Abgeordnetenhaus BERLIN

19. Wahlperiode

Plenar- und Ausschussdienst

Inhaltsprotokoll

Öffentliche Sitzung

Ausschuss für Digitalisierung und Datenschutz

– zu TOP 2 teilweise nichtöffentlich –

8. Sitzung
18. Mai 2022

Beginn: 09.38 Uhr
Schluss: 11.37 Uhr
Vorsitz: Christian Wolf (FDP)

Vor Eintritt in die Tagesordnung

Siehe Beschlussprotokoll.

Punkt 1 der Tagesordnung

Aktuelle Viertelstunde

Keine Wortmeldungen.

Punkt 2 der Tagesordnung

Besprechung gemäß § 21 Abs. 3 GO Abghs 0018
Digitale Sicherheit der Berliner Verwaltung DiDat
(auf Antrag der Fraktion der SPD, der Fraktion Bündnis 90/Die Grünen und der Fraktion Die Linke)

Tobias Schulze (LINKE) führt aus, sensible Daten auf Servern erforderten ein hohes Maß an IT-Sicherheit. Die Beispiele am Kammergericht und der TU Berlin zeigten zudem die Folgen gelungener Angriffe für Funktionalität. Die Eröffnung des Security-Operations-Centers im ITDZ und die aktuell angespannte Situation seien ein Anlass, sich dem Thema zu widmen.

Staatssekretär Dr. Ralf Kleindiek (SenInnDS) merkt an, er wolle zunächst über den Hackerangriff vom 14. Mai 2022 berichten. Dazu müsse Vertraulichkeit hergestellt werden.

Vorsitzender Christian Wolf stellt Einvernehmen fest, die Öffentlichkeit auszuschließen.

Weitere Beratung siehe nichtöffentliche Anlage zum Inhaltsprotokoll.

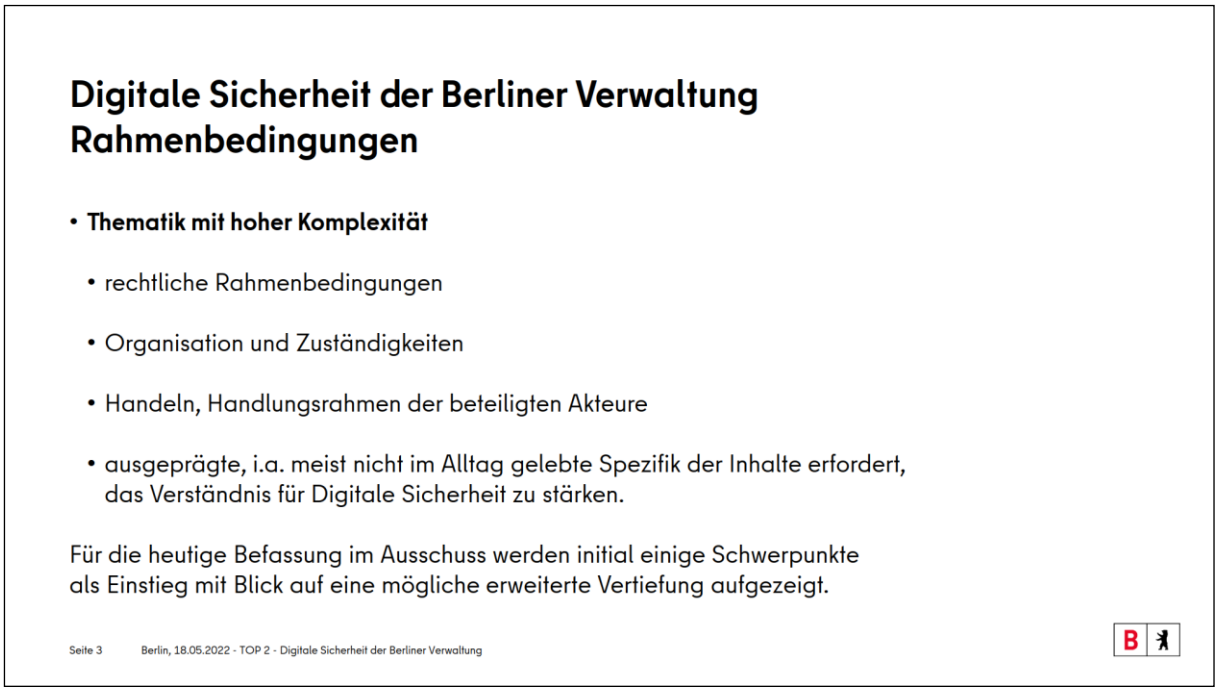
Vorsitzender Christian Wolf stellt die Öffentlichkeit wieder her.

Staatssekretär Dr. Ralf Kleindiek (SenInnDS) betont, Berlin müsse sich darauf einstellen, Ziel von Cyberattacken zu sein. Daten-, IT- und digitale Sicherheit seien wesentlich.

