zertifiziert sind, das heißt, wir haben in unserem Haus Prozesse für solche Fälle etabliert. Das heißt, wenn ein IKT-Notfall eintritt, wissen alle, welche Rolle sie haben, welche Verantwortung sie haben, wie die Kommunikationswege sind und was sie zu tun haben. Deswegen ist es möglich gewesen, innerhalb der Infrastruktur, die vom ITDZ Berlin betrieben wird, relativ schnell diese forensische Software zu installieren und dann zu dem Ergebnis zu kommen, dass aktuell nichts betroffen ist.

Wie ist das ITDZ in den allgemeinen IKT-Notfallstab eingebunden? – Aktuell agieren wir reaktiv, das heißt, wir reagieren auf explizite Anweisungen des Landesbevollmächtigten. Was wir bis jetzt gemacht haben: Wir haben bei den Änderungen der Passwörter unterstützt. Für die Passwörter im Clientsystem, die bei uns in der Betreuung sind, haben wir auch innerhalb von zwei Tagen alle Passwörter geändert. Wir haben in allen Fachverfahren, die bei uns im Betrieb sind, die administrativen Passwörter bereits geändert, bis auf 21 Verfahren, wo das nicht möglich ist, weil das Passwort fest in dem Quellcode verdrahtet ist, es ist also nur mit der Unterstützung des Softwareherstellers möglich, das zu tun. Wir sind im Austausch mit dem entsprechenden Verantwortlichen für das Fachverfahren und auch mit der IKT-Sicherheit, wie man da jetzt weiter vorgeht. Bei der Erstellung neuer Zertifikate haben wir bei allen unterstützt. Wir sind in der Lage, pro Tag 800 neue Zertifikate zu erstellen, wenn es sein muss. Wir haben zum Beispiel alleine für die Telefonie über 30 000 Passwörter geändert. Das bedeutet auch für uns mehr Aufwand. Wir sind dabei, diese Kosten zu sammeln, um zu schauen, was im Anschluss mit diesen Kosten passiert.

Zu unserer Einbindung in den IKT-Notfallstab muss ich sagen: Ich kann nur empfehlen, dass das Berlin-CERT besser eingebunden wird. CERT heißt Cyber Emergency Response Team. Wie der Name sagt, sitzen dort die Experten, die wissen, wie man in solchen Fällen zu reagieren hat und welche Maßnahmen zu treffen sind. Aktuell wird dieses Team aber nur als Ersteller für Lageberichte eingesetzt. Auch die Empfehlungen, die das Team in die Lageberichte schreibt, werden nicht alle wahrgenommen. Es ist dem CERT und auch unserem CDC – Cyber Defense Center – untersagt, andere Domänen zu untersuchen, außerhalb der Domänen, die sowieso in der Verantwortung des ITDZ Berlin sind, obwohl wir dort die Ressourcen und Kapazitäten hätten.

Auch die Einbindung in die Kommunikation ist schwierig. Das Berlin-CERT bekommt zum Beispiel von den Landesbetrieben sehr viele Anfragen; es ist ja auch die Anlaufstelle für solche Fragestellungen. Aber die Informationen können nur nach Freigabe durch die IKT-Sicherheit weitergegeben werden, was zu Verzögerungen bei der Informationsweitergabe und entsprechend zu Verärgerung bei den Landesbetrieben und bei anderen unserer Kunden führt. Zum Beispiel die IoC, die Frau Plattner erwähnt hat, diese Hinweise auf Kompromittierung, wurden erst letzte Woche zur Verfügung gestellt, weil erst letzte Woche die Freigabe da war. Auch die Kommunikation im CERT-Verbund, des Landes-CERT-Verbunds mit den CERTs von anderen Bundesländern, erfolgte erst nach der Freigabe durch die IKT-Sicherheit, was auch für einen Erfahrungsaustausch in diesem Zusammenhang nicht wirklich förderlich ist. Auch weitere Aufträge haben wir erst sehr spät bekommen, zum Beispiel wurde die Überwachung des Darknet, was beim CERT eigentlich zum täglichen Brot gehört, erst letzten Donnerstag erteilt. Wir, das ITDZ Berlin, leiden mit dem Rest des Landes darunter, und wir wünschen uns auch, dass so schnell wie möglich die Aufarbeitung beendet werden kann. Wir können an der Stelle mehr unterstützen, und ich kann nur appellieren, dass die Expertise, die wir im Berlin-CERT und im CDC haben, mehr genutzt und auch entsprechend das Expertenwissen eingesetzt wird.

