

Inhaltsprotokoll

Öffentliche Sitzung

Ausschuss für Digitalisierung und Datenschutz

78. Sitzung
28. September 2026

Beginn: 14.02 Uhr
Schluss: 16.22 Uhr
Vorsitz: Johannes Kraft (CDU), stellv. Vorsitzender

Vor Eintritt in die Tagesordnung

Siehe Beschlussprotokoll.

Punkt 1 der Tagesordnung

Aktuelle Viertelstunde

Es liegen keine Fragen vor.

Punkt 2 der Tagesordnung

Bericht aus der Senatskanzlei

Staatssekretär Florian Hauer (Skzl) informiert darüber, dass das Land Berlin bei der Verleihung des European Public Sector Award am 24. September mit dem BärGPT den 2. Platz in der Kategorie „Delivering User-Centric Services at Subnational Level“ gewonnen habe. Er verbinde damit ein großes Dankeschön an die damit befassten Kolleginnen und Kollegen der Senatskanzlei.

Der **Ausschuss** schließt die Behandlung des Tagesordnungspunkts ab.

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)

Vorsitzender Johannes Kraft erinnert daran, dass die Besprechungspunkte bereits in der letzten Sitzung begründet worden seien. – Sollte es zwischenzeitlich notwendig sein, die Öffentlichkeit auszuschließen, bitte er die Verwaltung um einen entsprechenden Hinweis.

Staatssekretär Florian Hauer (Skzl) erklärt eingangs, er werde sich in seinen Ausführungen auf die Entwicklungen der vergangenen drei Wochen beschränken, die sich an seinen letzten Bericht an den Ausschuss angeschlossen hätten, und einen Ausblick geben. – In Bezug auf die akute Gefahrenabwehr seien die forensischen Untersuchungen fortgesetzt worden. Die Sensorik sei in der Breite und in der Tiefe weiter ausgerollt worden, um sicherstellen zu können, dass der Angriff abgeschlossen sei bzw. nicht andauere. Nach wie vor lägen keine Anhaltspunkte dafür vor, dass es nach Mitte August Aktivitäten der Hackergruppe in der Berliner Landes-IT gegeben habe. Ebenso positiv könne festgehalten werden, dass die Wahlen zum Berliner Abgeordnetenhaus hinsichtlich der IT problemlos verlaufen seien. Die Fortschritte in Hinblick auf die forensische Sensorik stimmten ihn zuversichtlich, dass die Forensiker in Kürze einen Abschlussbericht zur Verfügung stellten und in der Folge, wenn sich der Befund, dass es keine Infiltrierung gebe, bestätige, der Notfall für beendet erklärt werden könne.

Zum Umgang mit den gestohlenen und im Darknet veröffentlichten etwa 1,4 Mio. Dateien sei zu berichten, dass es bis heute noch nicht gelungen sei, eine zentrale Erfassung und Sicherung durchzuführen. Das sei auf das langsame Herunterladen aus dem Darknet zurückzuführen. Die erforderliche Risikoanalyse und Bewertung der abgeflossenen Daten müsse daher noch immer anderweitig vorgenommen werden. Die in der letzten Sitzung geschilderte Herangehensweise an die kritische Infrastruktur, die in Teilen von den Datenabflüssen betroffen sei, komme nach wie zum Tragen. Mit Unterstützung des LKA würden die Dateien ausgewertet und risikobasiert priorisiert. Besonders sensibel erscheinende Dateien würden einzelfallbezogen geprüft und analysiert, und zwar mit den datenführenden Behörden. Bei Bedarf würden Maßnahmen daraus abgeleitet. Das Ganze sei ein äußerst aufwendiger, arbeits- und zeitintensiver Prozess. Für eine deutliche Beschleunigung sorgten in diesem Zusammenhang „technische Dinge“, die mit externer Hilfe implementiert würden.

Damit einher gingen die Fragen bezüglich der datenmäßigen Betroffenheit von Beschäftigten sowie Bürgerinnen und Bürgern. Der Senat habe den Anspruch, allen betroffenen Bürgerinnen und Bürgern möglichst zeitnah, verlässlich und umfassend eine Rückmeldung zu geben. Wenn sie von sich aus auf den Senat zukommen wollten, da sie befürchten müssten, dass sie

vom Datenabfluss betroffen seien, hätten sie seit einigen Wochen die Möglichkeit, an den Senat heranzutreten. Er verweise auf die Ansprechstellen der jeweils datenführenden Behörde. In der Senatskanzlei sei vor einigen Wochen zudem eine zentrale Steuerungseinheit geschaffen worden, die die damit verbundenen Prozesse koordinieren und unterstützen solle. Wenn sich Personen bei der Senatskanzlei meldeten, werde versucht, nähere Informationen in Erfahrung zu bringen. Ziel sei es, die Anliegen der Bürgerinnen und Bürger so schnell wie möglich zu bearbeiten. Angesichts der Fülle und der benannten technischen Herausforderungen gestalte es sich schwierig, sämtliche Betroffene zu identifizieren und proaktiv zu informieren. – Zum Umgang mit Datenschutzanliegen und -anfragen könne im weiteren Verlauf etwas gesagt werden.

Auch wenn bald der Zeitpunkt gekommen sein werde, dass der Notfall für beendet erklärt werden könne, bleibe Berlin, wenn nichts an der IT geändert werde, solchen Gefahren weiterhin ausgesetzt. Täglich komme es zu einer Vielzahl von Angriffen auf öffentliche Einrichtungen und Unternehmen, die überwiegend abgewehrt werden könnten. In Anbetracht des technischen Fortschritts sei mit einer Zunahme der Bedrohungen und Angriffe zu rechnen. Die Stichworte in diesem Kontext seien der Einsatz von KI und Quantencomputern. Es gelte sicherzustellen, dass sich das Land Berlin künftig besser gegen IT-Angriffe wehren könne, als das im August der Fall gewesen sei.

Im Zuge des Gefahrenabwehrmanagements habe erst einmal erfasst werden müssen, was alles Teil der Berliner Landes-IT sei. In den letzten Wochen seien dabei viele Softwareprodukte und -anwendungen entdeckt worden, die zuvor teils gar nicht auf dem Schirm gewesen seien, da sie dezentral geführt worden seien, Stichwort: Schatten-IT. Daher müsse es im ersten Schritt darum gehen, zentral zu erfassen, was an Software-IT im Land Berlin vorhanden sei. Diese Erfassung sei bis in alle Tiefen, vertikal und horizontal, vorzunehmen. Ein solcher Prozess sei aufgesetzt worden. Vor Kurzem habe er die Abfrage einer IT-Bestands- und Planungsübersicht in die Wege geleitet. Die Rückmeldefrist sei mit Mitte Oktober recht kurzfristig bemessen. – Weitere Dinge, die anzugehen seien, beträfen die Konzeption und Umsetzung einer abgestimmten und für das Land Berlin tragfähigen Lösung im gesamten Netzwerkbereich – Stichwort: Netzwerksicherheitsarchitektur für das Land Berlin im Ganzen –, die Etablierung eines landesweiten Information Security Management System – ISMS – und den Aufbau einer IKT-Sicherheitsarchitektur für alle Verfahren und Systeme. Hierzu gehöre etwa die Etablierung eines grundsätzlichen Lifecycle-Managements zur Vermeidung von End-of-Life Systems. Ferner gehe es um eine Modernisierung der teils schon sehr alten Fachverfahren, den Aufbau und die Etablierung einer landesweiten Schulungs- und Sensibilisierungsmaßnahme, eine Neukonzeption und den Aufbau eines landesweiten Active-Directory-Verbundes – dies hätten die Angriffsvektoren gezeigt – sowie den Aufbau und die Etablierung eines permanenten und das ganze Land Berlin umfassenden Monitorings bezüglich der Informationssicherheit. Überdies sollten in der nächsten Sitzung des Digitalkabinetts die neuen Business-Continuity-Management-Leitlinien auf den Weg gebracht werden. Die meisten der erwähnten Maßnahmen ließen sich jedoch nicht kurzfristig realisieren. Es handle sich nicht ausschließlich um organisatorische Aspekte. Vielmehr ergebe sich daraus auch ein Bedarf an Investitionen.

In diesem Zusammenhang warne er vor der sogenannten Katastrophendemenz. Er bitte alle, die künftig politische Verantwortung trügen und die Weichen für die nächste Koalition und den nächsten Haushalt stellten, den IKT-Notfall nicht zu vergessen. Der amtierende Senat sei

bereit zu unterstützen und weitere Informationen zur Verfügung zu stellen, auch Empfehlungen, wenn dies gewünscht sei. Nach dem Hackerangriff sei vor dem Hackerangriff. Trotz des enormen Schadens von 1,4 Mio. Dateien, die teils personenbezogene Daten umfassten, sei man im Ganzen gesehen noch relativ glimpflich davongekommen. Bei dem in Rede stehenden Angriffsvektor hätte es viel schlimmer ausgehen können. Bei einem künftigen Angriff könnte der Schaden viel größer ausfallen. Die notwendigen Maßnahmen müssten so schnell wie möglich in die Wege geleitet werden. Das, was kurzfristig getan werden könne, sei erfolgt. So sei in der vergangenen Woche ein Lessons-learned-Prozess aufgesetzt worden, der in der laufenden Woche mit ersten Bestandsaufnahmen beginne. Auch mit Blick auf das Notfallmanagement – Organisation, Strukturen, Prozesse – „in unserem Bereich“ bestehe ein Verbesserungsbedarf. Der Betrachtung folgten entsprechende Maßnahmen und Änderungen. Insgesamt gelte: Bis die mittelfristigen Maßnahmen, die der Erhöhung des Einbruchschutzes dienten, umgesetzt seien, müsse, gleichsam als Brückenlösung, zumindest ein funktionsfähiges Alarmsystem zur Verfügung stehen, um einen etwaigen neuen Angriff so schnell wie möglich zu detektieren und die nötigen Abwehrmaßnahmen zu ergreifen.