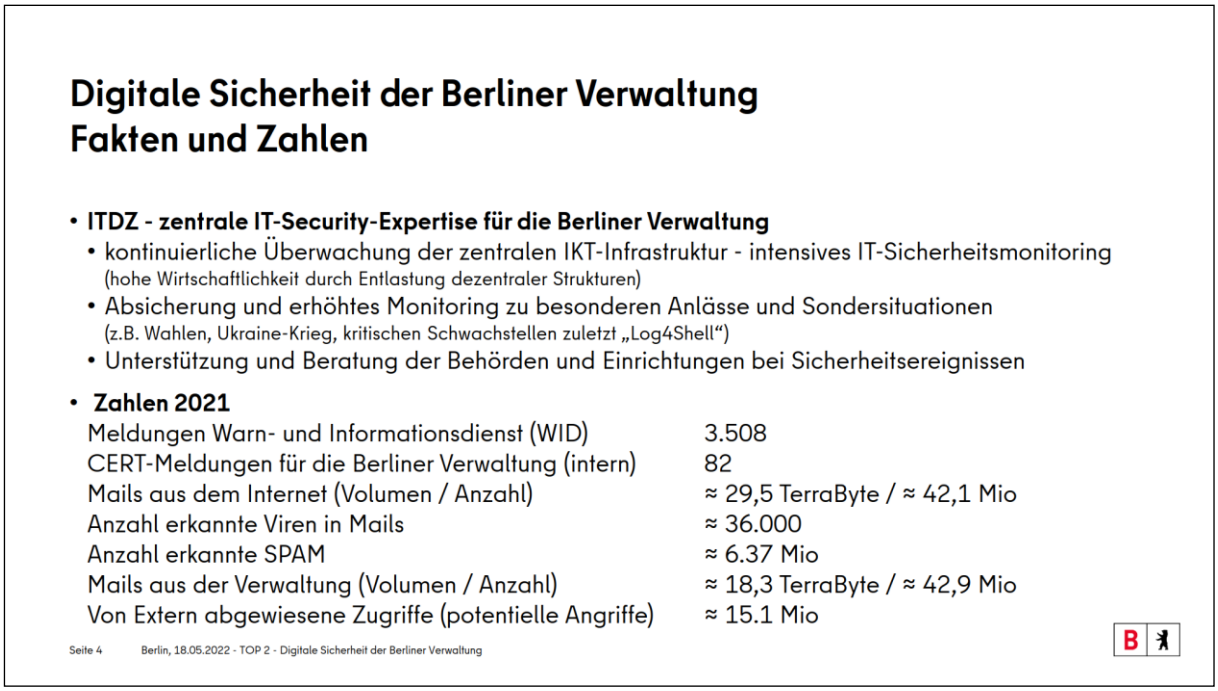
Klaus-Peter Waniek (SenInnDS; Landes-InfSiBe) erläutert, IT-Sicherheit sei die Sicherheit von IT-Systemen. Informationssicherheit wiederum schließe die IT-Sicherheit ein, enthält aber auch den Schutz digitaler und nicht digitaler Informationen. Cybersicherheit enthalte alle Technologien und Prozesse im Internet, und digitale Sicherheit umfasse den Schutz der Besitztümer und Personen im digitalen Raum.

Die relevanten Rechtsnormen hätten Rahmen und Abgrenzung voneinander, sodass unterschiedliche Organisationen und Zuständigkeiten gegeben seien. Bei den jeweiligen Organisationen könne er um Auskunft bitten oder Unterstützung anbieten.

