

Inhaltsprotokoll

Öffentliche Sitzung

Ausschuss für Digitalisierung und Datenschutz

– zu TOP 5 teilweise nichtöffentlich –

23. Sitzung
26. Juni 2023

Beginn: 14.03 Uhr
Schluss: 16.44 Uhr
Vorsitz: Johannes Kraft (CDU), stellv. Vorsitzender

Vor Eintritt in die Tagesordnung

Siehe Beschlussprotokoll.

Punkt 1 der Tagesordnung

Wahl der/des Vorsitzenden

Marc Vallendar (AfD) beantragt die Durchführung einer geheimen Wahl zu Tagesordnungspunkt 1.

Der **Ausschuss** führt zu Tagesordnungspunkt 1 eine geheime Wahl durch.

Vorsitzender Johannes Kraft gibt bekannt, dass der von der AfD-Fraktion für den Vorsitz vorgeschlagene Marc Vallendar (AfD) vom Ausschuss mehrheitlich abgelehnt worden sei.

Der **Ausschuss** vertagt den Tagesordnungspunkt.

Punkt 2 der Tagesordnung

Aktuelle Viertelstunde

1. Die IT-Dienstleistungszentren der Länder haben ein Gutachten zur Datenschutzkonformität von Microsoft Office 365 erstellen lassen. Was war das Ergebnis

dieses Gutachtens und welche Folgen zieht der Senat und das ITDZ aus diesen Ergebnissen? Unterscheidet sich das Ergebnis des Gutachtens der IT-Dienstleister von dem der Datenschutzkonferenz der Länder?

Staatssekretärin Martina Klement (Skzl) antwortet auf die Frage von **Jan Lehmann** (SPD), dass nicht die Ländern gemeinsam bzw. Berlin das Gutachten in Auftrag gegeben hätten. Es liege Berlin nicht vor; die beauftragte Rechtsanwaltskanzlei habe offenbar eine Verschwiegenheitserklärung unterschrieben. Sie gehe davon aus, dass das Gutachten zu dem Schluss komme, dass Office 365 nicht datenschutzkonform betrieben werden könne, und der Senat betreibe es auch nicht.

2. Was sind die Ergebnisse des Digitalministertreffens D16 vom 23.6.?

Staatssekretärin Martina Klement (Skzl) antwortet auf die Frage von **Christopher Förster** (CDU), dass die Digitalminister der Länder zusammen mit Bundesminister Wissing getagt hätten. Sie hätten über die IKT-Fachkräftesicherung gesprochen, die für Bund und Länder schwierig sei. In Berlin sei die Situation zusätzlich schwierig, da das Land auch immer mit dem Bund konkurriere, der besser zahle als das Land. Die Länderkollegen seien sich einig, dass sie sich mehr zu Best Practices austauschen und gemeinsame Kooperationen, eventuell mit Universitäten, anstoßen müssten. In Berlin schlage sie eine stärkere Kooperation mit der Verwaltungsakademie vor. Auch die Fachkräftegewinnung aus dem Ausland sei ein Thema.

Beim Thema KI seien selbst Experten von der schnellen Entwicklung überrascht, auch bzgl. ChatGPT. Eine übergeordnete Strategie fehle allen. Der Bundesminister habe darauf hingewiesen, dass die Kennzeichnung von KI ein großes Thema sei. Sie seien sich zudem einig, dass Politik schnell praxistaugliche und innovationsfreundliche Regelungen unter Einbeziehung der Datenschutzbehörden schaffen müsse.

Beim Digital-Services-Act seien sich die Länder einig, dass der Bund klarstellen müsse, wie er weiter vorgehen wolle und in welchem Verhältnis das NetzDG dazu stehe.

Sie hätten weiterhin die Weiterentwicklung der D16, das bisher ein informelles Treffen der Digitalminister sei, besprochen und wollten es 2024 zu einer Digitalministerkonferenz weiterentwickeln. Berlin und Brandenburg hätten den Vorsitz der D16 ab Anfang Juli für die nächsten 18 Monate übernommen, sodass sie auch den ersten Vorsitz der Digitalministerkonferenz übernehmen würden.

Stefan Ziller (GRÜNE) wirft ein, aus Fachverwaltungen hätten ihn Meldungen erreicht, dass in Chefgesprächen niedrige Priorisierung und Kürzungen bei Digitalisierungsprojekten anstünden. Wie könne der Senat Rückschritte bei Digitalisierungsprojekten verhindern?

Staatssekretärin Martina Klement (Skzl) verweist darauf, dass die Haushaltsverhandlungen im Gange seien, sodass sie über den genauen Stand der Verhandlungen der Chefgespräche keine Informationen habe, da sie nur bei ihrem eigenen Einzelplan bzw. dem der Senatskanzlei eingebunden sei. Wenn dem so sei, werde das spätestens Thema im parlamentarischen Verfahren sein.

Meike Kamp (BlnBDI) betont, für BlnBDI sei beim Thema Office 365 die Beschlussfassung in der DSK maßgeblich. BlnBDI habe beim ITDZ angefragt, ob sie das Gutachten einsehen könnten, was sie mit Verweis auf die Vertraulichkeit abgelehnt hätten. Zu dem Thema lägen im Übrigen bereits Anfragen nach IFG vor, die FragDenStaat veröffentlicht habe.

Die DSK habe vor Kurzem einen Beschluss zum politischen Targeting geschlossen. Ein Verordnungsentwurf dazu befinde sich auf europäischer Ebene in Verhandlungen im Trilogverfahren. Bei Interesse leite sie die Position der DSK gerne weiter.

Tobias Schulze (LINKE) erkundigt sich, ob die Havarie in den neuen Räumen der BlnBDI Auswirkungen auf die Arbeitsfähigkeit habe und ob BlnBDI politische Unterstützung brauche, um damit umzugehen.