Staatssekretär Arne Herz (SenMVKU) bemerkt, er wolle das ergänzen, was seit der letzten Ausschusssitzung in seiner Verwaltung an Berichtenswertem passiert sei. – SenMVKU habe am 10., 15. und 17. September auf Rat der Berliner Beauftragten für Datenschutz und Informationsfreiheit per öffentlicher Bekanntmachung einen umgrenzbaren Personenkreis – Bewerberinnen und Bewerber; ehemalige Beschäftigte der SenMVKU; die in einer Datenbank registrierten Teilnehmer der STADTRADELN-Kampagne; Menschen, die mit seiner Verwaltung in Kontakt gestanden hätten, insbesondere bezogen auf Beteiligte in Unternehmen – über eine mögliche Betroffenheit von dem IT-Vorfall informiert. Damit habe zum frühestmöglichen Zeitpunkt eine Sensibilität hervorgerufen werden sollen, ohne dass bisher einzelne Betroffene identifiziert werden könnten. – Für die Beschäftigten der SenMVKU hätten Senatorin Bonde, Staatssekretär Kraus und er selbst Mitte September zwei Informationsveranstaltungen angeboten; in der laufenden Woche kämen weitere zwei Veranstaltungen zum direkten Austausch hinzu. Dabei gehe es sowohl um die dienstliche Funktion in Beantwortung von Bürgeranfragen als auch um den Umgang mit privater Betroffenheit. Damit gehe man über die FAQs, die sein Haus im Intranet veröffentlicht habe, hinaus; die Senatskanzlei habe eine solche Sammlung auch für externe Betroffene angelegt.

In der vergangenen Woche habe ein externer Dienstleister die Umgebung bei SenMVKU eingerichtet, um die mutmaßlich abgeflossenen Dateien mithilfe einer KI zu untersuchen. In der laufenden Woche beginne, orientiert an Stichworten, die eine gewisse Sensibilität aufwiesen und vor allem aus dem Haus gekommen seien, die Suche in den rund 770 000 Dateien. Auch die fortlaufenden Hinweise insbesondere des LKA kämen dabei zum Tragen; mit einem ähnlichen Verfahren bitte es SenMVKU um Unterstützung, was sein Haus leiste, Stichwort: indexbasierte Suche.

Bislang seien 477 Auskunftersuchen an die SenMVKU gerichtet worden. Dabei könne nicht unterschieden werden, wo Betroffene konkret nach abgeflossenen Daten fragten und wo sie ihr allgemeines Auskunftsrecht nach DSGVO in Anspruch nähmen. Die gesetzlichen Fristen zur Beantwortung würden eingehalten, wobei wegen der Menge an Anfragen der Rahmen von drei Monaten ausgeschöpft werde. Gleichwohl verließen in dieser wie in der nächsten Woche die ersten Zwischenbescheide das Haus. Die sein Haus begleitende Kanzlei stimme sich insbesondere bei neuen Schritten eng mit der Landesdatenschutzbeauftragten ab.

Staatssekretär Alexander Slotty (SenStadt) stellt in Aussicht, dass zeitnah damit begonnen werden könne, den gesamten Vorgang abzuarbeiten. Der Abschlussbericht des beauftragten Forensikers werde selbstverständlich abgewartet, um dann über die bereits ergriffenen Maßnahmen hinaus organisatorische und technische Ableitungen vorzunehmen. – Mit Stand dieser Woche könne gesagt werden, dass dem Grunde nach alle technischen Systeme wieder nutzbar zur Verfügung stünden. Derzeit sei in seinem Geschäftsbereich die Nutzung des Internets noch eingeschränkt. Diejenigen Seiten, die in seiner Verwaltung für die tägliche Arbeit benötigt würden, seien jedoch zugänglich. Der noch von Einschränkungen betroffene Datenaustausch mit Externen solle in dieser Woche wieder zur Verfügung stehen. Auch das für die Bezirke wichtige 3a-Verfahren werde ab dieser Woche wieder funktionieren. Alle anderen IT-Fachverfahren stünden den Bezirken bereits wieder zur Verfügung, Stichwort etwa: Wohn-geld.

In der vergangenen Woche seien die Mitarbeiterinnen und Mitarbeiter der SenStadt über die von ihren Laufwerken und den Outlook-Archiven abgeflossenen Dateien informiert worden. Die entsprechenden Indexlisten hätten die Beschäftigten persönlich in verschlossenen Umschlägen erhalten. – Die strukturierte Auswertung des veröffentlichten Datenbestands werde noch Zeit in Anspruch nehmen. Die Kolleginnen und Kollegen könnten die Inhalte der abgeflossenen Dateien selbst am besten einschätzen. – Im Übrigen lägen seiner Verwaltung mit heutigem Stand 80 Auskunftersuchen nach Art. 15 DSGVO und ungefähr 200 Anfragen bezüglich einer Betroffenheit von dem Cyberangriff vor. Für Bürgerinnen und Bürger habe SenStadt zwischenzeitlich eine Informationsseite online gestellt. Hier ließen sich erste Hinweise zu den möglicherweise bestehenden Risiken und den Schutzmaßnahmen, die jeder individuell ergreifen sollte, finden. Auf der Webseite seien darüber hinaus die spezifischen Gruppen veröffentlicht, die betroffen seien, darunter Bewerberinnen und Bewerber, aktive wie ehemalige Mitarbeiterinnen und Mitarbeiter. Damit komme sein Haus den sich aus Art. 34 Abs. 3 Buchstabe c der DSGVO ergebenden Pflichten nach. Bei individueller Betroffenheit von Berlinerinnen und Berlinern und insbesondere von KRITIS-Unternehmen würden diese individuell informiert.

Meike Kamp (Berliner Beauftragte für Datenschutz und Informationsfreiheit) gibt an, sie wolle einmal ausführlicher darstellen, wie ihre Behörde aufsichtsbehördlich mit dem Thema umgehe. – In der akuten Krisensituation habe der Schwerpunkt darin gelegen, den Datenschutzvorfall aufsichtsbehördlich im Rahmen der Vorgänge zur Meldung von Datenschutzfällen zu bearbeiten und den Senat direkt zu beraten über administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Hinblick auf die Verarbeitung ihrer personenbezogenen Daten. Wichtig sei ihr dabei gewesen, so weit wie möglich Transparenz herzustellen, indem gewährleistet werde, dass potenziell Betroffene Informationen dazu erhielten, wie sie Risiken erkennen und abmildern könnten, und darauf hinzuwirken, dass Ansprechstellen für betroffene Personen zur Verfügung gestellt würden.

Da es derzeit danach aussehe, dass sich die Phase der akuten Gefahrenabwehr dem Ende zuneige, werde ihre Behörde den Schwerpunkt auf die datenschutzrechtliche Untersuchung des Vorfalls verlagern. Der Datenschutzvorfall, bestimmte Aspekte der Verarbeitung personenbezogener Daten vor dem Vorfall sowie die Auswirkungen und Konsequenzen des Datenschutzvorfalls würden nun in aufsichtsbehördlichen Verfahren weiter untersucht und aufgearbeitet. Unter Berücksichtigung der verfügbaren Ressourcen werde sich ihre Behörde auf die

im Folgenden näher zu charakterisierenden, nach eigenem aktuellen Kenntnisstand wesentliche Themenkomplexe konzentrieren.

Erstens gehe es um die Einhaltung ausreichender technisch-organisatorischer Maßnahmen gemäß Art. 24 und Art. 32 DSGVO bei den Senatsverwaltungen und im Berliner Landesnetz. Es werde untersucht, wie es zu dem Datenschutzvorfall konkret gekommen sei, welche Folgewirkungen sich aufgrund von Schnittstellen zum Berliner Landesnetz auch für das Landesnetz sowie sämtliche dort angeschlossenen weiteren Infrastrukturen ergäben und ob ausreichende technisch-organisatorische Maßnahmen bei SenStadt und SenMVKU und in Bezug auf das Berliner Landesnetz getroffen worden seien. Ihre Zuständigkeit in diesem Zusammenhang beschränke sich allerdings auf den Ausschnitt der erforderlichen IT-Sicherheitsvorkehrungen bezüglich der Verarbeitung personenbezogener Daten. Mithin sei es nicht die Aufgabe ihrer Behörde, die gesamte IT-Sicherheit des Landes zu untersuchen. Mit Blick auf die Senatskanzlei nehme man dabei aber zunächst eine zentrale Verantwortlichkeit für den Betrieb des Landesnetzes bzw. den Anschluss neuer Stellen an das Landesnetz an.

Zweitens befasse sich ihre Behörde mit der Frage der Einhaltung von Benachrichtigungspflichten im Fall der Meldung von Datenschutzvorfällen. Hierbei spiele auch die rechtzeitige Benachrichtigung eine Rolle. Im Kontext des Cyberangriffs habe man sieben Meldungen nach Art. 33 DSGVO erhalten, und zwar von Senatsverwaltungen, dem ITDZ, nachgeordneten Behörden oder landeseigenen Betrieben. Bei einem Datenschutzvorfall gelte es, nicht nur an die Datenschutzbehörde zu melden, sondern auch die betroffenen Personen zu benachrichtigen. Dadurch sollten diese auch darüber informiert werden, wie sie Risiken abmildern oder sich vor negativen Folgen von Datenveröffentlichungen oder sonstigen Datenabflüssen schützen könnten. – In Hinblick auf die potenziell betroffenen Personen, die keine Beschäftigten der Senatsverwaltung seien, habe SenMVKU am 10. September über ihre Webseite ein Informationsangebot geschaltet, und zwar, wie Staatssekretär Herz bereits dargelegt habe, als Benachrichtigung durch öffentliche Bekanntmachung. Diese Benachrichtigung werde, auch nach Beratung ihrer Behörde, fortlaufend aktualisiert für spezifische Betroffenengruppen, die bei den Analysen identifiziert würden. Man habe die Senatsverwaltung beraten, dass so vorzugehen sei, und erläutere, dass die öffentliche Bekanntmachung eine Individualbenachrichtigung dann entfallen lassen könne, wenn andernfalls ein unverhältnismäßiger Aufwand entstünde. Für die Risikovorsorge sei es in manchen Situationen wichtiger, dass alle informiert würden, als abzuwarten, wer konkret betroffen und dann darüber zu informieren sei. – Dass SenStadt ein Informationsangebot geschaltet habe, sei ihr neu; möglicherweise bestehe es erst seit Kurzem. Sie rege an, dass Herr Slotty dazu noch einmal Stellung nehme. – Bezüglich der Beschäftigten der Senatsverwaltungen und anderer Behörden, die gemeldet hätten, habe ihre Behörde bislang keine konkreten Erkenntnisse darüber, wann mit welchen Informationen an diese herantreten worden sei. Man werde das im Rahmen der Meldevorgänge noch weiter erfragen und prüfen. Auf konkrete Antworten warte ihre Behörde zum Teil; diesbezüglich seien Fristen abgelaufen.