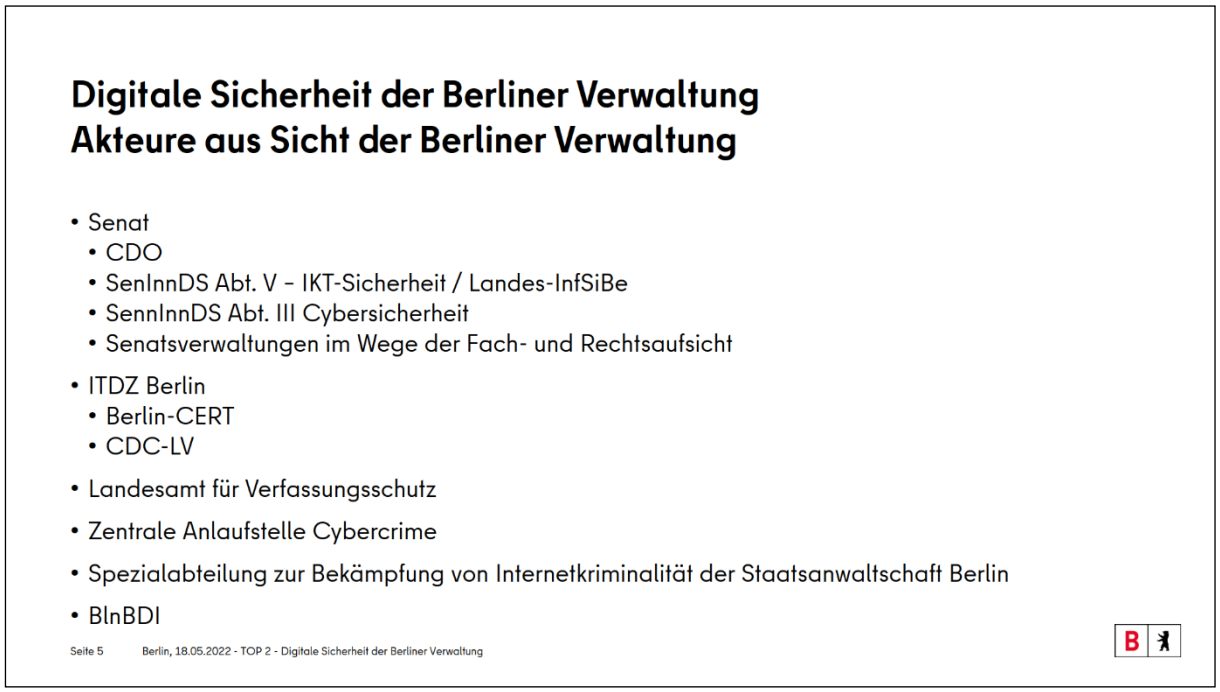
Die zentrale Sicherheitsexpertise liege beim ITDZ. Es überwache die zentrale IKT-Infrastruktur, und sichere dadurch auch die dezentralen Strukturen. Das Monitoring werde zudem anlassbezogen verstärkt, zum Beispiel zur vergangenen Wahl oder beim aktuellen Krieg in der Ukraine. Dabei sei es auch wichtig, Geräte mit Schwachstellen zu erkennen. Seine Stelle unterstütze Behörden und interpretiere regelmäßig CERT-Warnmeldungen und verteile diese an alle Sicherheitsbeauftragten.

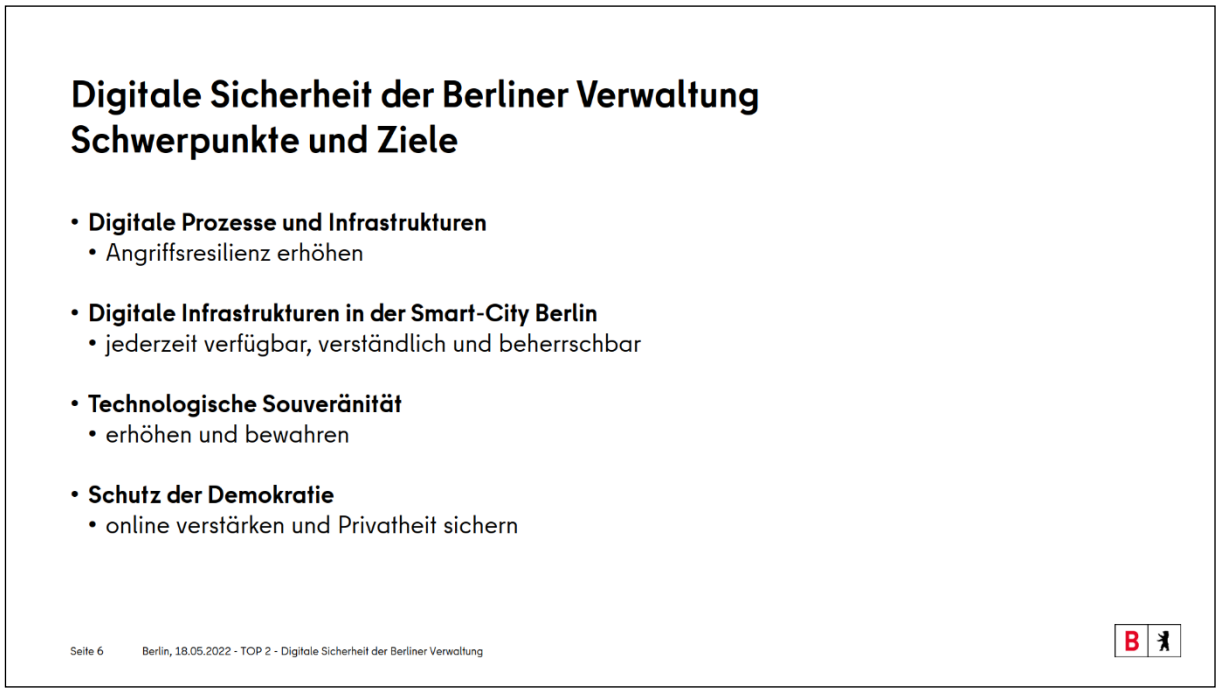


Seine Stelle habe 3 508 Warnmeldungen gegeben – siehe nächste Folie –, davon 82 interpretierte Warnmeldungen. Es seien 36 000 Viren in Mails erkannt worden. Betroffene Mails seien nicht zugestellt worden. 6,37 Mio. Mails seien als Spam erkannt worden. Es seien 42,1 Mio. Mails empfangen und 42,9 Mio. Mails versendet worden. 15,1 Mio. Zugriffe auf die Website seien abgewiesen worden, weil diese über einen anderen Port erfolgt seien als beim Aufruf mit dem Browser üblich, zum Beispiel auch Portscans.