Meike Kamp (BlnBDI) fasst zusammen, in der Nacht von Donnerstag auf Freitag sei in einem Büro die Decke heruntergebrochen. Am Freitag hätten verschiedene Personen der BIM, Architekten und ein Statiker die Situation begutachtet. Der Statiker habe gesagt, dass Mitarbeiterinnen und Mitarbeiter nicht in Büros arbeiten sollten, in denen die Decke wie in dem betroffenen Büro abgehängt sei, was sämtliche Räume der Dienststelle mit Ausnahme von fünf Büros betreffe. Für heute habe die Behörde für alle Mitarbeiterinnen und Mitarbeiter, bei denen das möglich sei, Arbeit im Homeoffice angeordnet. Die Dienstfähigkeit sei momentan teilweise eingeschränkt. Derzeit finde eine Begehung durch einen Gutachter, einen Statiker und den Architekten statt. Die Wahrscheinlichkeit sei recht hoch, dass sie die Räumlichkeiten weiterhin nicht nutzen könnten.

Tobias Schulze (LINKE) fragt, ob sie Ausweichräume brauche oder ob es Gespräche mit der BIM gebe.

Meike Kamp (BlnBDI) antwortet, für die Beantwortung der Frage müsse sie das abschließende Ergebnis der Begehung abwarten. Der Bürger- und Polizeibeauftragte sitze im gleichen Gebäude und habe noch Kapazitäten. Da BlnBDI ihm in der Vergangenheit geholfen habe, sei denkbar, dass er die Behörde unterstützen werde. Sie werde Bedarf mitteilen.

Vorsitzender Johannes Kraft bittet BlnBDI darum, den Ausschuss via Ausschussbüro über die Situation zu informieren, sobald ein Sachstand gegeben sei, damit er agieren könne.

Der **Ausschuss** schließt die Aktuelle Viertelstunde ab.

Punkt 3 der Tagesordnung

Besprechung gemäß § 21 Abs. 3 GO Abghs
**3 Punkte aus dem Bericht der
Landesdatenschutzbeauftragten 2022 – Teil 1**
(auf Antrag der Fraktion der CDU und der Fraktion der
SPD)

[0045](#)
DiDat

Jan Lehmann (SPD) führt ein, der Ausschuss habe sich mit BlnBDI darauf verständigt, dass sie in mehreren Teilen einzelne Teile des Datenschutzberichtes vortrage. Sie habe sich für den

Stand der Digitalisierungsprojekte mit OZG-Verbindung, das Transparenzgesetz und den Rundfunkstaatsvertrag entschieden. Bei letzterem sei er gespannt, in welche Bereiche Datenschutzbeauftragte eingreifen dürften.

Vorsitzender Johannes Kraft weist darauf hin, dass BlnBDI die drei Punkte verabredungsgemäß am 21. Juni 2023 per E-Mail übermittelt habe.

Stand der Digitalisierungsprojekte mit OZG-Verbindung

Meike Kamp (BlnBDI) führt aus, sie habe in der Vergangenheit über Beratungsvorgänge der Behörde bei Rahmendatenschutzkonzeptionierungen und Datenschutzfolgeabschätzungen im Zusammenhang mit der E-Akte berichtet und diese Beratungen auch im Jahresbericht dargestellt. Die Zuweisung der datenschutzrechtlichen Verantwortlichkeit im Zusammenhang mit der Verwaltungsdigitalisierung sei immer wieder relevant.

Im Jahresbericht hätten sie einen Vorgang zum Onlineantrag für Ukraineflüchtlinge dargestellt. Die gemeinsame Verantwortlichkeit zwischen IKT-Steuerung und Fachamt entspreche nicht der datenschutzrechtlichen Bewertung, denn die Fachämter seien datenschutzrechtliche Verantwortliche, denen in Gesetzen bestimmte Aufgaben zugewiesen seien. Zur Erfüllung dieser Aufgaben bearbeiteten sie personenbezogene Daten. Im Übrigen müsse die Einbindung der IKT-Steuerung in diesem Zusammenhang als Auftragsverarbeitungsvertrag ausgestaltet werden. Dazu sei ihre Behörde noch im Gespräch. Da es bei der Verwaltungsreform insgesamt um Zuständigkeiten gehe, weise sie darauf hin, dass auch die datenschutzrechtliche Verantwortungszuweisung ein relevanter Punkt sei, um Dinge gesetzlich einmal zu regeln und keine Probleme mehr zu haben.

Die Verwaltung möge ihre Behörde frühzeitig bei der Überarbeitung des OZG in Berlin und EGovG Bln einbinden.

Ihre Behörde begrüße, dass das Bundeskabinett in der Sitzung am 24. Mai 2023 den Entwurf eines Gesetzes zur Änderung des OZG beschlossen habe. Im Rahmen der Kontaktgruppe „OZG 2.0“ der DSK sei ihre Behörde federführend für alle Bundesländer im Gespräch mit dem BMI und habe intensiv bei der Ausarbeitung des Gesetzentwurfes mitberaten. Viele ihrer Änderungs- und Ergänzungsvorschläge fänden sich nun im Gesetzentwurf.

In der Neuregelung des EGovG Bln fehle noch eine explizite Regelung, dass das Datenschutzcockpit als Transparenzmaßnahme abbilden müsse, wenn eine Verwaltung notwendige Nachweise aus einem Register abrufe, die die Steuerliche Identifikationsnummer verwendeten. Der Innenausschuss des Bundesrats habe den Gesetzentwurf letzte Woche beraten, und ihre Behörde habe frühzeitig versucht, die zuständigen Ressorts zu beteiligen. Sie hätten einen Antragsentwurf geschrieben, den Berlin letztlich nicht in den Innenausschuss eingebracht habe. SenInnSport habe die Position vertreten, dass es für die Länder keine Relevanz habe und für die Betroffenen schon Transparenz nach den üblichen Auskunftsansprüchen der DSGVO gegeben sei. Das sei richtig, aber bei der Registermodernisierung habe es viele Diskussionen zur Verfassungsmäßigkeit bei der Verwendung der Steuerlichen Identifikationsnummer gegeben; ein großer Punkt, um Verhältnismäßigkeit zu schaffen, sei gewesen, zusätzliche, proaktive Transparenz über Datenschutzcockpits zu schaffen. Der Koalitionsvertrag und die Richtlinien der Regierungspolitik sähen vor, das Datenschutzcock-

pit auszubauen. Vor dem Hintergrund wäre es wünschenswert gewesen, diese Klarstellung vorzunehmen.