Drittens untersuche man die Organisation der Datenverarbeitung auf den kompromittierten Laufwerken der Senatsverwaltungen, das Auswertungsverfahren sowie die Auskunftsverfahren. Zu den sich stellenden Fragen gehöre, wie die Datenverarbeitung auf den von dem Cyberangriff betroffenen Fileservern organisiert gewesen sei, welche internen Anweisungen und Vorgaben es zu deren Nutzung gegeben habe, welche technisch-organisatorischen Maßnah-

men vor dem Angriff ergriffen worden seien, um u. a. die Löschung personenbezogener Daten auf diesen Fileservern sicherzustellen.

Viertens nehme ihre Behörde die Rollenverteilung in datenschutzrechtlicher Dimension und das Vorliegen von Auftragsverarbeitungsverträgen zwischen den Senatsverwaltungen und deren nachgeordneten Behörden in den Blick. Die Meldungen zu den Datenschutzvorfällen und die Informationen, die beide Senatsverwaltungen in der Ausschusssitzung am 24. August gegeben hätten, böten aus Sicht ihrer Behörde Anlass, danach zu fragen, wer in welchen Zusammenhängen personenbezogene Daten als Verantwortlicher oder als Auftragsverarbeiter verarbeite. Auch in den Meldungen der nachgeordneten Behörden bzw. Stellen bleibe teils offen, wie das datenschutzrechtliche Rollenverhältnis zur jeweiligen Senatsverwaltung ausgestaltet sei und ob hier Auftragsverarbeitungsverhältnisse bestünden.

Fünftens werde man sich der Prüfung des Einsatzes des Dienstleisters CrowdStrike und der Analysesoftware für forensische Analysen zur Detektion, ob der Cyberangriff noch andauere, zuwenden. In der akuten Krisensituation habe ihre Behörde die Senatskanzlei darauf hingewiesen und darum gebeten, die verantwortlichen Senatsmitglieder entsprechend zu informieren, dass die betroffenen Beschäftigten über den Einsatz von CrowdStrike in Kenntnis zu setzen, die Anforderungen der Auftragsverarbeitung und die Drittenstaatenabsicherung einzuhalten seien und hier ggf. vertraglich nachgeschärft werden müsse. Eine tiefergehende Prüfung von Amts wegen sei nun eingeleitet. Ihre Behörde habe eine von Reihe von Fragen gestellt und Unterlagen angefordert, die inzwischen zum Teil eingegangen seien; wesentliche Informationen fehlten aber noch.

Sechstens beschäftige sich ihre Behörde mit den Zuständigkeiten und Strukturen im Bereich der Informationssicherheit in Berlin. Insgesamt habe man wahrgenommen, dass im Land Berlin eine Reihe von Unklarheiten in Bezug auf die Verantwortlichkeiten bei einem Cyberangriff auf gemeinsam genutzte Infrastruktur, selbst betriebene Netze und vom ITDZ betriebene IT bestünden. Das betreffe vor allem die Befugnisse und Verantwortlichkeiten der Senatskanzlei im Bereich des Chief Digital Officer – CDO –, des Berlin-CERT und des ITDZ und das gesamte Zusammenspiel zwischen den Akteuren und weiteren an das Landesnetz angeschlossenen Behörden, Senatsverwaltungen, nachgeordneten Stellen in Bezug auf das übergreifende Ziel der IT-Sicherheit. Diesbezüglich werde man auf die Senatskanzlei bzw. das ITDZ zugehen und darüber sprechen, welcher Optimierungsbedarf hier gesehen werde, insbesondere hinsichtlich der Befugnisse des Landesbeauftragten für Informationssicherheit und einer Fortentwicklung dieser Position zu einem Chief Information Security Officer und entsprechend erforderlicher gesetzlicher Regulierung. Ein IT-Sicherheitsgesetz für Berlin sei ihrer Überzeugung nach geeignet, dabei zu helfen, viele offene Fragen zu klären und für klare Verantwortlichkeiten zu sorgen. In diesem Zusammenhang erscheine es sinnvoll, das höchst aktuelle und vorbildliche Informationssicherheitsgesetz Mecklenburg-Vorpommern in den Blick zu nehmen.

Tobias Schulze (LINKE) schickt voraus, dass die IT-Sicherheit unabhängig von der künftigen Koalition in Hinblick auf Organisation, Finanzen und Verwaltungsstrukturen hohe Priorität in der neuen Legislaturperiode genießen müsse. Es gelte, nun die Schlussfolgerungen aus dem IT-Vorfall zu ziehen. Die vorhandenen IT-Strukturen müssten deutlich beschleunigt und deutlich stringenter standardisiert werden. Zudem seien die entsprechenden Sicherheitsinfrastrukturen einzubauen, Stichwort: Brandmauern zwischen den verschiedenen Sektoren der IT.

Gleichzeitig komme es auf Fortschritte bei der zentralen Administration an. Zweifellos koste das alles viel Geld. Außerdem gebe es ein Zusammenspiel mit der Verwaltungsreform. Einigkeit bestehe wohl dahin gehend, dass ein solcher Vorfall nicht noch einmal passieren dürfe. Dinge, die ein Nice-to-have wären, müssten in diesem Zusammenhang etwas zurückstehen.

Zu den Fragen: Bislang vermisse er konkrete Ausführungen darüber, warum die beiden betroffenen Senatsverwaltungen nicht selbst bemerkt hätten, dass Daten abfließen. Seine Fraktion bzw. er selbst habe es bisher so verstanden, dass diese Erkenntnis ein Beifang des ITDZ gewesen sei. Daher bitte er um Auskünfte darüber, wie die Detektion der Angriffe und abfließenden Daten gelaufen sei und aus welchen Gründen die Täter mehr oder weniger unbemerkt im Netz hätten sein können. Wie solle das in Zukunft laufen?

Des Weiteren interessiere ihn, ob die Mitarbeitenden in den Verwaltungen auf „diese Art von Phishingmails“ geschult worden seien. Schließlich seien bestimmte Angriffsvektoren genutzt worden, Stichwort: ClickFix. Seien derartige Schulungen für die Zukunft geplant?

In der letzten Ausschusssitzung sei zur Sprache gekommen, dass es 21 Fachverfahren geben solle, bei denen die Passwörter mit gecodet worden seien, was es den Angreifern besonders leicht gemacht habe. Existiere eine Strategie, wie das mithilfe von Sicherheitsinstrumenten wie der Mehr-Faktor-Authentifizierung vermieden werden solle?

Frau Dr. Borelli habe in der letzten Sitzung mitgeteilt, dass die Kompetenzen des ITDZ bislang nicht so abgerufen worden seien, wie das möglich wäre; Stichwort u. a.: CERT. Vor diesem Hintergrund wolle er wissen, ob das ITDZ vom Senat mittlerweile stärker in die Aufarbeitung des Vorfalls und in Ansätze für die Zukunft der IT-Sicherheit eingebunden sei.

Mit Blick auf die wiederholte Aussage von Staatssekretär Hauser, wonach Fachverfahren gefunden worden seien, von denen man zuvor nichts gewusst habe, weise er auf die Antwort auf eine Schriftliche Anfrage hin, in der es heiße, dass im Zuge der Beantwortung der Anfrage Fachverfahren gefunden worden seien. – Das Thema Schatten-IT habe ihn sehr belustigt; eine frühere CDO habe dies „Technikzoo“ genannt. – Seit mindestens fünf Jahren gebe es Versuche, eine Bestandsübersicht der Berliner IT zu erhalten. Dennoch würden noch immer Fachverfahren gefunden. Warum sei es dem Senat innerhalb von fünf Jahren nicht gelungen, eine Übersicht über die Hard- und Software der Berliner IT zu erstellen? Was müsste politisch getan werden, um das zu ändern?

Zum Thema CrowdStrike: Sei inzwischen eine Lösung für das datenschutzrechtliche Problem gefunden worden, dass die Bezirke einem Anbieter, der der amerikanischen Regierung gegenüber rechenschaftspflichtig sei, erlauben sollten, auf ihre Laufwerke zuzugreifen? Laufe CrowdStrike inzwischen in allen Bezirken? Funktioniere das Produkt? Aus Steglitz-Zehlendorf sei zu vernehmen gewesen, dass der Einsatz der Software zu Dysfunktionalitäten in den dortigen Laufwerken geführt habe.

Stefan Ziller (GRÜNE) sagt, dass er sich den grundsätzlichen Bemerkungen nur anschließen könne. In der Tat müsse einiges in kürzerer Zeit als bisher geplant passieren. Das Ganze müsse für jede neue Regierung Priorität haben. – Die Ausführungen vonseiten des Senats habe er an vielen Stellen eher nicht als faktenbasiert und fundiert empfunden. Bis heute sei unklar, wie hoch die Zahl der Betroffenen sei. Könnten Angaben dazu gemacht werden, wie groß die

benannten Gruppen jeweils seien? Gebe es tatsächlich keinen Überblick, oder sei das aus Zeitgründen weggelassen worden?

SenStadt und SenMVKU gingen nach seiner Beobachtung unterschiedlich mit den Daten und Betroffenheiten um. Staatssekretär Slotty habe davon gesprochen, dass den Mitarbeitenden die Indexlisten zur Verfügung gestellt worden seien. Die betreffenden Personen könnten vollständig über die mutmaßlich abgeflossenen Daten informiert werden; von der Belastbarkeit der Indexlisten könne ausgegangen werden. Daraus ließen sich durchaus Zahlen und Fakten ableiten; das vermisse er.

Hinsichtlich der Aussage von Herrn Hauer, Berlin sei glimpflich davongekommen, rate er zur Vorsicht, zumal der Staatssekretär auch gesagt habe, dass noch nicht alle Daten heruntergeladen worden seien. Die Faktenlage sei noch zu dünn für eine stichhaltige Bewertung. Mit Blick auf die Indexlisten interessiere ihn zudem, um welche Arten von Dateien es sich handele.