Zu Ihrer Frage, ob wir jetzt einen Auftrag haben: Haben wir nicht. Wir haben aktuell keinen Auftrag, bei Ihnen in der Verwaltung oder in den Bezirken zu unterstützen. Wir haben einige, die uns um Hilfe gebeten haben. Ich hatte heute mit der Gesundheitsverwaltung ein Gespräch darüber, wie wir sie unterstützen können, ihre Systeme zu härten, schneller die Migration in das Berliner Landesnetz zu bewerkstelligen, damit sich auch ihre Sicherheitslücken schließen, aber einen eindeutigen Auftrag haben wir nicht.

Zu der Frage nach der digitalen Akte: Ja, auch die digitale Akte wurde im Rahmen der forensischen Untersuchung mit der Software untersucht. Es konnte dort nichts festgestellt werden. Die digitale Akte ist aber heute noch nicht richtig für die Kommunikation zwischen Behörden ertüchtigt. Jeder –

Vorsitzender Johannes Kraft: Frau Dr. Borelli, Entschuldigung, wenn ich Sie unterbreche! Wir haben jetzt das Ende der Sitzungszeit erreicht. Ich will Sie gerne noch ausreden lassen, aber vielleicht können Sie –

Dr. Maria Borelli (ITDZ): Ja! Ich bin schon fast fertig. – Die digitale Akte ist in dem Sinne nicht betroffen, weil jeder seine eigenen Mandanten hat, eine Kommunikation zwischen Mandanten findet also noch nicht statt.

Die letzte Frage war, wann die Migration von SenStadt und SenMVKU geplant ist. Die ist nicht geplant, weil wir aktuell noch mit der IKT-Steuerung über den Vertrag zu dem Projekt OneIT 2027 verhandeln. Die Verantwortung dafür soll komplett vom ITDZ übernommen werden, aber wir haben noch keine Einigung über die genauen Modalitäten. Insofern haben wir eine Planung für den Rollout des BerlinPC für dieses und das kommende Jahr noch nicht. Dazu muss die Frage der vertraglichen Bedingungen und Finanzierung geklärt werden. – So, jetzt bin ich fertig.

Vorsitzender Johannes Kraft: Vielen Dank! – Jetzt möchte Staatssekretär Hauer abschließend noch einen Satz sagen, und dann würden wir den Tagesordnungspunkt verlassen. –

[Zuruf] – Die Sitzungszeit ist vorbei. Noch mal: Meine Vermutung wäre, dass wir uns gleich dazu verständigen werden, dass es eine weitere Sitzung gibt, und zwar in naher Zukunft. – Frau Kamp, aus zehn Minuten wurden 20 Minuten, jetzt werden es noch mal zwei Minuten. Meine Erfahrung ist, dass zwei Minuten nicht ausreichen werden. Frau Kamp, gibt es Dinge, die nicht bis kommenden Montag warten können? – Dann hätten Sie gerne kurz das Wort.

Meike Kamp (Berliner Beauftragte für Datenschutz und Informationsfreiheit): Ich gehe davon aus, dass öffentliche Stellen im Rahmen ihrer gesetzlichen Aufgaben auch aus dem Darknet Daten herunterladen können, um insbesondere IT-Sicherheitsanalysen durchzuführen, die dringend notwendig sind. Wenn wir über Individuen sprechen – deswegen würde ich es gerne sagen –, möchte ich generell sagen: Nur, weil Daten öffentlich geworden sind, heißt das nicht, dass man die ohne Weiteres als Privatperson für irgendwelche anderen Zwecke weiter verwenden darf. Zur Strafbarkeit kann ich mich nicht äußern, das ist nicht meine Aufgabe, aber datenschutzrechtlich gibt es hier kein Jedermannsrecht. Das wollte ich einmal generell gesagt haben.

Vorsitzender Johannes Kraft: Vielen Dank für diesen zweiten praktischen Hinweis in dem Zusammenhang! – So, jetzt Florian Hauer, bitte!

Staatssekretär Florian Hauer (Skzl): Danke! – Frau Kamp, vielen Dank auch noch mal für diesen Hinweis. Ich glaube, das war ein wichtiger Hinweis für uns, aber auch für etwaige andere Adressaten, die dann keinen gesetzlichen Auftrag zur Nutzung dieser Daten haben, wie sie damit umgehen sollten oder nicht umgehen sollen.