Stefan Ziller (GRÜNE) fragt, welche Erwartungen BlnBDI konkret an das Land Berlin habe.

Der Hauptausschuss habe in der letzten Sitzung darüber geredet, dass SenFin mit diversen Beratungsaufträgen ein „Rundum-sorglos-Paket“ für den eigenen Bereich schaffe, sich aber niemand Gedanken mache, wie es mit anderen Fachverwaltungen aussehe. Für Beratungen, wie sie SenFin derzeit mache, würden andere Verwaltungen keine Mitzeichnung erhalten. Würden die DSGVO und Datenschutzleitlinien in den Fachverwaltungen angenommen? Bauten sie Kompetenzen auf, oder schaffe SenFin nur für sich selbst eine Umgehung? Der Senat müsse den Kompetenzaufbau in den Verwaltungen sicherstellen.

Tobias Schulze (LINKE) erkundigt sich, wie BlnBDI die Zukunft der OZG-Umsetzung einschätze. Das bisherige OZG sei gescheitert, ein reformiertes OZG müsse sehr viel weiter gehen. Komme es bei dem Prozess voraussichtlich zu größeren Fragen im Datenschutz? Sei der Berliner OZG-Umsetzungskatalog auch von datenschutzrechtlichen Problemen betroffen?

Meike Kamp (BlnBDI) gibt zu bedenken, es gebe eine große Dynamik in dem Prozess; im Innenausschuss des Bundesrats hätten über 50 Änderungsanträge zu dem Gesetzentwurf vorgelegen. Im Rahmen des Entwurfsprozesses mit dem BMI sei viel aus der Kontaktgruppe „OZG 2.0“ eingeflossen. Die Verantwortlichkeitszuweisung sei wesentlich. Sie wisse nicht, ob es von Länderseite noch Änderungsbedarf gehe, aber im parlamentarischen Verfahren könne sich noch eine Menge ändern.

BlnBDI hätte begrüßt, wenn Berlin Regelungen zur Klarstellung des Datenschutzcockpits eingebracht hätte. Obwohl es im Koalitionsvertrag stehe, habe SenInnSport keinen Bedarf gesehen. BlnBDI habe ausreichend unterstützt, damit Berlin den Antrag hätte stellen können. Das Datenschutzcockpit sei aber sehr relevant, da wie erwähnt Bedenken zur Verhältnismäßigkeit der Nutzung der Steuerliche Identifikationsnummer beständen und Verfahren liefen. Gesteigerte Transparenz könne verfassungsrechtliche Bedenken möglicherweise ausgleichen.

Die Nachfrage der Fachbehörden nach datenschutzrechtlicher Beratung durch ihre Behörde sei enorm. Es sei erforderlich, dass Datenschutzkompetenz unabhängig von den behördlichen Datenschutzbeauftragten laufe, die eher kontrollierende Personen seien. Bei der Implementierung müssten Behörden Datenschutzkompetenz aufbauen, denn es sei problematisch, Datenschutzfolgeabschätzungen in Auftrag zu geben, ohne die Kompetenz, Anforderungen zu formulieren oder das Ergebnis evaluieren zu können, zu haben. Die Ergebnisse externer Stellen seien zudem stark überarbeitungsbedürftig.

Stefan Ziller (GRÜNE) fragt, wie SenInnSport die Datenschutzkompetenzfrage bewerte. Werde jede Senatsverwaltung alleine vorgehen?

Manfred Weyrich (SenInnSport) teilt mit, er könne dazu keine Aussagen machen.

Vorsitzender Johannes Kraft hält fest, dass die Senatsverwaltung die Antwort auf die Frage schriftlich nachreiche.

Stefan Ziller (GRÜNE) bittet für die Zukunft darum, dass für Tagesordnungspunkte auf der Tagesordnung jemand von der zuständigen Senatsverwaltung vor Ort und auskunftsfähig sei.

Vorsitzender Johannes Kraft entgegnet, dass Staatssekretärin Klement und Herr Weyrich anwesend seien. Sie könnten nicht auf alle Punkte im Detail vorbereitet sein.

Staatssekretärin Martina Klement (Skzl) bestätigt, bei der Neufassung des OZG sei gebe es noch viel zu klären. Das betreffe nicht nur Datenschutzfragen, sondern noch größere Fragen, auch ob es noch alles finanziert werde.

Rundfunkstaatsvertrag

Meike Kamp (BlnBDI) führt aus, ihre Behörde habe auch die Novellierung des RBB-Staatsvertrag zur Errichtung einer gemeinsamen Rundfunkanstalt der Länder Berlin und Brandenburg im Jahresbericht behandelt. Momentan sei BlnBDI für die Aufsicht des wirtschaftlich-administrativen Bereichs zuständig und die RBB-Datenschutzbeauftragte für den journalistischen Bereich. Die DSGVO sehe die Aufteilung auch so vor, und Mitgliedsstaaten dürften nur Regelungen vornehmen, wo die DSGVO eine Öffnungsklausel enthalte. Die gebe es im Bereich der Meinungsfreiheit und der Medien, beschränke sich aber auf Ausnahmen im journalistischen Bereich. Dass die gesamte Aufsicht auf die RBB-Datenschutzbeauftragte übergehen solle, sei aus Sicht ihrer Behörde nicht mit der DSGVO zu vereinbaren. Die bisherige Aufteilung habe sich zudem bewährt, und Brandenburg, Bremen und Hessen praktizierten dies ebenso.