In Bezug auf die Passwörter habe er gehört, dass beispielsweise das Landesamt für Bürger- und Ordnungsangelegenheiten – LABO – nicht in der Lage sei, Passwörter schnell zu ändern, sondern bis Weihnachten oder noch länger benötige, um für LABO-Verfahren, auf die andere Ämter Zugriff brauchten, die Passwörter zu ändern und sie diesen mitzuteilen. Er rate der IKT-Steuerung, sich das Ganze einmal anzuschauen, zumal es die Funktionsfähigkeit ernsthaft beeinträchtige. Er hoffe, dass senatsseitig etwas dazu gesagt werden könne.

Angesichts der Aussicht, dass der Notfall innerhalb kürzerer Zeit für beendet erklärt werden könne, wolle er wissen, was das für die Kosten bedeute. Sei bereits überschlagen worden, welche Kosten im Zeitraum des Notfalls entstanden seien? Sei sichergestellt, dass alles, was notfallbedingt bezahlt werde, danach weiterbezahlt werde? Er gehe davon aus, dass die angesprochenen Alarmsysteme auf dem Notfallniveau fortgeführt werden müssten, aber zuvor nicht finanziell abgesichert gewesen seien. Könne die Senatskanzlei die Dimension dessen beziffern, was an Investitionen im nächsten und übernächsten Jahr im IKT-Sicherheitsbereich nötig sei?

Mit Blick auf die Zukunft wolle er wissen, inwiefern die IT-Bestands- und Planungsübersicht – IT-BePla – nun neu abgefragt werde. Gebe es Gespräche, wie diese Übersicht digital abgebildet werden könnte? Alle dezentralen Admins verfügten schließlich über eine digitale Übersicht über ihre Server. Aus seiner Sicht könne eine grundlegende IT-Bestands- und Planungsübersicht durch entsprechende Schnittstellen oder das Zusammenschalten von digitalen Informationen, die dezentral vorlägen, verhältnismäßig aktuell umfangreich erstellt werden.

Vonseiten des ITDZ interessiere ihn, welche konkreten Arbeitsaufträge oder Verträge mit Bezahlung die Behörde für den Aufbau von Neuem derzeit habe. Die Überwachung des Landesnetzes sei aus seiner Sicht die Aufgabe des ITDZ. Es müsse in der Lage sein, alle dezentralen Netze mit Technik, die State of the Art sei, zu überwachen. Glücklicherweise sei das ITDZ BSI-zertifiziert und verfüge über die höchsten Standards. Er vermute, es sei nicht geplant, jede Senatsverwaltung einzeln zu zertifizieren.

Zwar seien senatsseitig einzelne Punkte herausgegriffen worden, doch wolle er sich erkundigen, ob es einen verschriftlichten Fahrplan für die IKT-Architektur und die nächsten Schritte gebe. Grundsätzlich bedürfe es eines Zusammenspiels. Im Ausschuss sei bereits über Brand-

mauern in den verschiedenen Netzsegmenten gesprochen worden. Es erscheine sinnvoll, wenn der Senat solche Dinge verschriftlichte und dem Ausschuss zur Verfügung stellte. Er rege an, dass dazu in der neuen Legislaturperiode eine Anhörung mit Fachleuten stattfinde. Nur die Schlagworte in den Raum zu stellen, reiche nicht aus. Auch die Reihenfolge der einzelnen Schritte bzw. die Reihenfolge innerhalb derselben habe er nicht verstanden.

Wie er gehört habe, sei geplant, ein Security Operations Center außerhalb des ITDZ zu dopen. Treffe das zu? Gebe es diesbezüglich ein Zusammenspiel? – Was CrowdStrike angehe, wolle er wissen, ob Richtung Bund der Arbeitsauftrag formuliert worden sei, auf ein europäisches Tool hinzuwirken, um die digitale Souveränität Deutschlands und der EU zu gewährleisten, oder bestehe in dieser Hinsicht noch Handlungsbedarf?

Marc Vallendar (AfD) merkt an, dass Digitalisierung ohne IT-Sicherheit nicht funktionieren werde. Es treffe zu, dass die nächste Regierungskoalition eine Vielzahl an Aufgaben finanzieller wie struktureller und ggf. gesetzgeberischer Art zu bewältigen habe. – Mit Blick auf die Anlaufstelle für Bürger und Mitarbeiter, die aus drei E-Mail-Postfächern und einem Kontaktweg über berlin.de/cyberangriff bestehe, interessiere ihn, wie viele Anfragen bislang eingegangen seien. Auf welche Weise gewinne der Senat einen Überblick darüber, wie viele konkret Betroffene es insgesamt gebe? – In Bezug auf den am 7. September verlangten schriftlichen Lagebericht mit einer Chronologie wolle er wissen, ob ein solches Papier im Senat vorliege. Wenn nicht, wann sei damit zu rechnen, beziehungsweise werde überhaupt noch ein Bericht erstellt?

Darüber hinaus erkundige er sich in Hinblick auf die parlamentarische Aufklärung in der neuen Legislaturperiode, ob angeordnet worden sei, dass alle Unterlagen, E-Mails und Protokoll-daten zu dem Cyberangriff bei der Senatskanzlei, bei SenStadt, SenMVKU und im ITDZ gegen eine Löschung gesichert würden. Seit wann gelte eine solche Anordnung ggf.? – Für den Fall, dass Ausweispapiere oder Pässe bzw. deren Kopien im Darknet veröffentlicht worden seien, interessiere ihn, ob das Land Berlin die Gebühren für die Beantragung der neuen Dokumente übernehme. Habe der Senat bereits über diese Frage entschieden? – Ferner sei von Interesse, wie weit die Vertragsverhandlungen über die Migration der IT von SenStadt und SenMVKU zum ITDZ vorangeschritten seien. Gebe es einen Zeitplan? – Überdies wolle er wissen, aus welchem Kapitel und welchem Titel die bereits erteilten Aufträge, etwa für die Forensik und Datenanalyse, bezahlt worden seien. Wann werde der Hauptausschuss einen ersten Kostenbericht erhalten? – Des Weiteren interessiere ihn, ob der Senat bei den einzelnen Senatsverwaltungen und den Bezirken nachgefragt habe, wo Verschlusssachen digital abgelegt worden seien. Mit welcher Frist sei das vonseiten des Senats erfolgt?

In Hinblick auf die senatsseitig getroffene Aussage, dass man noch glimpflich davongekommen sei, erkundige er sich danach, wie Staatssekretär Hauer zu diesem Schluss komme, wenn die Datenanalyse noch nicht abgeschlossen sei. – Was könne zum aktuellen Ermittlungsstand des Bundeskriminalamts mitgeteilt werden? Habe sich der Erkenntnisstand in den letzten drei Wochen geändert?

Jan Lehmann (SPD) bringt vor, er wolle die Gelegenheit ergreifen, sich für die vergangenen fünf Jahre zu bedanken. Darin schließe er die Kollegen von Grünen und Linken ebenso ein wie die CDU-Fraktion und deren Sprecher für Digitalisierung und Datenschutz Herrn Förster. Auch den CDOs Frau Klement und Herrn Hauer danke er für die stets kollegiale, sofortige

Information nach bestem Wissen und Gewissen. – Inhaltlich komme er zunächst auf die Aussage von Staatssekretär Hauer zu sprechen, wonach das Ausrollen der Sensorik fast fertig sei. Was sei bereits abgeschlossen, was fehle noch, und warum fehle es noch? – Wie lange werde CrowdStrike noch auf den bezirklichen Servern laufen? Würden die Bezirke informiert? Könne Näheres zur Sicherheit von CrowdStrike mitgeteilt werden? – Darüber hinaus interessiere ihn, ob es Erpressungsversuche auch auf Personen oder Unternehmen gegeben habe. Ließen sich Trittbrettfahrer feststellen, die sich Daten heruntergeladen hätten und damit Missbrauch betrieben? – Dass man den Modus der Gefahrenabwehr nach Auskunft von Herrn Hauer nach und nach verlasse, beziehe sich aus seiner Sicht nur auf den konkreten IT-Vorfall. Die Gefahrenabwehr allgemein gelte es fortzusetzen. Sei es bereits zu Änderungen in Firewalls gekommen? Kämen Weiterbildungen von Mitarbeitenden in Bezug auf den Umgang mit Links in Betracht? – Im Zuge der letzten Sitzung habe die Überlegung im Raum gestanden, Dienstvergehen zu ahnden, wenn Passwörter im Freitext in Dokumenten mit der Bezeichnung „passwort.docx“ zu finden seien. Wie weit sei man in dieser Hinsicht? Gebe es eine Art Kulanzregelung? Liefen bereits Verfahren?

Carsten Schatz (LINKE) schildert, für ihn ergäben die bisherigen Ausführungen des Senats folgendes Bild: Es sei zu einem Einbruch gekommen. Die Phase, dass die Tür zugehalten werden müsse, scheine sich dem Ende zu nähern; sie bleibe zu. Ferner sei festgestellt worden, dass sämtliche Fenster geschlossen und keine weiteren eingeschlagen seien. Mithin sei das Haus erst einmal sicher. – Bezüglich der Frage nach dem ITDZ, die Herr Schulze gestellt habe, erhoffe er sich Antworten von Frau Dr. Borelli. Unbenommen davon müssten noch einmal jene Fragen gestellt werden, die in der letzten Sitzung gestellt und nicht beantwortet worden seien. Wie verhalte es sich mit der belastbaren Ereignis- und Entscheidungszeitleiste, die am 7. September zugesagt worden sei? Er bestehe darauf, dass dort stets folgende Dinge dokumentiert seien: der Zeitpunkt; der Kenntnisstand; welche Informationen seien eingegangen?; woher seien diese Informationen gekommen?; welche Entscheidung sei von wem getroffen worden?; welche Folgen hätten sich daraus ergeben? – Eine solche Aufstellung diene auch der Nachvollziehbarkeit, welche Struktur geholfen habe und welche nicht.