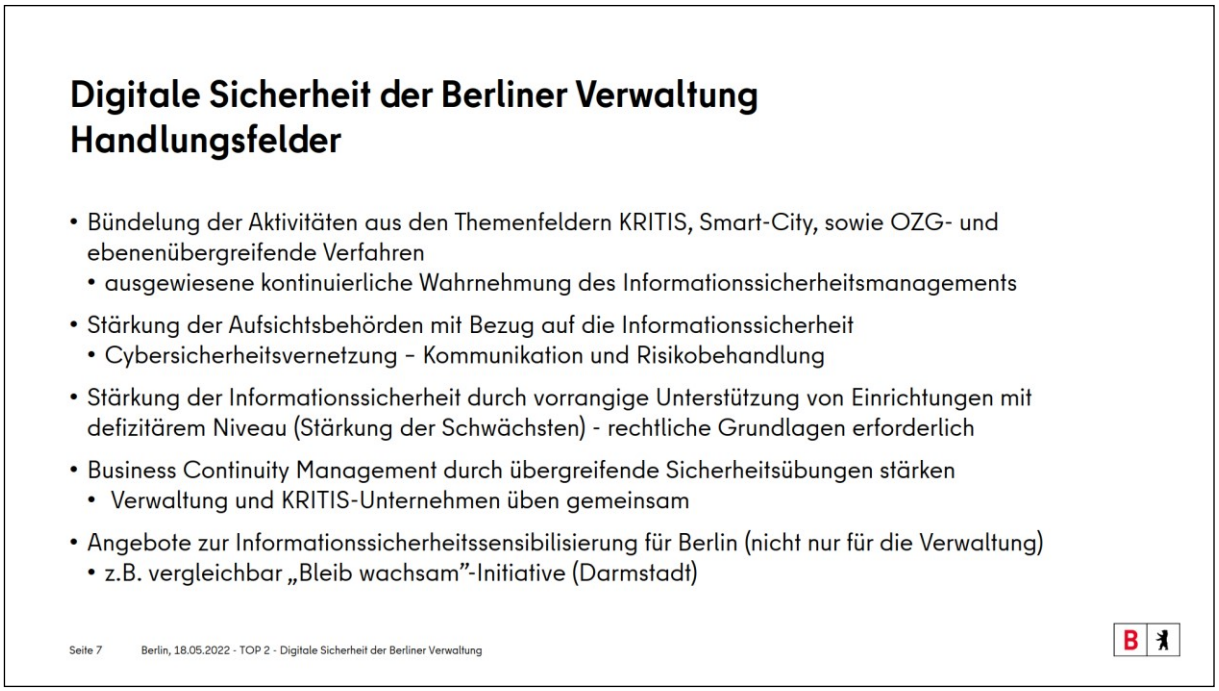


Zu den relevanten Akteuren für die Sicherheit in der Berliner Verwaltung – siehe nächste Folie – gehörten der Senat, das ITDZ, das Landesamt für Verfassungsschutz, die Zentrale Anlaufstelle Cybercrime, die Zentralstelle Bekämpfung der Organisierten Kriminalität der Generalstaatsanwaltschaft Berlin und BlnBDI. Mit letzterem sei eine enge Zusammenarbeit notwendig, weil in der Datenschutz-Grundverordnung festgehalten sei, dass Informationssicherheit die Basis für Datenschutz sei. Die schließe Grundsätze wie das Gebot der minimalsten Datenerhebung ein.





Zu den Schwerpunkten und Zielen – siehe vorherige Folie – gehörten eine hohe Angriffsresilienz, digitale Infrastrukturen und die Smart-City, technologische Souveränität bei Software und Hardware und der Schutz der Demokratie einschließlich des Schutzes der Persönlichkeitsrechte und der Privatheit.



Zu Handlungsfelder für die digitale Sicherheit der Berliner Verwaltung gehörten die Aktivitäten von KRITIS, Smart-City und OZG- und ebenenübergreifenden Verfahren. Diese Aktivitäten müssten gebündelt werden, weil hier die die Informationen der Bürger zusammenliefen. Informationssicherheitsmanagement sei eine kontinuierliche Aufgabe. Dazu gehörten auch Meldewege, wenn sich an einem Punkt ein Sicherheitsvorfall ereigne.