Ich wollte nur noch einen Satz zu dem sagen, was Frau Dr. Borelli gesagt hat: Wenn Sie das Gefühl haben, dass das ITDZ an der Stelle noch mehr einbringen könnte, und Sie das Gefühl haben, es hakt irgendwo in der Kommunikation, weil die Stellen, die dort wirklich täglich und nächtlich daran arbeiten, Ihnen nicht schnell genug Rückmeldung geben, Sie aber das Gefühl haben, das wäre wichtig, dann rufen Sie mich bitte direkt an. Sagen Sie es mir, dann können wir das veranlassen. Das war mir wichtig in dem Zusammenhang, dass wir dann einfach miteinander kommunizieren. – Danke!

Vorsitzender Johannes Kraft: Vielen Dank! – Dann beenden wir jetzt diesen Tagesordnungspunkt. Meine Vermutung wäre, wir schließen ihn nicht ab. Sehe ich das richtig? – Ich sehe zustimmendes Nicken. Da es den Wunsch gab, die wichtige Debatte hier fortzusetzen, würde ich an dieser Stelle versuchen, dass wir jetzt hier in dieser Runde einen Termin finden. Da vermutlich nur die kommende Woche noch infrage kommt, wäre der Vorschlag, das am Montag zur selben Zeit zu machen, also heute in einer Woche. – Herr Kollege Schatz!

Carsten Schatz (LINKE): Ich bezweifle, dass wir in einer Woche schon viele neue Dinge wissen. Sicherlich wird es weitere Dinge geben, aber ich glaube, nicht in dem Maße, wie wir das vielleicht brauchen, um weiter diskutieren zu können. Da der Ausschuss so lange im Amt ist, bis ein neues Abgeordnetenhaus sich konstituiert, was meines Wissens am 29. Oktober passieren soll, ist mein Vorschlag, zwei Termine heute hier festzulegen, nämlich den 28. September – das ist heute in drei Wochen –, und dann noch mal drei Wochen später, das müsste im Oktober sein. Ich glaube, dann ist genug Zeit dazwischen, dass die Verwaltung entsprechend arbeiten kann, wir dann über neue Stände hier diskutieren können, vielleicht irgendwann auch mal die Zeitleiste bekommen und dann tatsächlich so eine Aufarbeitung

hinkriegen können, mit der die Kolleginnen und Kollegen, die ab dem 29. Oktober hier die Verantwortung für unsere schöne Stadt tragen, weiterarbeiten können.

Vorsitzender Johannes Kraft: Können wir gerne so machen. Ich hatte es so verstanden, dass es doch einen dringlicheren Gesprächsbedarf gibt. – Herr Vallendar, bitte!

Marc Vallendar (AfD): Ich möchte dem Vorschlag der Linkspartei zustimmen. Ich halte es auch für zu früh, wenn wir uns jetzt nächste Woche Montag wieder treffen, zumal wir alle noch voll im Wahlkampf sind. Das heißt, ich halte es tatsächlich – auch für den Kenntnisstand, der noch ein bisschen mehr sein sollte, als er es jetzt schon war – für angezeigt, dass wir die Sondertermine nach die Wahl legen. Ich würde sagen, es reicht jetzt vielleicht erst mal ein Termin, und dann können wir uns immer noch in der Sondersitzung auf einen zweiten Termin einigen, wenn das erforderlich wird.

Vorsitzender Johannes Kraft: Gut! Das war jetzt also kein Widerspruch. Der Vorschlag vom Kollegen Schatz ist der 28. September, das wäre heute in drei Wochen, und als Reservetermin für den Hinterkopf gilt der 19. Oktober. Gibt es etwas dagegen einzuwenden? – Herr Matz, bitte!

Martin Matz (SPD): Da der 19. Oktober in die Herbstferien fällt und die Präsidentin, glaube ich, dort üblicherweise keine Ausschusssitzungen ansetzt, ist der Termin, glaube ich, ein bisschen unglücklich gewählt. Den 28. September können wir schon mal vereinbaren; dann kann darauf, wenn erforderlich, der Montag davor, also der 12. Oktober, folgen.

Vorsitzender Johannes Kraft: Vielen Dank für den Hinweis! – Zwischen den Terminen lägen dann zwei Wochen. Wie gesagt, das war erst mal für den Hinterkopf und noch nicht festgesägt, aber ich habe jetzt keinen Widerspruch gegen den 28. September gehört. – Das halten wir mal fest; wir müssen die Sitzung ja auch beantragen. Dann verständigen wir uns in dieser Sitzung, ob es noch eine weitere braucht. Dafür stehen jetzt der 19. Oktober – mit dem Hinweis auf die Ferien – beziehungsweise eine Woche vorher, der 12. Oktober, im Raum. – Dann beenden wir jetzt diesen Tagesordnungspunkt, ohne ihn abzuschließen.

Punkt 4 der Tagesordnung

Verschiedenes

Siehe Beschlussprotokoll.