Außerdem lenke er den Blick nochmals auf den Haushalt. Im Zuge der Beratungen über „den Nachtragshaushalt 2024“ seien 12 Mio. Euro bei dem Landesnetz herausgenommen worden, darunter 2 Mio. Euro bei der Eindringungserkennung. Ihn interessiere nach wie vor, welche Maßnahmen zur Eindringungs- und Anomalieerkennung infolge jener Kürzung verschoben, reduziert oder nicht umgesetzt worden seien. Dabei gehe es ihm nicht um Schuldzuweisungen, sondern darum, dass man sich in diesem Bereich künftig keinen Wankelmut leisten könne. Wer das Ziel eines sicheren Landesnetzes befürworte, müsse die notwendigen finanziellen Mittel zur Verfügung stellen und ggf. an anderen Stellen sparen. Hätten Maßnahmen, die dann weggefallen seien, dazu geführt, dass der Datenabfluss früher entdeckt worden wäre?

Zu den zu treffenden Entscheidungen gehöre, alle Senatsverwaltungen in die Regie des ITDZ zu überführen, Stichwort: OneIT@Berlin. Wie gestalte sich dies bezüglich der Zeitplan für SenMVKU und SenStadt? Werde nun eine Beschleunigung in Angriff genommen, oder werde es weiter nicht ernsthaft angegangen?

Allgemein heiße es, man müsse besser und koordinierter werden. Laut Frau Kamp handelten SenStadt und SenMVKU jedoch unterschiedlich, was die Information der Betroffenen angehe, obgleich sie eine gemeinsame IT-Stelle hätten. Das verstehe er nicht. Gebe es keine Ab-

stimmung? – Eine Verständnisfrage: Worum handele es sich bei dem erwähnten 3a-Verfahren? – Ferner: Sei die Aussage, dass Personen, die mit SenMVKU in Kontakt gestanden hätten, möglicherweise betroffen seien, so zu verstehen, dass dies alle einschließe, die jemals eine E-Mail an SenMVKU geschrieben hätten?

Staatssekretär Florian Hauer (Skzl) wendet sich zunächst den verschiedentlich gestellten Fragen zu, was er mit „glimpflich“ meine: Er habe von „relativ glimpflich“ gesprochen. Zudem habe er deutlich darauf hingewiesen, dass der den betroffenen Bürgerinnen und Bürgern entstandene Schaden immens sei, aber glimpflich im Verhältnis zu dem Schaden, der hätte entstehen können. Er erinnere daran, dass im Ausschuss vor einigen Wochen gefragt worden sei, ob die Wahlen verschoben werden müssten. Ferner verweise er auf das Vorgehen der Tätergruppe in der Vergangenheit, Stichwort: Ransomware. Vorstellbar gewesen wäre im konkreten Fall auch eine Verschlüsselung oder Manipulation von noch viel größeren Datenbeständen bis hin zu einem möglicherweise notwendigen Komplettaufbau der Berliner Landes-IT. Insofern sei das Land Berlin glimpflich davongekommen, wenngleich er den entstandenen Schaden nicht kleinreden wolle. Im Übrigen habe er eingangs gesagt, dass eine abschließende Analyse, besonders zur kritischen Infrastruktur, noch nicht vorliege, und darauf verwiesen, was es für den einzelnen Bürger bedeute, wenn seine Personal- oder Bankdaten öffentlich verfügbar seien. Er wisse aus eigener Erfahrung, wie es sei, Opfer von Identitätsdiebstahl zu sein.

Zum Stichwort Schatten-IT: Er habe angeführt, dass die Anfrage zur Bestandsübersicht eingeleitet worden sei. § 20 Abs. 3 E-Government-Gesetz Berlin biete die klare gesetzliche Grundlage dafür. Die Senatskanzlei erwarte klare Antworten. Er schließe nicht aus, dass es Schwierigkeiten gebe und zu Verzögerungen über die bis Mitte Oktober gesetzte Frist hinaus komme. Er hoffe, dass die Bedeutung der Informationen allseits bekannt sei; ggf. werde man nachhaken müssen. Generell stelle sich die Frage, wie Fachverfahren definiert werden sollten. Einzelne Dienststellen der Bezirksämter verfügten über Softwarelösungen, die seit Jahren in Eigenregie betrieben würden und die außerhalb der Dienststelle bislang gänzlich unbekannt gewesen seien. Wenn diese Software alt sei, nicht mehr aktualisiert werde, keine Updates mehr stattfänden, ergebe sich ein Risiko für das gesamte Landesnetz, sofern es aus diesen Stellen eine Verbindung ins Landesnetz gebe. Solche Fälle müssten so schnell wie möglich erfasst und abgestellt werden. Für eine gesetzliche Nachschärfung – Frau Kamp habe auf das IT-Sicherheitsgesetz in Mecklenburg-Vorpommern verwiesen – sei er offen, zumal mit einzelnen Bezirksämtern in den letzten Wochen Schwierigkeiten bestanden hätten. Für künftige IT-Vorkommnisse sei ggf. ein Durchgriffsrecht für die oder den CDO gegenüber allen Stellen im Land Berlin vorzusehen.

Mit Blick auf CrowdStrike hätten die betroffenen Bezirksämter ihm am Ende vermittelt, dass ihre datenschutzrechtlichen Bedenken mit den Ausführungen der Senatskanzlei – zumindest ad hoc – aus der Welt seien. Das sei sein Eindruck gewesen. Außerdem stehe man senatsseitig im Austausch mit dem Hauptpersonalrat. So, wie er es verstanden habe, gebe es dort ein Verständnis für die Notwendigkeit des Einsatzes jener Sensorik in dieser Situation; diese Information sei dann auch so in die Breite, an die örtlichen Personalräte getragen worden. – CrowdStrike laufe derzeit noch nicht auf allen rund 150 000 Clients in der Berliner IT. Die erwähnten Probleme bei dem Bezirksamt Steglitz-Zehlendorf seien nicht datenschutzrechtlicher Natur gewesen, sondern lägen in technischen Aspekten. Die dort bereits genutzte Sicherheitssoftware und CrowdStrike seien nicht miteinander kompatibel gewesen. Wenn er die

Forensiker richtig verstanden habe, sei die 100-prozentige Abdeckung durch CrowdStrike nicht zwingend erforderlich, wenn es darum gehe, auf der Grundlage des Abschlussberichts den akuten Notfall für beendet zu erklären. Je länger der IT-Vorfall zurückliege, desto geringer sei die Notwendigkeit, 100 Prozent zu erreichen, um die Risikoabschätzung vorzunehmen.

Zu der Frage in Bezug auf die Passwörter und das LABO könne er nichts sagen. Falls Herr Dr. Kroll-Peters das aus dem Stegreif nicht beantworten könne, müssten die Informationen über SenInnSport ermittelt und dann nachgereicht werden. – Was die Kosten betreffe, so seien diese noch nicht abschließend erhoben worden. Grundsätzlich müssten sie erhoben werden, vor allem von der Staatsanwaltschaft, da sie für die strafrechtliche Bewertung der Frage entscheidend seien, welcher Schaden eingetreten sei. Zu den Kosten gehörten nicht nur die Ausgaben für externe Dienstleister, sondern darin flössen auch sonstige Schäden mit Blick auf den Arbeitseinsatz und das eigene Personal ein. Wer im Zweifelsfall für die Kosten für einen neuen Personalausweis aufkommen müsse, wisse er derzeit noch nicht. Das könne erst dann juristisch geprüft werden, wenn konkrete Ansprüche gegenüber dem Senat erhoben würden. Solche Dinge müssten auch in eine Kostenrechnung miteinfließen. – [Dr. Matthias Kollatz (SPD): Es kommt aber darauf an, ob der überhaupt da sein durfte, der Personalausweis!] – Dem zurufenden Abgeordneten gegenüber wolle er klarstellen, dass er dabei nicht an den Beschäftigten gedacht habe, sondern daran, dass ein Bürger einen Antrag gestellt und in diesem Zuge Daten übermittelt habe, die dann abgefließen seien. Eine einzelfallbezogene Betrachtung sei unabdingbar; dies schließe pauschale Aussagen zum jetzigen Zeitpunkt aus.

In Hinblick auf das ITDZ und das Cyberabwehrzentrum gehe er davon aus, dass Frau Dr. Borrelli näher ausführen werde, worin genau die Rolle des Berlin-CERT, des Cyberabwehrzentrums an der Stelle liege.

Die Zeitliste, nach der mehrfach gefragt worden sei, habe die Senatskanzlei weder vergessen, noch werde sie die Bitte darum ignorieren. Er bitte aber um Nachsicht dafür, dass die Phase der akuten Gefahrenabwehr noch andauere. Nach Aufhebung des Notfalls könne rückwirkend dargestellt werden, was wann gemacht worden sei. Bei allem Verständnis für die wichtige parlamentarische Kontrolle erscheine es sinnvoll, nicht beides parallel zu tun.

Zum Stichwort Löschmoratorium: In einem laufenden strafrechtlichen Ermittlungsverfahren dürften keine Daten gelöscht werden. Selbst wenn in zwei oder drei Jahren noch kein Untersuchungsausschuss existierte, nähme der Senat wahrscheinlich trotzdem von einer Löschung Abstand. Die Frage eines etwaigen Moratoriums stellte sich erst dann, wenn der Senat gesetzlich zu einer Datenlöschung verpflichtet wäre. Im Übrigen wolle er mitteilen, dass alles, auch die Sitzungen des Notfallstabs und anderer Gremien, ordnungsgemäß dokumentiert werde.

Für die vom Abgeordneten Lehmann geäußerten Worte bedanke er sich. In der Phase der akuten Gefahrenabwehr habe er selbst es als angenehm wie hilfreich empfunden, mit den Ausschussmitgliedern ins Gespräch zu kommen. – In Anlehnung an das bisher Gesagte zum Thema CrowdStrike sei es so, dass die Sensorik für die Dauer der Phase der akuten Gefahrenabwehr aufrechterhalten werde. – Von weiteren Erpressungsversuchen sei ihm in seiner amtlichen Funktion nichts bekannt. Er könne aber nicht ausschließen, dass er bei Wikipedia etwas Derartiges über diese Gruppe gelesen habe; das sei jedoch nichts Belastbares.