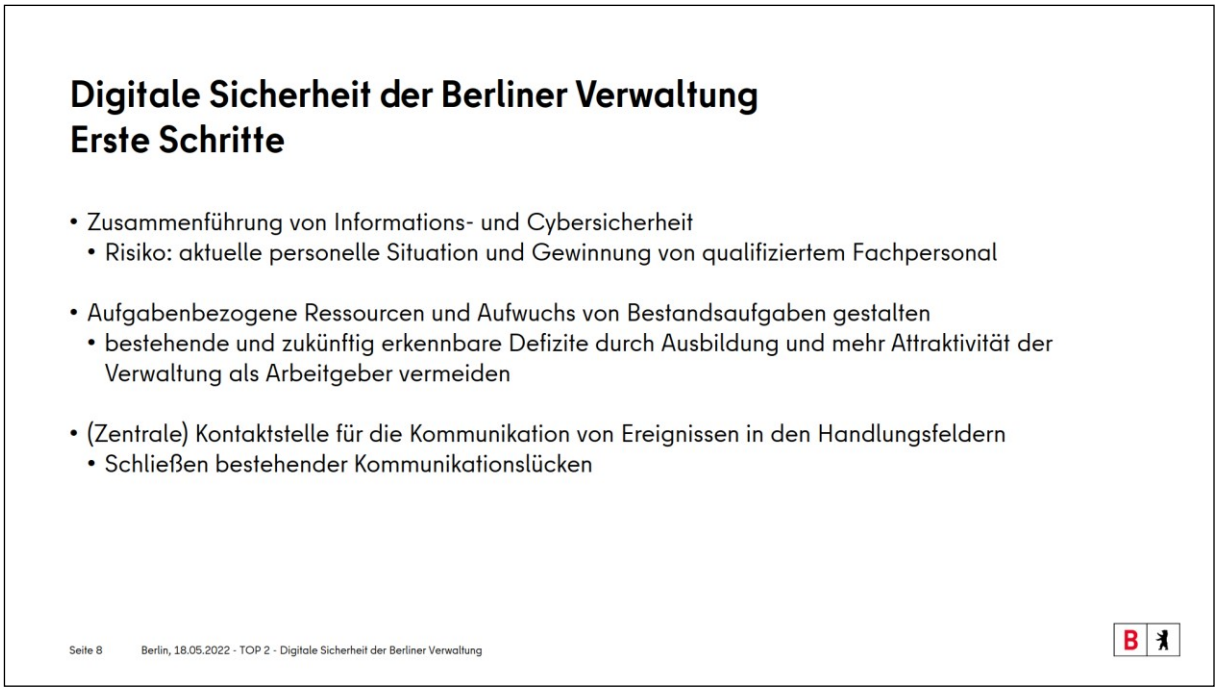
Die verantwortlichen Aufsichtsbehörden müssten in ihren Rechten gestärkt werden.

Gestärkt werden müssten zudem die schwächsten Verwaltungen. Dies betreffe die Bezirke in der Praxis weniger als andere Verwaltungen, die noch nicht im Fokus seien. Dafür müsse die Politik Haushaltsmittel vorsehen.

Eine weitere Maßnahme seien Sicherheitsübungen im Sinne von Urban Continuity-Management, um die Verfügbarkeit von Verwaltungsdienstleistungen zu stärken.

Zuletzt müssten Verwaltung und Bürger auf Maßnahmen zur Informationssicherheitssensibilisierung zugreifen können.

Ein erster in Planung befindlicher Schritt sei es, Informations- und Cybersicherheit zusammenzuführen – siehe nächste Folie. Die Verwaltungen müssten dafür qualifiziertes Fachpersonal gewinnen, auch durch Ausbildung. Um Informationslücken zu schließen, biete es sich zudem an, eine zentrale Kontaktstelle für Ereignisse im Sinne der aufgezählten Handlungsfelder einzurichten.



Stephan Standfuß (CDU) erkundigt sich, ob manche Teile der Verwaltungen nicht ans ITDZ angebunden seien. Wie seien die geschützt?

Was seien zudem die Standards wie zum Beispiel Zertifizierungen des ITDZ?

Wie sei der Schutz des Landesnetzes gestaltet?

Tobias Schulze (LINKE) will wissen, was das Security-Operations-Centers von bisher bestehenden Organisationseinheiten zur Cybersicherheit unterscheide.

Seien verpflichtende Sicherheitsschulungen für Verwaltungsbeschäftigte denkbar? Unachtsamkeit sei ein großes Sicherheitsproblem, wie das Beispiel des Kammergerichts zeige.

Stefan Ziller (GRÜNE) bittet darum, die Anwesenden mögen den bundesweiten Digitaltag in ihren Netzwerken bewerben und für IT-Sicherheitssensibilisierung nutzen. Es sei zudem überlegenswert, den Stadtteilzentren zentral Unterstützung anzubieten.

Wie unabhängig müsse IT-Sicherheit von der Verwaltung sein, und in welchem Maße müsse es gegenüber anderen Interessen priorisiert werden?

Das Know-how des CERT müsse weiterentwickelt werden. Die Landespolitik müsse überlegen, ob ein Landesamt für Sicherheit in der Informationstechnik sinnvoll sei, wie verschiedene Akteure im Bereich IT-Sicherheit gebündelt werden könnten und wie kleine und mittelständische Unternehmen im Land, die sich keine IT-Fachkräfte leisten könnten, gebündelt auf Know-how zugreifen könnten.

Auf Verwaltungsfesten könne IT-Sicherheit möglicherweise als Erlebnis vermittelt werden. Attacken könnten nie ausgeschlossen werden, aber Berlin sei auf einem guten Weg.