Die Auskunftsrechte für datenschutzrechtliche Fragen im wirtschaftlich-administrativen Bereich regle ein Rundfunkänderungsstaatsvertrag. Dort gebe es Vorgaben, die nicht mit der DSGVO in Einklang stünden. Bei der Durchsetzung dieser Rechte wäre die Datenschutzbeauftragte der Rundfunkanstalt zuständig, und die Beitragszahlenden fänden keine unabhängige Datenschutzaufsicht mehr vor. Dies betreffe viele Menschen, die von der Beitragszahlung befreit seien, und es komme immer wieder zu Schwierigkeiten, ihre Rechte durchzusetzen.

Gollaleh Ahmadi (GRÜNE) erklärt, aufgrund der Wahlwiederholung und Verhandlungen zwischen Senatskanzlei Berlin und Staatskanzlei Brandenburg habe der Ausschuss die Novellierung nicht beraten können. Dass die Datenschutzvereinbarung geändert werden solle, habe sie zum ersten Mal im Jahresbericht gelesen. Sie werde das Thema für die weitere Beratung in den EnBuMe-Ausschuss und in Runden medienpolitischer Sprecherinnen und Sprecher mitnehmen. Journalistischer Datenschutz solle aber beim RBB bleiben.

Tobias Schulze (LINKE) fragt, ob die Stellungnahme dazu einsehbar sei. Zudem seien Datenschutzfragen von Regierungsinteresse; hätten die beteiligten Landesregierungen dazu reagiert?

Jan Lehmann (SPD) erkundigt sich vor dem Hintergrund, dass Abgeordnete Ahmadi das Thema mitnehmen wolle, ob es Regelungen in anderen Bundesländern oder beim ZDF gebe, die als Vorbild dienen könnten.

Gollaleh Ahmadi (GRÜNE) stellt klar, sie nehme mit, dass in dem Fall keine Novellierung erfolge.

Johannes Kraft (CDU) begrüßt den Weg, die Trennung beizubehalten. Er habe Abgeordneten Lehmann so verstanden, dass die Koalition das als eine gute Variante empfinde.

Meike Kamp (BlnBDI) äußert, sie müsse nachreichen, ob die Stellungnahme einsehbar sei. Ihr gehe es darum, dass die Aufteilung bestehen bleibe.

Gollaleh Ahmadi (GRÜNE) bittet darum, der Senat möge dem Ausschuss nähere Informationen zur RBB-Novellierung mitgeben.

Staatssekretärin Martina Klement (Skzl) bekennt, dass sie bei der Novellierung die Aufgaben und Befugnisse für den Datenschutz neu regeln wollten. Was vorbesprochen sei, könne sie nachreichen.

Meike Kamp (BlnBDI) kündigt an, ihre Behörde schreibe im Nachgang zur Sitzung einen Brief an alle Fraktionen und füge die Stellungnahme an.

Berliner Transparenzgesetz

Es sei an der Zeit, ein modernes Transparenzgesetz zu schaffen, und sie begrüße die Vorankündigung im Koalitionsvertrag. Wenn es dabei bleibe, dass Bereichsausnahmen nur für den Verfassungsschutz vorgesehen seien, stelle dies eine Verbesserung gegenüber früheren Entwürfen dar. Berlin könne in Sachen Transparenz wieder einen Spitzenplatz einnehmen – das IFG von 1999 sei das zweite Gesetz seiner Art gewesen. Ihre Behörde werde auch zum Gesetzentwurf, der von den Fraktionen Bündnis 90/Die Grünen und Linke vorliege, Stellung nehmen.

Stefan Ziller (GRÜNE) erinnert, der Gesetzentwurf der Fraktionen Bündnis 90/Die Grünen und Linken liege vor und möge nach dem Sommer beraten werden, um Berlin wieder an die Spitze zu bringen. Plane der Senat alternativ ein Senatsgesetz mit Mitzeichnung, und gebe es dazu einen Zeitplan?

Tobias Schulze (LINKE) bestätigt, der Gesetzentwurf des letzten Senats enthalte vieles von dem, was die neue Koalition vorgeschlagen habe. Im Übrigen habe der Senat der Volksinitiative versprochen, ein Gesetz auf den Weg zu bringen; sie hätten daraufhin davon abgesehen, das Volksbegehren weiterzuverfolgen, sodass Berliner Politik das Thema voranbringen müsse.

Jan Lehmann (SPD) verweist auf eine neue Initiative der Koalition. Sie planten, sie im Sommer zu besprechen und möglicherweise im Herbst um Mitarbeit des Senats bitten. Die alte Koalition habe vor der Wahlwiederholung keine verfassungsändernden Gesetze auf den Weg bringen wollen. Er gebe Abgeordneten Schulze recht, dass sie das Thema vor dem Hintergrund der Volksinitiative behandeln müssten, aber es habe keine Eile, da es erst mit der E-Akte und dem Transparenzportal relevant werde. Bis dahin sei es gut umsetzbar.

Marc Vallendar (AfD) wirft ein, die E-Akte sei nicht Bedingung für das Transparenzgesetz. In Hamburg habe es das Transparenzgesetz vor der E-Akte gegeben. Wenn ein Volksentscheid sich Mühe mache, die erforderlichen Unterschriften zu sammeln, und das Parlament und vor allem der vergangene Senat suggeriere, dass sie es nicht zur Abstimmung bringen müsste, gebe es Eilbedürftigkeit. Der vergangene Senat habe zudem in seinem Entwurf die Schulverwaltung, die Steuerverwaltung und die landeseigenen Unternehmen aussparen wollen, sodass er weitestgehend sogar hinter dem IFG zurückbleibe. Plane der neue Senat ähnliche Aussparungen? Der Ausschuss benötige im Übrigen eine Anhörung, um festzustellen, ob das Transparenzgesetz eine Verbesserung zu den bisherigen gesetzlichen Regelungen darstelle.