Wenn der Notfall beendet sei, könne nicht einfach zu dem vorherigen Zustand zurückgekehrt werden. – Aus seiner Sicht bestehe so weit die Gewissheit, dass, was das sprachliche Bild angehe, der Einbrecher nicht mehr im Haus sei. Ob die Fenster und Türen verriegelt seien? – Er habe davon gesprochen, dass mittelfristig der Einbruchschutz erhöht werden müsse. Bis dahin benötige man zumindest eine funktionierende Alarmanlage. – Die Frage, welche Auswirkungen die vorgenommenen Kürzungen von Haushaltsmitteln gezeitigt hätten, habe ihre Berechtigung. Gleichwohl lägen ihm keine Erkenntnisse im Sinne einer Kausalkette vor, wonach die Einsparungen bzw. nicht zusätzlich zur Verfügung stehenden Mittel dazu geführt hätten, dass diese oder jene Maßnahme habe unterbleiben müssen, und das Unterlassen der betreffenden Maßnahmen den geschehenen Angriff befördert oder ermöglicht habe.

Abschließend wolle er noch betonen, dass die Zusammenarbeit mit dem Unternehmen CrowdStrike sehr gut gewesen sei. Er wisse nicht, wie die notwendigen Arbeiten anders hätten bewerkstelligt werden können. Überdies habe Frau Kamp angekündigt, dass sie in der nächsten Zeit wieder mehr von der Beratungs- in die Aufsichtsfunktion wechseln werde und noch Fragen habe. So, wie er diese Software verstehe, erfasse sie Metadaten, Verbindungsdaten, die von personenbezogenen Daten der Beschäftigten zu unterscheiden seien. Dem Senat sei versichert worden, dass CrowdStrike DPF-zertifiziert sei und damit dem EU-US Data Privacy Framework unterliege und die Daten im Bereich der EU gehostet würden. Daher sehe er keine Anhaltspunkte für die Annahme, dass sensible personenbezogene Daten von Berliner Beschäftigten in einen Bereich kämen, der neue Gefährdungen mit sich brächte.

Staatssekretär Alexander Slotty (SenStadt) tritt dem durch die gestellten Fragen vermittelten Eindruck entgegen, wonach der Senat den Ausschuss in den letzten Wochen völlig im Unklaren über die in Rede stehenden Vorgänge gelassen habe. Der Abgeordnete Vallendar habe zwei Fragen gestellt, die er in seinem Eingangsstatement beantwortet habe. So habe er bereits eingangs die 80 Auskunftersuchen nach Art. 15 DSGVO und die 200 Anfragen hinsichtlich der Betroffenheit von dem Cyberangriff genannt. Was den Bericht angehe, so lege seine Verwaltung diesen gerne vor. Allerdings sei SenStadt selbst u. a. von dem noch nicht vorliegenden Bericht der Forensik abhängig. Hier gehe Gründlichkeit vor Schnelligkeit.

Des Weiteren weise er die Aussage zurück, dass die Entdeckung des Hackerangriffs ein Beifang gewesen sei. Das habe er niemals behauptet. Vielmehr habe er dem Ausschuss bereits den genauen zeitlichen Ablauf dargelegt. Die Detektion der Schadsoftware sei am 10. August durch die IT-Stelle von SenStadt selbst erfolgt. Zeitgleich sei es zu Auffälligkeiten an anderen Stellen im Landesnetz gekommen. Insofern könne von parallelen Erkenntnissen über irreguläre Vorgänge gesprochen werden. Am 12. August habe die Firewall von SenStadt den Datenabfluss unterbunden. An jenem Tag habe sich das ITDZ seinerseits mit der Information gemeldet, dass da etwas sei. Zwei Tage später seien die beiden betroffenen Senatsverwaltungen angesichts des befürchteten Ausmaßes eines Hackerangriffs in Absprache mit dem ITDZ vom Landesnetz abgekoppelt worden. Er selbst sei in den Mittagsstunden des 14. August über den Vorgang informiert worden. Am Folgetag habe er den Krisenstab der SenStadt aktiviert. Seitdem werde eine vollständige Chronologie und Dokumentation aller Vorgänge und Entscheidungen durchgeführt. Gegen Löschungen müsse nichts gesondert verfügt werden. Schon wegen des laufenden Ermittlungsverfahrens dürfe nichts gelöscht werden. Sein Haus habe der Staatsanwaltschaft, dem LKA und den anderen Behörden jederzeit alles zur Verfügung gestellt, was abgefragt worden sei, und außerdem proaktiv aufgeliefert.

Der Angriff und die Erkenntnis darüber lägen ungefähr sechseinhalb Wochen zurück. In absehbarer Zeit werde die Phase der akuten Gefahrenabwehr enden. Der ganze Aufarbeitungsprozess laufe. Die Kolleginnen und Kollegen der IT-Stelle seiner Verwaltung hätten in den zurückliegenden Wochen fast durchgängig gearbeitet, anfangs sieben Tage die Woche bis in die Nacht. Insofern hätten die Schadensbegrenzung und die Dokumentation im Vordergrund gestanden; ein Spielraum, um mit Aufarbeitungen zu beginnen, sei nicht vorhanden gewesen. Er gestehe zu, dass das aus Sicht der Abgeordneten wahrscheinlich unbefriedigend sei, zumal sein Haus die eine oder andere Frage nicht beantworten könne. Im Rahmen eines Austausches mit der Staatsanwaltschaft und dem LKA in der letzten Woche habe SenStadt die klare Ansage bekommen: „Diese Information können Sie aktuell nicht weitergeben!“ – Er bitte um Verständnis dafür, dass seine Verwaltung nicht frei darin sei, alle Informationen, die man mit den Strafverfolgungsbehörden geteilt habe, dem Ausschuss kundzutun. Zudem bereite sich SenStadt auf die Beantwortung aller Fragen und Zurverfügungstellung aller Unterlagen vor, die im Zuge des Ermittlungsverfahrens noch auf seine Verwaltung zukämen.

Zur Frage, wie die Kolleginnen und Kollegen im Vorfeld des IT-Vorfalles geschult worden seien: Wie er in einer der vergangenen Ausschusssitzungen gesagt habe, seien SenStadt und SenMVKU die einzigen Verwaltungen, die SoSafe nutzten. Mittels einer digitalen Schulungsplattform würden die Mitarbeiterinnen und Mitarbeiter beider Senatsverwaltungen fortlaufend geschult. Er habe dargelegt, dass das System ihn immer wieder daran erinnere, das nächste Modul zu aktivieren. Der Prozess höre nie auf; nach Beendigung der Schulung beginne sie von Neuem, und zwar mit neuen, aktualisierten Inhalten. Zum Inhalt der Schulung habe gehört, die Beschäftigten vor den Gefahren, die sich aus den in Rede stehenden Angriffsvektoren ergäben, zu warnen; exemplarisch nenne er eine Phishingmail. Unmittelbar nach Bekanntwerden des Angriffsvektors sei die Schulung noch einmal aktualisiert und nachgeschärft worden.

In Hinblick auf die Frage, welche weiteren Maßnahmen ergriffen würden, habe er eingangs bereits erwähnt, dass SenStadt die IT-Sicherheit unmittelbar nach dem Angriff auf ein absolutes Maximum hochgefahren habe. Es ergebe keinen Sinn, in einer Art Übersprungshandlung „irgendwelche Maßnahmen“ zu ergreifen, um ein Gefühl der Sicherheit zu erzeugen. Man warte auf den umfangreichen Bericht, der Indizien liefern solle, was vorher hätte besser sein können. Er selbst habe am ersten Tag im Kontext des Angriffs gefragt: Was sei mit der eigenen Hard- und Software? Habe es Updates gegeben? Seien irgendwelche Probleme festzustellen? – Die Antwort sei: Die Hard- und Software inklusive Virens Scanner, Firewall und Ähnlichem seien auf dem aktuellsten Stand gewesen.

Der schrittweise Wiederanlauf und Betrieb der IT von SenStadt, umfassend die Funktionalität und die IT-gestützten Prozesse, erfolge weiterhin, unabhängig von der Frage, ob der IKT-Notfall weiterhin offiziell erklärt oder für beendet erklärt sei, unter einer 24/7-Überwachung mit aktiver Eingriffsmöglichkeit und in direkter Abstimmung mit der Senatskanzlei und dem ITDZ. – Das angefragte 3a-Verfahren sei Teil des Liegenschaftswesens; dort fänden sich Datenbestände zu Liegenschaften.

Abschließend wolle er kundtun, dass er in dem gewählten Vorgehen von SenMVKU und SenStadt keinerlei Unterschiede erkennen könne. Möglicherweise sei die Umsetzung ein und derselben Entscheidung zu unterschiedlichen Zeitpunkten vorgenommen worden. Das habe auch damit zu tun, dass es sich um unterschiedliche Organisationen handele, die eine unter-

schiedliche Größe sowie voneinander zu unterscheidende Themen und Aufgaben aufwiesen. Bis zu der vergangenen Woche habe die gemeinsame Taskforce täglich getagt; mittlerweile tage sie dreimal pro Woche: montags, mittwochs und freitags. Auch darüber hinaus stimmten sich die beiden Häuser, wenn es erforderlich sei, ab. Überdies verweise er auf die gemeinsame externe Anlaufstelle. Die Öffentlichkeit sei zwar zeitlich verschieden, aber auf dem gleichen Wege informiert worden. Das liege darin begründet, dass SenMVKU deutlich eher externe Anfragen erhalten habe. Im Übrigen seien die Kolleginnen und Kollegen seiner Verwaltung zeitgleich informiert worden. Dabei seien beide Häuser durchaus unterschiedlich vorgegangen. Während Senatorin Bonde eine Videobotschaft an ihre Mitarbeiterinnen und Mitarbeiter gerichtet habe, sei im Hause von Senator Gaebler jeden Freitag eine Informationsveranstaltung mit den Abteilungsleitungen und den Stabsstellen abgehalten worden. Er selbst – Redner – habe in dieser Woche einen Termin mit allen Führungskräften seiner Verwaltung, bei dem über den aktuellen Stand berichten werde. Insgesamt sei das Vorgehen der beiden Senatsverwaltungen gut abgestimmt. Häufig habe man auf die jeweils andere Verwaltung gewartet.