Marc Vallendar (AfD) erkundigt sich, ob unabhängig von der Firewall des ITDZ für das Berliner Landesnetz noch Landesbehörden direkt ans Internet angebunden seien. Wenn ja, wer kümmere sich um diese Sicherheitsaspekte, und wann werde der Zugang zum direkten Internet abgeschaltet und die Behörden in die Verwaltung des ITDZ eingegliedert?

Dass viele Arbeitsplatzrechner in den Bezirken dezentral verwaltet würden, stehe einem berlineinheitlichen Sicherheitsstandard im Weg. Ab wann könne das ITDZ Arbeitsplatzrechner verwalten, und wann sei die notwendige Migrationsreadiness hergestellt?

Beabsichtige die Verwaltung, sich von Microsoft abzukehren und die Arbeitsplatzrechner mit einem Open-Source-Betriebssystem zu betreiben? Sei weiterhin beabsichtigt, Dokumentenanzeigeprogramme zu verwenden, die nicht erforderten, Dokumente direkt auf dem Arbeitsplatzrechner abzuspeichern?

Plane die Verwaltung zur Sicherheit innerhalb der Behörden Reviews und stichprobenartige Kontrollen der Zulieferer und technischer Maßnahmen im ITDZ, um Risiko zu minimieren? Plane das ITDZ, Firewalling zwischen einzelnen IKT-Fachverfahren anzuwenden, um Behörden auch untereinander zu schützen?

Fertige das ITDZ Mehrfach-Back-ups an, oder seien solche geplant?

Seien beim Black-out-Notbetriebskonzept der Verwaltung Fortschritte erzielt worden?

Roman-Francesco Rogat (FDP) legt dar, dass die Attackensteigerung bei über 90 Prozent liege. Gleichzeitig betrage Berlins Reifegrad laut IT-Sicherheitsbericht im Schnitt 60 Prozent, die Weiterentwicklung nur 1,8 Prozent. Es sei zu Beginn des Tagesordnungspunktes berichtet worden, dass es ein paar Vorkehrungen gebe. Die reichten aber nicht aus. Es sei zwar beruhigend, dass das ITDZ im Sicherheitsreifegrad 100 Prozent erreiche, aber wie könne Berlin es schaffen, den Schnitt zu verbessern und Ausreißer zu vermeiden?

Der IT-Sicherheitsbericht zeige zudem eine Spreizung des Sicherheitsreifegrad von 4 Prozent bis – dank ITDZ – 100 Prozent. Wie könnten Ausreißer nach unten vermieden werden?

Das Informationssicherheitsmanagementteam habe laut Bericht keine zugewiesenen Aufgaben, sondern sei nur beratend tätig, was nicht der BSI-Empfehlung entspreche. Plane die Senatsverwaltung Änderungen?

Seien Schulungen geplant, die nicht nur auf Phishing abzielten, sondern auch auf Informationssicherheit?

Das ausgeschriebene Informationssicherheitstool komme noch nicht flächendeckend zum Einsatz. Wie sei dabei der Stand?

Habe das Security-Operations-Center reibungslos seine Arbeit aufgenommen?

Die IT-Sicherheitsverordnung Portalverbund sei im Januar in Kraft getreten. Wie wirke sich das auf die OZG-Leistungen des Land Berlins aus?

Dr. Matthias Kollatz (SPD) will wissen, wo neben den Gerichten die wichtigsten Baustellen seien und wie schnell Unzulänglichkeiten beseitigt werden könnten.

Einige IT-Anwendungen mit großen Nutzerzahlen wie Konferenzmodalitäten und Onlinelehrveranstaltungen der Verwaltungsakademie Berlin seien noch nicht von der Firewall des ITDZ geschützt, weil sie sonst nicht betriebsfähig seien. Sei es sinnvoll, kritische und weniger kritische Anwendungen zu unterscheiden, anstatt alles durch eine Firewall zu schützen?

Christian Wolf (FDP) merkt an, bei 42,1 Mio. eingehenden und 42,9 Mio. ausgehenden Mails seien dies auf 200 Arbeitstage und 80 000 Beschäftigte gerechnet 2,6 eingehende Mails und 2,7 ausgehende Mails je Beschäftigtem. Die Zahl sei niedrig. Würden Mails verschickt, die nicht in der Statistik auftauchten?

Jan Lehmann (SPD) erkundigt sich, wie Warnmeldungen priorisiert würden.

Stephan Standfuß (CDU) fragt, wann der letzte IT-Sicherheitsbericht veröffentlicht worden sei und wie häufig er aktualisiert werde. Hätten alle Berliner Bezirke Sicherheitsbeauftragte? Wie seien sie organisiert, seien es Voll- oder Teilzeitstellen? Welche Qualifikationen hätten die Sicherheitsbeauftragten? Wie würden sie fortgebildet und sensibilisiert? Welche weiteren Maßnahmen könnten Sicherheit in den Bezirken verbessern?

Staatssekretär Dr. Ralf Kleindiek (SenInnDS) weist darauf hin, dass er auf Bewertungen der Vorkehrungen aus dem nichtöffentlichen Teil nur nichtöffentlich Stellung nehmen könne.