Stefan Ziller (GRÜNE) widerspricht der Aussage, das Transparenzgesetz sei erst mit der E-Akte sinnvoll. Ein Transparenzgesetz regle eine Reihe von Dingen. Auf der Open-Data-Seite Berlins seien Senatsbeschlüsse zum Beispiel als Kategorie vorgemerkt, aber es gebe keine, weil es heute nicht transparent sei. Das gleiche gelte für Beschlüsse vom Rat der Bürgermeister, Bezirksämter. Teilweise veröffentlichten Stellen Beschlüsse, aber ein Transparenzgesetz schaffe dafür einen geordneten Rahmen. Der Senat möge das Verfahren selbst angehen und nicht darauf warten, dass aus der Koalition vielleicht im Sommer oder Herbst etwas zum Senat gelange.

Staatssekretärin Martina Klement (Skzl) stellt klar, dafür sei SenInnSport zuständig. Sie kenne keinen Zeitplan, es solle aber im Sommer vorangehen. Der neue Senat werde das von den Fraktionen Bündnis 90/Die Grünen und Linken vorgelegte Transparenzgesetz nicht einfach übernehmen. Die Notwendigkeit sei aber unabhängig von der E-Akte gegeben.

Manfred Weyrich (SenInnSport) erläutert, ein konkreter Zeitplan für den Gesetzentwurf liege nicht vor, aber die Festlegung in den Richtlinien der Regierungspolitik beschreibe, dass der Senat schnellstmöglich einen Entwurf vorlege. Der Senat werde zu Beginn der Ausschussberatung zum Entwurf der Fraktionen Bündnis 90/Die Grünen und Linke bzw. auch zu weiteren Fraktionsentwürfen Stellung nehmen. Weiterhin orientiere sich der Senat eng an den Richtlinien der Regierungspolitik.

Meike Kamp (BlnBDI) merkt an, es schaffe Hoffnung, wenn die Orientierung eng an den Richtlinien der Regierungspolitik erfolge, sodass es nach Hamburger Vorbild und nur mit einer Bereichsausnahme für den Verfassungsschutz erfolge. Auch sie betrachte es unabhängig von der E-Akte. Es gebe bereits viele Dokumente in der Berliner Verwaltung, die digitalisiert seien und bereits jetzt einem Transparenzportal zur Verfügung gestellt werden könnten.

Stefan Ziller (GRÜNE) bittet darum, bei zukünftigen Einladungen, die benannten Themen in den Titel zu schreiben. Der Titel des aktuellen Tagesordnungspunktes sei sehr unkonkret.

Vorsitzender Johannes Kraft erwidert, das hänge auch damit zusammen, wie sich die Sprecherrunde abspreche. Beim letzten Mal habe sie vereinbart, auf die Zuarbeit von Frau Kamp zu warten. Der Ausschuss müsse aber auch BlnBDI Zeit für die Zuarbeit geben.

Der **Ausschuss** schließt die Besprechung ab.

Punkt 4 der Tagesordnung

Besprechung gemäß § 21 Abs. 3 GO Abghs
Digitale Verwaltung: Berliner Open-Source-Strategie
(auf Antrag der Fraktion Bündnis 90/Die Grünen und der Fraktion Die Linke)

[0038](#)
DiDat

Tobias Schulze (LINKE) führt ein, die letzte Koalition habe sich auf ein weitgehendes Open-Source-Konzept für die Verwaltung geeinigt, und das Abgeordnetenhaus habe einen Antrag beschlossen, damit sich der Grundsatz „public money, public code“ durch alle IT-Beschaffungen ziehe, sodass es einen Open-Source-Vorbehalt für alle Ausschreibungen und Vergaben gebe. Auch der BerlinPC, ein Arbeitsplatzrechner mit Open-Source-Software, sei Teil dessen gewesen, und Open-Source-Spezialistinnen und -Spezialisten sollten in allen Verwaltungen in IT-Stellen integriert sein. Zudem müsse Berlin innovative Instrumente offener Beschaffung nutzen und Innovationspartnerschaften mit Open Source verbinden. Es gehöre dazu, einen Zweck anstelle fertiger Software auszuschreiben. In den Richtlinien der Regierungspolitik behandle die neue Koalition das Thema allerdings weniger umfassend, sodass sich der Ausschuss verständigen möge, wie es mit der Open-Source-Strategie für Berlin weitergehe.

Der WissForsch-Ausschuss habe besprochen, dass das Helmholtz-Zentrum Berlin nach einem IT-Angriff auf Windows-Rechner arbeitsunfähig sei. Auch auf Bundesebene laufe eine Debatte zu digitaler Souveränität, was Schnittmengen mit Open Source habe. Der Ausschuss müsse deshalb darüber sprechen, welche Möglichkeiten der Senat sehe, um digital souveräner zu werden und von unsicheren Lösungen wegzukommen, die Berlin bisher einsetze, und welche Rolle Open Source bei einer zukunftsfähigen Verwaltungsdigitalisierung spiele.

Staatssekretärin Martina Klement (Skzl) führt aus, in der Open-Source-Strategie des letzten Senats stehe viel Gutes, auch wenn der neue Senat nicht alles teile. Berlin brauche Open Source, um digital souverän zu werden, aber sie sehe keinen Einsatz in allen Bereichen. Ob Berlin eine Priorität für Open Source wolle, müsse Berlin im Rahmen des Digitalgesetzes festlegen. Sie gehe davon aus, dass Open Source eher für Fachverfahren relevant sein werde. Zudem werde das ITDZ im laufenden Jahr ein Open-Source-Kompetenzzentrum eröffnen.

Lothar Sattler (SenInnSport) stellt klar, die Digitalstrategie sein ein Prozess, den sie aus zwei Blickwinkeln betrachteten. Sie wollten praktische Ergebnisse liefern. Open Source werde nun nicht anders betrachtet als zuvor. Im Kern erfahre Open Source in der IKT-Architekturliste Version 1.9 Vorrang.