Staatssekretär Arne Herz (SenMVKU) erklärt, er könne bestätigen, was sein Vorredner gesagt habe. In diesem Kontext sei darauf hinzuweisen, dass die Feststellung der Betroffenheit im Ausmaß zu unterschiedlichen Zeitpunkten geschehen sei. Daher wäre es selten möglich gewesen, zeitgleich zu handeln. Zudem wolle er in Erinnerung rufen, dass dieselbe Kanzlei, die sein Haus gebunden habe, auch SenStadt zur Verfügung gestellt worden sei. Darin sei ein einheitliches inhaltliches Handeln zu erblicken. – Eine Indexliste hätten auch die Beschäftigten von SenMVKU erhalten; er habe es zuvor nur nicht erwähnt. In der Ausschusssitzung am 7. September habe er dargelegt, dass die Mitarbeiterinnen und Mitarbeiter am selben Tag darauf hingewiesen worden seien, dass nicht ausgeschlossen werden könne, dass von allen Homelaufwerken und Verzeichnissen der Abteilung Z Daten, die die einzelnen Kolleginnen und Kollegen betreffen, abgefließen sein könnten. Zusätzlich seien den Beschäftigten Hinweise zum Umgang gegeben worden. Das von Frau Kamp erwähnte Instrument der öffentlichen Bekanntmachung diene dazu, eine Sensibilisierung für eine bestimmte abtrennbare Gruppe potenziell Betroffener zum frühestmöglichen Zeitpunkt sicherzustellen. Mit Blick auf die Frage, ob jeder, der einmal eine E-Mail an SenMVKU geschrieben habe, betroffen sein könnte, weise er darauf hin, dass man sich mit der öffentlichen Bekanntmachung an aktive und ehemalige Beschäftigte von öffentlichen und privaten Unternehmen wende, die vor dem 14. August beruflichen Kontakt zur SenMVKU gehabt hätten. Hinsichtlich verschiedenster Umstände wie öffentlicher Ausschreibungen oder Beteiligten an einem Verwaltungs- oder Gerichtsverfahren könne er nicht ausschließen, dass personenbezogene Daten abgefließen seien.

Auf die Frage des Abgeordneten Vallendar hin wiederhole er, dass seinem Haus momentan 477 Anfragen über die E-Mail-Adresse datenschutzvorfall@senmvku.berlin.de vorlägen. – Eine Zählung der Betroffenheiten sei, solange „die Datei“ nicht in Gänze bekannt sei, nicht möglich. Dafür bedürfte es einer händischen Durchsuchung der potenziell betroffenen Dateien, die nicht leistbar sei. Angesichts dieser Herausforderungen komme sowohl eine inhaltliche, durch KI unterstützte Suche zum Einsatz als auch im weiteren Verlauf ein anderer Weg, der sich auf natürliche Personen beziehe.

Dr. Maria Borelli (ITDZ; Vorständin) nimmt Stellung zu der Frage, inwiefern die Kompetenzen des ITDZ in den letzten Wochen in Anspruch genommen worden seien. In der vergangenen Woche habe es eine Informationsveranstaltung zum Cyberangriff für mehrere Landes-

behörden und Beteiligungsunternehmen gegeben, zu der auch das ITDZ von der Senatskanzlei eingeladen worden sei und teilgenommen habe. Davon abgesehen habe ihr Haus keine weiteren konkreten Aufträge von der IKT-Sicherheit erhalten. Ihr lägen Anfragen einzelner Senatsverwaltungen vor, die einen Beratungsbedarf hinsichtlich des Aufbaus von IKT-Notfallprozessen und der Eindringungserkennung hätten. Das ITDZ mit seinem Know-how und seiner Expertise stehe bereit. Viele Prozesse, die für das Land aufgebaut werden müssten und die Herr Hauer erwähnt habe, seien im ITDZ bereits implementiert worden. Das treffe beispielsweise auf das Thema ISMS zu. Jenes Informationssicherheitsmanagementsystem laufe in ihrem Haus seit Jahren und werde immer wieder im Rahmen der BSI-Auditierungen bestätigt. Auch das Business Continuity Management – in diesem Themenbereich fehle noch die Landesleitlinie – sei bereits im ITDZ implementiert worden. Demnach lägen Notfallvorsorgekonzepte und -handbücher sowie Kommunikationskonzepte für Krisen und Notfälle im ITDZ vor; ferner seien alle Rollen entsprechend besetzt und alle Ansprechpartner bekannt. Aus diesen Gründen sei es ihrem Haus gelungen, das, was sich in eigener Hoheit befinde, schnell zu monitoren und zu untersuchen. Es komme nicht nur auf die technischen Tools für die Forensik an, sondern auch auf die Prozesse.

Bei dem ITDZ sei das Cyber Defence Center der Landesverwaltung etabliert worden. Diesem obliege die permanente Analyse anhand von Monitoringdaten. Das Security Operations Center – SOC – des Cyber Defence Center greife bei Bedarf, etwa im Fall von Sicherheitspatches, operativ ein. Das Cyber Defence Center diene dem Schutz des kompletten Berliner Landesnetzes und der eigenen Infrastruktur in Rechenzentren und entsprechend aller Infrastruktur und Fachverfahren, die durch das ITDZ betrieben würden. Überdies werde auch die dezentrale Infrastruktur, die standardisiert worden sei, geschützt, Stichwort: OneIT@Berlin. Nicht umfasst von dem Schutz sei diejenige dezentrale IT, die von den Behörden und Senatsverwaltungen in eigener Verantwortung betrieben werde.

Im ITDZ gebe es auch das Computer Emergency Response Team – CERT –, das sich in ständigem Austausch mit anderen Institutionen wie dem BSI, dem LKA und dem BKA befinde. In diesem Rahmen finde ein reger Wissenstransfer in beide Richtungen statt. Das CERT sei prinzipiell für die Teilnahme an den IKT-Notfallstäben vorgesehen und dort beratend tätig; es erstatte bei IT-Sicherheitsvorfällen Bericht an den Landesbeauftragten für Informationssicherheit.

Unter bestimmten Rahmenbedingungen könnten die im ITDZ bestehenden Einheiten und Instrumente auch anderen Stellen im Land Berlin zugutekommen. Zuallererst komme es auf eine verbindliche Finanzierung an. Es bedürfe konkreter Aufträge, um die für das ITDZ aufgebaute Infrastruktur skalieren zu können, sowie der entsprechenden Prozesse und des entsprechenden Personals. Außerdem werde mit Blick auf Verantwortlichkeiten und Zuständigkeiten eine verbindliche Rollenklärung zwischen dem ITDZ, der IKT-Sicherheit und den Verwaltungen benötigt. Ferner brauche es allgemeine und für alle geltende IT-Sicherheitsstandards. Es nutze nichts, wenn immer nur das ITDZ sich vom BSI zertifizieren lasse und diese hohen Anforderungen dann nur für ihr Haus, nicht aber für die anderen Infrastrukturen Geltung beanspruchten.

Was die Frage nach anderen Eindringungserkennungstools betreffe, könne sie berichten, dass sich das ITDZ bereits seit 2024 damit beschäftige. In Zusammenarbeit mit der IKT-Steuerung habe man damals an einer Lösung gearbeitet, doch sei die Finanzierung jener Lösung gestri-

chen worden. Daraufhin habe sie die damalige CDO Frau Klement auf die Folgen dessen angesprochen. Indes habe das ITDZ die Lösung in Eigenregie für das eigene Haus weiterentwickelt. Angesichts der finanziellen Situation habe dies nicht so schnell erfolgen können, wie es nötig gewesen wäre. Mittlerweile stehe die Lösung; ab Oktober werde sie ausgerollt. Ihr sei eine Senatsverwaltung bekannt, die schon ihr Interesse daran bekundet habe und bei der die Lösung zum Einsatz kommen werde.

Gegen CrowdStrike habe sie keine Einwendungen. Es handele sich um ein mächtiges Tool. Ein Hauptkritikpunkt daran sei jedoch, dass die zentrale Analyse der Daten, die das Werkzeug sammle, um Angriffe zu entdecken, nur auf Servern von CrowdStrike in den USA stattfinden könne. – Das ITDZ habe sich für eine Lösung entschieden, bei der die Möglichkeit bestehe, diese zentralen Analyseserver in der ITDZ-Cloud zu betreiben. Die Frage danach, wo die Daten blieben und was mit ihnen passiere, erübrigte sich dann. – Nichtsdestotrotz sei es für akute Notfälle wie den in Rede stehenden wichtig, sich auf eine Auswahl von Tools zu stützen. Ein Werkzeug allein genüge nicht. Im Sinne der digitalen Souveränität erscheine es sinnvoller, mehrere Werkzeuge einzusetzen.

Dr. Olaf Kroll-Peters (Skzl; Landesbevollmächtigter für Informationssicherheit) begrüßt, dass in der Diskussion bereits die Stichworte Standardisieren und Segmentieren gefallen seien. Es freute ihn, wenn in dieser Hinsicht künftig Fortschritte erzielt werden könnten. – Aufgrund der Passwortdebatte habe man eine Umfrage im Land Berlin durchgeführt. Er persönlich habe telefonisch 53 Antworten erhalten, wonach die Lage sehr unterschiedlich sei. Die angesprochene Multi-Faktor-Authentifizierung könne in vielen Fällen nicht eingesteuert werden. In einem ersten Schritt sei nun ermittelt worden, in welchen Systemen die vorgegebenen 16 Zeichen für Passwörter nicht funktionierten. Gemeinsam mit dem BSI werde eine Strategie angestrebt, wie jene Systeme „gekapselt“ oder individuell behandelt werden könnten. Dafür bedürfe es einer Einzelfallbetrachtung. Näheres zum erwähnten LABO werde er öffentlich nicht kundtun; das könne bei Interesse bilateral erfolgen. – Unter anderem bei „unserem Dienstleister“ gebe es Systeme, für die 16 Zeichen zu viel seien. – Laut BSI wiederum seien selbst 16 Zeichen zu wenig für Passwörter; besser wären 20 bis 25 Zeichen. In der Kürze der Zeit könne er die Berliner Verwaltung davon nicht überzeugen.

Warum sei man gleichsam mit einem blauen Auge davongekommen? – Ergänzend zu den bisherigen Ausführungen weise er darauf hin, dass bereits Werkzeuge auf den Systemen gesehen worden seien, die das, was Herr Hauer angesprochen habe, einfach hätten machen können – wenn jemand „raufgedrückt“ hätte. Insofern habe mit Glück gehabt, das kurz vorher noch gesehen zu haben; andernfalls wären die Auswirkungen bei Weitem gravierender gewesen. Auf das, was die Accounts, die er in der vorletzten Sitzung im nichtöffentlichen Teil erwähnt habe, alles hätten machen können, wolle er an dieser Stelle nicht eingehen; man habe nichts gesehen, was wirklich ausgeführt worden sei.