Das ITDZ erhalte in Kürze die zweite Sicherheitszertifizierung durch das BSI.

Das Security-Operations-Center biete eine Bündelung und bessere Operationalisierung im Fall von Sicherheitsvorkommnissen. Es erleichtere die Zusammenarbeit innerhalb Berlins, mit den Bezirken, zwischen den Verwaltungen und mit Stellen außerhalb des Landes und erlaube, Informationen besser zu verwerten und Gefahrensituationen besser zu bearbeiten.

Schulungen zur IT-Sicherheit seien notwendig, aber SenInnDS habe noch keine abschließende Meinung zu verpflichtenden Schulungen. Er wolle es von einer Bestandsaufnahme abhängig machen und mit einzelnen Verwaltungen diskutieren.

Die Anregungen zum nächsten Digitaltag am 24. Juni 2022 und zur Erlebnisorientiertheit von IT-Sicherheit nehme er auf. Für Sommerfeste habe SenInnDS keine Planungen.

Im Koalitionsvertrag sei der Prüfauftrag beschrieben, ob ein Landesbevollmächtigter für Informationssicherheit als unabhängige Stelle eingerichtet werden solle. Dies sei nur sinnvoll, wenn es passende Rahmenbedingungen gebe, wie zum Beispiel qualifiziertes Personal. Daran arbeite er zusammen mit SenFin.

Die vom Abgeordneten Vallendar angesprochenen Punkte seien gute Gründe für das Migrationsprogramm. Bis Ende 2024 solle die Migration der Hauptverwaltungen abgeschlossen sein. Das Kernstück sei der BerlinPC, der einen Standard in Sicherheit bieten solle.

Open Source werde immer eine Abwägung sein, auch unter Berücksichtigung von digitaler Sicherheit, digitaler Souveränität, Funktionalität und Stabilität. Dafür werde im ITDZ ein Open-Source-Kompetenzzentrum eingerichtet, das Verwaltungen Beratung anbiete.

Auf Stromausfälle sei Berlin mit redundanten Systemen, Generatoren und Batterieversorgung vorbereitet.

Eine allgemeine wichtige Baustelle sei die Zentralisierung beim ITDZ. Bis dahin seien Sensibilisierung und gute Zusammenarbeit notwendig. Er könne keine konkrete Verwaltung nennen, die vor den größten Herausforderungen stehe.

Sicherheit, Datenschutzkonformität und Funktionalität stünden immer in einem Zielkonflikt. Laptops für Auszubildende an der Verwaltungsakademie seien nach Abwägung beispielsweise nicht an das Landesnetz angeschlossen.

Klaus-Peter Waniek (SenInnDS; Landes-InfSiBe) weist darauf hin, dass im Oktober wie jedes Jahr der European Cyber-Security-Month stattfinde.

Zur Gamification von Cybersicherheit forschten auch Hochschulen. Die TH Wildau sei ein Beispiel und biete zudem Ausbildungskurse für Informationssicherheitsbeauftragte geprüft nach BSI an.

Informationssicherheit sei ein ständiger Prozess, für den Einrichtungen Verantwortung übernehmen müssten.

Die Kommunikation müsse – für den Anschluss an die Netze des Bundes verpflichtend – in Zukunft immer über das Netz des ITDZ laufen, auch mit Drittnetzen, die dadurch aber nicht grundsätzlich ausgeschlossen seien.

Die VAK sei durch die Freiheit von Forschung und Lehre nicht komplett ins Landesnetz eingebunden. Manche Regularien lägen außerhalb des EGovG.

Verfahren innerhalb des ITDZ würden gemäß Schutzbedarf betrieben. Die Netzverfahren seien bei hohem Schutzbedarf gegeneinander abgeschottet. Bei den Verfahren in Eigenverantwortung gehe er davon aus, dass die Verwaltungen die Standards des BSI umsetzten und ihre Selbstauskunft entsprechend vornähmen. Gleiches gelte für Zulieferer.

Eine nach EGovG abnahmepflichtige Behörde, die nicht über den Einzelplan 25 finanziert werde, sondern mit einem eigenen Wirtschaftsplan arbeiten müsse, bringe das manchmal finanzielle Probleme, alle Anforderungen über die Fachaufgabe hinaus zu erfüllen. So kämen Spreizungen zustande.

Datensicherung sei im BSI-Grundschutz geregelt. Die Behörden seien verantwortlich. Das ITDZ sorge ausreichend vor.

Maßnahmen gegen Phishing und Spam seien im Haushalt angemeldet. Entsprechende Mails müssten von Mitarbeitern datenschutzkonform überprüfbar sein. Schulungen müssten Personalvertretungsrechten entsprechen.

Das ITDZ habe ein Tool bereitgestellt, welches das Informationssicherheitsmanagement unterstütze. Nach der Hauptpersonalratsbeteiligung könne das ITDZ das Tool freigeben.