Um das fortentwickeln zu können, müsse die Verwaltung ertüchtig sein, mit Open Source umgehen zu können. Zum Ende des Jahres eröffne das schon länger geplante Open-Source-Kompetenzzentrum, das die Verwaltung beraten und ertüchtigen werde. Es werde zudem Partnerschaften generieren – wie von Abgeordneten Schulze angesprochen – und das Thema für die Verwaltung handhabbar machen.

Die Senatsverwaltung habe sich an den Drucksachen 19/0480 und 19/0535 zur Open-Source-Strategie für Berlin orientiert und die drei Handlungsfelder aus den Beschlüssen des

Abgeordnetenhauses abgeleitet. Für die Fachverfahren würden sie das Referenzmodell generieren, und sie würden an dem Grundsatz „public money, public code“ festhalten. Auf Bundesebene, im IT-Planungsrat, bewege sich das Thema, und es sei sinnvoll, das Geschehen als Land zu beobachten.

In der Phase, in der Berlin den BerlinPC einführe, sei es aber nicht klug, das Thema Open Source als weitere Entwicklungsphase einzubringen, da dies den Prozess überfrachte. Dass sie es parallel weiterentwickeln müssten, sei aber selbstverständlich.

Staatssekretärin Martina Klement (Skzl) fügt hinzu, es müsse nicht grundsätzlich „public money, public code“ gelten.

Meike Kamp (BlnBDI) unterstreicht, ihre Behörde stehe einer Berliner Open-Source-Strategie weiterhin grundlegend positiv gegenüber. Das Wording im Koalitionsvertrag habe sich von einem Default zu „einen besonderen Raum einräumen“ geändert, sodass es gut zu hören sei, dass grundsätzliche Entscheidungen weiter bestehen blieben. Open Source schaffe offene Standards, erleichtere die Datenportabilität, erhöhe die Interoperabilität und vermeide Lock-in-Effekte oder den Abfluss und die Verarbeitung von Telemetriedaten, über die der Ausschuss oft spreche. Um behördenübergreifend Interoperabilität zu schaffen, wäre die Festlegung einer Softwareumgebung aus Open-Source-Betriebssystemen und Open-Source-Anwenderprogrammen, zu denen zukünftige Entwicklungen und Beschaffungen kompatibel sein müssten, sinnvoll. Ein Open-Source-BerlinPC könne ein sinnvoller Schritt sein. Ob eine solche Strategie wirksam sei, hänge davon ab, wie einfach es sein werde, doch Entscheidungen zugunsten der Beschaffung proprietärer Software zu treffen.

Stefan Ziller (GRÜNE) sagt zu, mit einem deutlichen Schritt in die Richtung könnten sie auch leben. „Public money, public code“ habe er nie als Dogmatismus verstanden, aber er würde sich freuen, wenn sich der Senat dazu bekennen würde, den Weg wann immer möglich zu gehen.

Sei der Zeitplan von Fachverfahren vor dem Hintergrund der Open-Source-Umsetzungsstrategie mit den Haushaltsberatungen verbunden?

Die Idee des Open-Source-BerlinPC sei entstanden, als Dataport mit der dPhoenixSuite vorgelegt habe. Inzwischen gebe es auf Bundesebene Arbeiten für einen digital souveränen Arbeitsplatz, der mit dem BerlinPC und OneIT@Berlin kompatibel sei: Software, bestenfalls Open-Source-Software, die auf Windows, später vielleicht auch auf anderen Betriebssystemen, laufe, die Grundfunktionalität souverän darstelle und im bundesweiten Zusammenspiel entwickelt werde. – Integriere Berlin dies in absehbarer Zeit in den BerlinPC? In welchem Verhältnis stehe der Berliner Basisdienst Kollaboration mit Blick darauf, dass der digital souveräne Arbeitsplatz das auch anbiete; werde Berlin weiter den eigenen Weg gehen?

Der Bund biete als Plattform der öffentlichen Verwaltung Open CoDE. Was plane der Senat für die Berliner Verwaltung in diesem Zusammenhang?

Tobias Schulze (LINKE) weist darauf hin, dass der Beschluss des CDU-Parteitag vom November 2019 „Digitalcharta Innovationsplattform“ eine sehr saubere Herleitung enthalte,

warum offene Software wichtig und als Grundprinzip für E-Government und digitale Verwaltung ein gutes Prinzip sei. Schön ausgeführt sei darin auch Openness über alle Bereiche hinweg.

Er habe vor einer Weile eine schriftliche Anfrage zum Umfang von Open-Source-Software in der Verwaltung gestellt. Dabei sei aufgefallen, dass Open-Source-Software im Serverbereich wesentlich verbreitet sei als im Bereich der Arbeitsplätze. Wie sei die Entwicklung gelaufen?

Sei es denkbar, den BerlinPC parallel mit Windows laufen zu lassen und Beschäftigten eine Wahl zu bieten?

Habe der Senat mit dem Hauptpersonalrat darüber gesprochen? Der Ausschuss habe ihn eingeladen gehabt, und die Einstellung der Beschäftigten sei ein Hinderungsgrund. Es müsse einen dauerhaften Dialog mit Personalrätinnen und -räten geben.

Im Koalitionsvertrag und den Richtlinien der Regierungspolitik sei ein zweiter IT-Dienstleister beschrieben mit der Zielrichtung, Fachverfahren und externe Expertise einzubinden. Sei geplant, Open Source mit einzubinden und den IT-Dienstleister zu nutzen, um innovative Beschaffungsverfahren auszuprobieren?

Gebe es einen Zeitplan für das Digitalgesetz?

Staatssekretärin Martina Klement (Skzl) betont, sie könne nicht zusagen, dass Open Source immer eingesetzt werde, wenn möglich, aber sie könne zusagen, dass sie prüfen würden, wann es möglich sei, den Weg zu gehen.