Die Idee, einmal zu schauen, was andere im Einsatz hätten, finde er gut. Auf der Tagung der CISO – Chief Information Security Officers –, die am Folgetag in Berlin stattfinden werde, sei eine Befassung damit geplant. Mittlerweile schaue man sich nicht nur CrowdStrike, sondern auch andere Systeme an. Momentan laufe noch die Gefahrenabwehr. Das bedeute, die konkrete Bedrohung könne gesehen und eliminiert werden. Das heiße nicht, dass es keine anderen Gefahren gebe. Das leite über zum Stichwort Trittbrettfahrer: Vor zwei Minuten habe er erneut eine Nachricht in diesem Zusammenhang erhalten. Natürlich gebe es Menschen, die

die in Rede stehenden Daten hätten und versuchten, damit „etwas anderes“ zu machen. – Nach der Gefahrenabwehr stehe eine Bereinigung an. Die Werkzeuge hätten einige Fingerzeige gegeben, in welchen Bereichen – Passwörter, Zertifikate, Segmentierung – Veränderungen durchaus sinnvoll wären.

Den Ausführungen von Frau Dr. Borelli entnehme er, dass davon auszugehen sei, dass der landesweite ISMS-Dienst in diesem Jahr nach einer gewissen Verzögerung in Betrieb genommen werden könne. Das begrüße er in seiner Funktion.

Klarstellen wolle er, dass sich die beauftragten CrowdStrike-Server in Frankfurt am Main befänden. Gleichzeitig sei allgemein bekannt, was „beauftragt“ bedeute und wie die reale Welt tickte. Er persönlich wolle hinschauen, dass alles seine Richtigkeit habe. Mit Frau Kamp sei er sich einig, dass in dem Bereich „noch ein bisschen aufgeräumt“ werden müsse.

Stefan Ziller (GRÜNE) verleiht der Auffassung Ausdruck, dass einige Fragen nicht zufriedenstellend beantwortet worden seien. Vor dem Hintergrund, dass einige Kanzleien Sammelklagen vorbereiteten, hätte er sich nach sechs Wochen zumindest eine grobe Einschätzung gewünscht, unter welchen Bedingungen das Land schadensersatzpflichtig sei. Bezüglich der Ansicht, dass die verfügbaren Daten nicht auf Betroffenheiten überprüfbar seien, wolle er exemplarisch darauf verweisen, dass eine einfache Testung ergeben könnte, wie viele E-Mail-Adressen in dem Datensatz enthalten seien. Die betreffenden Personen könnten dann angeschrieben und darüber informiert werden, dass ihre E-Mail-Adressen dort auftauchten. Mithin hätte er sich mehr Bemühen gewünscht, um die Betroffenheiten herauszufinden und Personen zu identifizieren. Nach seinem Verständnis sei es sehr wohl möglich, genauer hinzusehen. Möglicherweise sage aber das LKA dem Senat, dass er dies nicht tun oder nicht darüber reden dürfe.

Besonders unbefriedigend erscheine die Unklarheit darüber, welche Schritte als Nächstes folgen müssten. Laut ITDZ fänden keine Gespräche statt; es sei zu einer Informationsveranstaltung eingeladen worden. Ihn interessiere, wann damit begonnen werde, die IKT-Architektur der nächsten Jahre miteinander abzustimmen. Wann werde welcher Schritt in Richtung Zentralisierung gegangen, und wann werde wer mitgenommen? Existiere wenigstens ein interner Entwurf für eine IKT-Architektur, die eine Segmentierung vorsehe? – Er habe nicht das Gefühl, dass der Senat an solchen Dingen arbeite; das sei bitter.

Tobias Schulze (LINKE) kommt zurück auf die Aussage, dass die Bestandsaufnahme zur IKT-Infrastruktur laufe: Seine Frage habe sich jedoch auf die jahrelangen Vorarbeiten dafür bezogen. Welche Vorarbeiten seien vorhanden, und warum würden dennoch immer noch Fachverfahren entdeckt?

Darüber hinaus wolle er ansprechen, dass die Hackergruppe im Netz ein weiteres Archiv zur Verfügung gestellt habe, von wo aus die Daten abrufbar seien. Begründet werde dieses Vorgehen mit der hohen Nachfrage. – Habe das eine Beschleunigung des Downloads bewirkt? Ferner: Sei mittlerweile näher bekannt, wie viele geheime Dateien darunter seien?

Staatssekretär Florian Hauer (Skzl) wiederholt, dass über Schadensersatzansprüche und dergleichen nicht pauschal geurteilt werden könne. Stattdessen bedürfe es einer einzelfallbezogenen Betrachtung und juristischen Prüfung. Hier stelle sich etwa die Frage, ob fahrlässiges

Verhalten vorliege, oder wie es zu werten sei, wenn es sich um Daten von Beschäftigten handle, denen selbst Fehler unterlaufen seien.

Was die Frage nach den nächsten Schritten angehe, habe er stets betont, dass zunächst das akute Krisenmanagement im Vordergrund stehe. Wenn diese Phase abgeschlossen sei, werde man sich einer umfassenden Ursachenanalyse zuwenden. Allerdings habe der Senat in den vergangenen zwei, drei Wochen auch im Rahmen des akuten Krisenmanagements einige Punkte erkannt, die sich aufdrängten. Diese Punkte, die nun zügig anzugehen seien, habe er eingangs genannt. Mit Blick auf große strukturelle Reformen habe er in der Vergangenheit bereits deutlich gemacht, dass man tendenziell nicht um mehr Zentralisierung herumkomme. Das beziehe sich etwa auf die Steuerbarkeit und Durchgriffsrechte. Zudem habe er vorhin die Idee eines IT-Sicherheitsgesetzes mit einem Chief Information Security Officer, der bei einem IT-Vorfall umfassende Rechte ausüben könnte, aufgegriffen. Derlei Dinge leuchteten ihm sofort ein; diese Idee sei intern auch schon geäußert worden. Fakt sei, dass die Strukturen nur auf gesetzlicher Grundlage geändert werden könnten. Notwendig seien solche Änderungen unbestritten, doch sei das eine Aufgabe für die neue Legislaturperiode. In diesem Kontext erinnere er an sein Angebot, dass die Senatskanzlei Empfehlungen aufschreibe, die in den Koalitionsverhandlungen genutzt werden könnten. Dabei werde es gewiss auch möglich sein, die Ideen mit einem näherungsweisen „Preisschild“ zu versehen.

Mit Blick auf die Bestandsaufnahme bezüglich der IKT-Architektur und den dazugehörigen Vorlauf mache er geltend, dass er damals noch keine Verantwortung dafür getragen habe. Daher könne er nur vermuten, dass die Dinge seinerzeit nicht abschließend beantwortet worden seien oder man nicht alles selbst gesehen und aufgeschrieben habe. Wie dargestellt, sei die Bestandsaufnahme vor dem Hintergrund der aktuellen Geschehnisse nun erneut gestartet worden. Er gehe davon aus, dass die Informationen nunmehr mit der nötigen Ernsthaftigkeit, Sensibilität und Dringlichkeit fristgerecht geliefert würden, sodass die Bestandsaufnahme umfassend und abschließend durchgeführt werden könne.

Er bitte seinen Vorredner, die Frage nach dem Archiv noch einmal zu wiederholen.

Tobias Schulze (LINKE) bemerkt, er wolle wissen, ob der Download der Daten nun, wo die Hackergruppe ein zweites Archiv in das Darknet gestellt habe, schneller vonstattengehe.

Staatssekretär Florian Hauer (Skzl) bekundet, das könne er nicht beurteilen. Dem Vernehmen nach gehe es auch da nach wie vor langsam vonstatten. Anders, als es sich die Sicherheitsbehörden gewünscht hätten, sei es nicht möglich, das komplette Datenpaket innerhalb weniger Tage herunterzuladen, zu separieren und abzusichern. Nach wie vor habe man es mit einer geringen Bandbreite zu tun.

Der Klarstellung halber wolle er anfügen, dass die Senatskanzlei in Gestalt des Landesbevollmächtigten für Informationssicherheit und des IKT-Notfallstabs in den Wochen seit dem Cyberangriff sehr eng mit dem ITDZ zusammengearbeitet habe. In allen Notfallstäben, dem gewöhnlichen wie auch dem Extranotfallstab in Vorbereitung und Absicherung der Wahlen, sei das ITDZ vertreten gewesen. Auf operativer Ebene gebe es eine enge wie gute Zusammenarbeit.

Staatssekretär Arne Herz (SenMVKU) kommt auf den Wortbeitrag des Abgeordneten Ziller zu sprechen, der zu wenig Bemühen beklagt habe. Er selbst – Redner – als Nichtinformatiker vermöge nicht zu beurteilen, ob es so einfach wäre, wie der Angesprochene es dargestellt habe. Allerdings treffe die Beschreibung auf das, was die Kolleginnen und Kollegen, aber auch die Verantwortlichen der Häuser leisteten, durchaus nicht zu. Unbenommen davon sei eine jede Person nicht immer mit jedem Ergebnis zu jedem Zeitpunkt zufrieden. Die genauen Dateien, in denen man dann suchte, seien noch nicht bekannt. Dort, wo Betroffenheiten schon jetzt identifiziert oder zumindest umrissen werden könnten, werde versucht, dies in Form der öffentlichen oder konkreten Bekanntmachung zu vermitteln. Gleichzeitig gebe man senatsseitig sowohl den Beschäftigten als auch externen Betroffenen Instrumente bzw. Empfehlungen an die Hand, wie sie mit den Behörden umgehen könnten, sollten und dürften und wie sie sich selbst schützen könnten. Das, was jeweils an Möglichkeiten und Erkenntnissen vorhanden sei, werde weiterhin in konkretes Handeln umgesetzt, um sowohl aufzuklären als auch einen Umgang zu finden und dabei die Häuser zukunftsfest aufzustellen.

Vorsitzender Johannes Kraft hält fest, dass die Besprechungen zu den Punkten 3 a und 3 b damit abgeschlossen seien.

Punkt 4 der Tagesordnung

Verschiedenes

Siehe Beschlussprotokoll.