Anfang Mai sei die Begründung zur Informationssicherheitsverordnung veröffentlicht worden. Bund und Länder tauschten sich eng aus, wie die Kommunikationswege und der Austausch zur Kommunikationssicherheit verbessert werden könne. An die Verfahren seien in der Verordnung klare Anforderungen wie Pentests und regelmäßige Sicherheitskonzeptaktualisierungen formuliert, die Mehraufwände bedeuteten.

IT-Projekte des ITDZ, die für das Land bereitgestellt werden sollten und im Haushalt ausgewiesen seien, seien neue und aktualisierte IKT-Basisdienste, eine aktualisierte Nutzerverwaltung und eine Public-Key-Infrastruktur für eine bessere Signierung.

Der Zähler erfasse nur Mails, die aus dem Landesnetz oder in das Landesnetz verschickt worden seien. Das Gesamtaufkommen sei insgesamt deutlich höher.

Von den mehreren Zehntausenden Meldungen hätten 3 508 Meldungen auf Elemente auf der IKT-Architekturliste zugetroffen. Produkte außerhalb der Liste müssten von den Verantwortlichen auf Basis der Warnmeldungen des BSI kontrolliert werden.

Der Informationssicherheitsbericht werde jährlich seit 2011 erstellt und sei zuletzt für 2021 veröffentlicht worden. Informationen zur Ausstattung der Bezirke, die über den Informationssicherheitsbericht hinausgehe, oblägen der Verantwortung der Behördenleitung.

Lothar Sattler (SenInnDS; Leitung IKT-Steuerung, Digitalisierung der Verwaltung und Bürgerdienste) hebt hervor, dass die Anforderungen an IKT-Sicherheit stiegen, Beschäftigte altersbedingt ausschieden und Fachkräfte zunehmend schwieriger anzuwerben seien. Die Sicherheit der aktuellen dezentralen, heterogenen Infrastruktur sei auf Dauer nicht gegeben. Kräfte müssten aus diesen Gründen schon jetzt zentral gebündelt werden.

IKT-Sicherheit langfristig im Haushalt zu verankern sei deutlich wichtiger, als mit Einzelmaßnahmen unter Beschäftigten und in der Bevölkerung Bewusstsein zu schaffen.

Roman-Francesco Rogat (FDP) erklärt, er habe keine Vertraulichkeiten verletzt, da alle von ihm zuvor angesprochenen Punkte im öffentlichen Teil des Berichts enthalten seien.

Inwiefern könne eine zentrale Stelle durchgreifen, sodass Ausreißer vermieden würden? Wie könne Ressourcenmangel zentral geregelt werden?

Die Einführung des Informationssicherheitsmanagementtools sei für 2022 geplant gewesen. Wie lange dauere eine Prüfung vor Einführung? Wann werde es eingeführt?

Staatssekretär Dr. Ralf Kleindiek (SenInnDS) erläutert, im Anwendungsbereich des EGovG seien Durchgriffsmöglichkeiten und zentrale Steuerungshoheit möglich. Von diesem Recht solle Gebrauch gemacht werden. Dies beziehe sich auch auf den Bereich der verfahrensunabhängigen IKT.

Klaus-Peter Waniek (SenInnDS; Landes-InfSiBe) fügt hinzu, beim Informationssicherheitsmanagementtool stehe das Beteiligungsverfahren beim Hauptpersonalrat aus. Die Hauptschwerbehindertenvertretung, die Frauenvertreterinnen und BlnBDI müssten Stellungnahmen abgeben. Anschließend werde der Hauptpersonalrat es innerhalb einer Frist bearbeiten und Nachfragen stellen könne. Es sei nächste Woche für die vorgelagerten Beteiligungsvorgänge bereit. Je nach Anzahl der Fragen des Hauptpersonalrat werde es voraussichtlich Ende Juni oder im Juli abgeschlossen sein.

Vorsitzender Christian Wolf erklärt die Besprechung für abgeschlossen.

Punkt 3 der Tagesordnung

Antrag der Fraktion der CDU	0013
Drucksache 19/0245	DiDat
IT-Sicherheit in allen Behörden und Landesbetrieben sicherstellen!	

Der **Ausschuss** beschließt ohne Aussprache, dem Plenum die Ablehnung des Antrags Drucksache 19/0245 zu empfehlen.

Punkt 4 der Tagesordnung

Verschiedenes

Volker Brozio (BlnBDI; kommissarischer Leiter) berichtet, der Jahresbericht 2021 sei gestern an Vizepräsidentin Cornelia Seibeld übergeben worden sei. Heute werde er an die Regierende Bürgermeisterin übergeben und in der nächsten Woche veröffentlicht. Die Mitglieder des Ausschusses erhielten ein Exemplar, sodass der Inhalt behandelt werden könne.

Der Jahresbericht sei von Corona geprägt. In diesem Zusammenhang sei eine höhere Anzahl an Beschwerden, unter anderem zu Terminvergaben und Testungen, eingegangen. Ein weiterer Schwerpunkt sei das Thema Schule.

Weiteres siehe Beschlussprotokoll.