Vor den Haushaltsverhandlungen sei es nicht sinnvoll, in Sachen Open Source an die Fachverwaltungen heranzugehen.

Es dauere noch eine Weile, bis sie zum BerlinPC sprechfähig seien.

Open CoDE als Plattform zur Dokumentation wäre wünschenswert, aber alles gleichzeitig würde nicht gehen.

Der CDU-Parteitagbeschluss komme aus Zeiten vor Corona und Krieg in der Ukraine, und die Prioritäten hätten sich verschoben.

Zur Frage zum Thema größerer Verbreitung von Open-Source-Software im Serverbereich als im Bereich der Arbeitsplätze bitte sie um nochmalige Einreichung einer Anfrage, da dies vor der Wiederholungswahl geschehen sei.

Mit dem Hauptpersonalrat habe sie ein Gespräch zusammen mit dem Regierenden Bürgermeister und eines separat geführt. Sie hätten viele Themen zur Verwaltungsmodernisierung und -reform und -digitalisierung angesprochen. Es müsse weitere Gespräche geben, da sie Mitarbeiterinnen und Mitarbeiter mitnehmen müssten, um erfolgreich zu sein.

Der Prüfauftrag zu einem zweiten IT-Dienstleister seit noch nicht durchgeführt worden. Es sei eine gute Idee, dass sich ein solcher zweiter IT-Dienstleister um innovative Beschaffungsmaßnahmen kümmern könne.

Ein Zeitplan zum Digitalgesetz komme so schnell wie möglich.

Lothar Sattler (SenInnSport) stellt in Aussicht, die einzelnen Aspekte rund um die Open-Source-Strategie bis 2024 auf eine Zeitachse zu bringen, um Transparenz zu schaffen, wann was machbar sei. Vieles hänge mit Ressourcen zusammen.

Der BerlinPC sei momentan nicht Open Source, aber als Zielprodukt sicherlich. Ziel sei eine sinnvolle Strategie bis Ende 2024.

Stefan Ziller (GRÜNE) fasst zusammen, der BerlinPC sei die Basis und werde mit Software aus der IKT-Architekturliste gespeist. Sein Verständnis des digital souveränen Arbeitsplatzes des Bundes sei, dass es ein Set von Software sei, das man auf den BerlinPC über die Architekturliste einbauen könne. Könne die Senatsverwaltung beim nächsten Architekturboard den Einsatz verfügbarer Programme in Berlin erlauben, sodass man dann immer noch schauen könne, wann sie zum Einsatz kämen? Andere Bundesländer teilten Software, die das Land Berlin nachnutzen könnte. Berlin solle bei den Bundesbemühungen für digitale Souveränität mitmachen. Berlin möge zudem Open-Source-Software, die es bereits verwende, über die gemeinsame Plattform mit den anderen Bundesländern teilen.

Lothar Sattler (SenInnSport) hebt hervor, dass die Festlegungen Berliner Architektur auf Beschlusslagen des IT-Planungsrats beruhten. Wo Nachnutzungen möglich seien, werde Berlin das machen. Nachnutzung erfolge aber tatsächlich noch nicht intensiv, und ob ein neues OZG dies verbessere, sei noch unklar. Finanzmittel und politische Haltung spielten eine Rolle. Berlin bringe sich ein und arbeite in nahezu allen Netzwerken und AGs mit, müsse aber auch nicht immer Vorreiter sein.

Berlin dürfe nicht nur auf Dataport schauen, sondern müsse auch eigene Möglichkeiten verfolgen.

Staatssekretärin Martina Klement (Skzl) fügt hinzu, sie teile die Meinung des Abgeordneten Ziller, dass Berlin vorangehen müsse und nicht nur hinterherlaufen solle.

Der **Ausschuss** schließt die Besprechung ab.

Punkt 5 der Tagesordnung

Besprechung gemäß § 21 Abs. 3 GO Abghs
**IKT-Sicherheit im Land Berlin – Sachstand und
wachsende Anforderungen**
(auf Antrag der Fraktion der CDU und der Fraktion der
SPD)

[0039](#)
DiDat

Christopher Förster (CDU) geht darauf ein, dass es seit dem Angriffskrieg auf die Ukraine mit Blick auf IT-Sicherheit im Land Berlin vermehrt Angriffe gebe. Der Ausschuss möge sich damit auseinandersetzen, wie sicher die Berliner Verwaltung aufgestellt sei.

Klaus-Peter Waniek (SenInnSport) zeigt die Präsentation „IKT-Sicherheit im Land Berlin – Sachstand und wachsende Anforderungen“. Die IT-Sicherheitslage spitze sich zu – siehe nächste Folie –, die Zahl der Schwachstellen steige sowohl bei Open-Source- als auch Closed-Source-Software. Die letzte Ausprägung des Kriegs in der Ukraine umfasse den Fake einer Website des BMI, die geschützt war, sodass es Probleme gegeben habe, sie abzuschalten.

IKT-Sicherheit im Land Berlin - Einleitung

- **Sicherheitslage** (allgemein)
 - „IT-Sicherheitslage spitzt sich zu“ (Quelle BSI: Lagebericht Deutschland 2022)
 - „Zahl der Schwachstellen steigt weiter“ (Quelle BSI: Lagebericht Deutschland 2022)
 - Ukraine Konflikt führt in verstärktem Maße zu Cyberaktivitäten
- **IKT-Sicherheit**
 - **ist in enger Vernetzung mit Cybersicherheit Teil der Digitalen Sicherheit**
 - beinhaltet übergreifend Inhalte von IT-Sicherheit und Informationssicherheit
 - wird i.a. über Schutzziele definiert, die i.w.S. auch auf den Datenschutz gerichtet sind.

IKT-Sicherheit im Land Berlin - Einleitung

- **Digitalisierung benötigt IKT-Sicherheit auf hohem Niveau für**
 - ein ordnungsgemäßes Handeln der Verwaltung und
 - Vertrauen der Bürger in Online-Dienstleistungen (Grundpfeiler der OZG-Umsetzung)
- **Umsetzung mittels kontinuierlichem Verbesserungsprozess *Planen - Umsetzen - Überprüfen - Handeln* für das Informationssicherheitsmanagementsystem (ISMS) nach den Standards des BSI**

IKT-Sicherheit sei die Sicherheit der Berliner Verwaltung und stehe in enger Vernetzung mit Cybersicherheit als Teil der digitalen Sicherheit. Digitale Sicherheit sei der Schutz und die Sicherheit der Besitztümer und Personen in einem digital geprägten Raum. Das EGovG Bln definiere, dass Berlin den Schutz nach vom BSI definierten Schutzziele aufbaue. Eingeschlossen seien auch Schutzziele des Datenschutzes.

Für ein ordnungsgemäßes Handeln müsse Berlin IKT-Sicherheit auf einem hohen Niveau umsetzen – siehe vorherige Folie. Auch für Vertrauen von Bürgern sei Sicherheit wichtig. Berlin könne das nach den Vorgaben des BSI durch planmäßiges Vorgehen und einen kontinuierlichen Verbesserungsprozess erreichen, so wie es im Informationssicherheitsmanagementsystem – ISMS – vorgesehen sei.

Für diesen komplexen Prozess – siehe nächste Folie – habe Berlin bereits einige Bausteine verfügbar. Das ITDZ sei seit Jahren BSI-zertifiziert und mache im nächsten Jahr eine Rezertifizierung für den Betrieb der IT im Land Berlin. Das Berliner CERT erfülle die Vorgaben des Standards, den der IT-Planungsrat beschlossen habe, vollständig.

IKT-Sicherheit im Land Berlin - Aktuelle Situation

- **BSI-Zertifizierung ITDZ** - Audit 2023 erfolgreich abgeschlossen / Rezertifizierung 2024 wird vorbereitet
- **Berlin-CERT** - alle Kennzahlen des Umsetzungsplanes zur InfoSic-LL des IT-PIR werden zu 100% erfüllt
- **Cyber-Defence-Center der Landesverwaltung (CDC-LV)** - Vertragsabschluss initiiert
- **DDoS-Schutz für Internet-Zugang der Landesverwaltung (BeLa)** - Schutz wirksam etabliert
- **Unterstützungswerkzeug für ISMS-Dokumentation** - im Prozess der Beteiligung Beschäftigtenvertretungen
- **IT-Sicherheits- / Notfallübung nach §23 EGovG Bln 2023** - seit 2020 (außer 2021) jährlich

Berlin betreibe zudem ein Cyber-Defence-Center der Landesverwaltung mit einem Security-Operations-Center als Leitstelle. Es gebe für Internetzugänge der Landesverwaltung auch einen Schutz gegen DDoS-Angriffe, der sehr wirksam sei und den sie regelmäßig testeten. Es gebe Unterstützungswerkzeug für ISMS-Dokumentation, gerade in der Beteiligung mit den Beschäftigtenvertretungen. Der Grundschutz des BSI ist komplex, das Werkzeug sei komplex, und die Bücher des BSI dazu seien komplex und nicht barrierefrei.

Seit 2020 müssten sie infolge eines Beschlusses des Abgeordnetenhaus Notfallübungen durchführen; dies stehe nun auch im EGovG Bln. 2021 habe sie coronabedingt ausfallen müssen. Die diesjährige Übung sei in der Vorbereitung.

Zu den Schwerpunkten Berliner IKT-Sicherheit – siehe nächste Folie – gehöre es, die digitale Sicherheit digitaler Prozesse und Infrastrukturen zu stärken und Angriffsresilienz zu erhöhen. Digitale Infrastrukturen in der Smart-City Berlin müssten jederzeit verfügbar, verständlich und beherrschbar sein. Technologische Souveränität sei ein weiterer Schwerpunkt. Zudem gehörten der Schutz der Demokratie, der online verstärkt werden müsse, und Privatheit dazu. Sie hätten einen großen Aufwand für die Absicherung der Wahl und der Wiederholungswahl gehabt.

IKT-Sicherheit im Land Berlin - Schwerpunkte

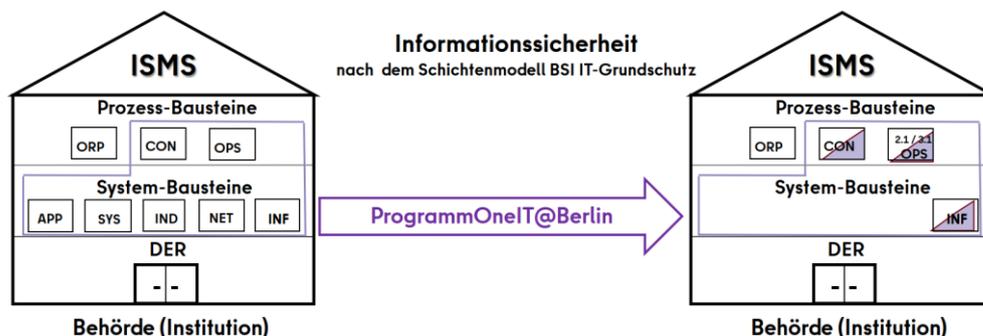
- **Digitale Prozesse und Infrastrukturen**
 - Digitale Sicherheit stärken - Angriffsresilienz erhöhen
- **Digitale Infrastrukturen in der Smart-City Berlin**
 - jederzeit verfügbar, verständlich und beherrschbar
- **Technologische Souveränität**
 - erhöhen und bewahren
- **Schutz der Demokratie**
 - online verstärken und Privatheit sichern

Seite 8 Berlin, 26.06.2023 DiDat TOP 05 - IKT-Sicherheit im Land Berlin -



IKT-Sicherheit im Land Berlin - Schwerpunkt Digitale Prozesse und Infrastrukturen

- **Programm OneIT@Berlin => Digitale Sicherheit stärken - Angriffsresilienz erhöhen**



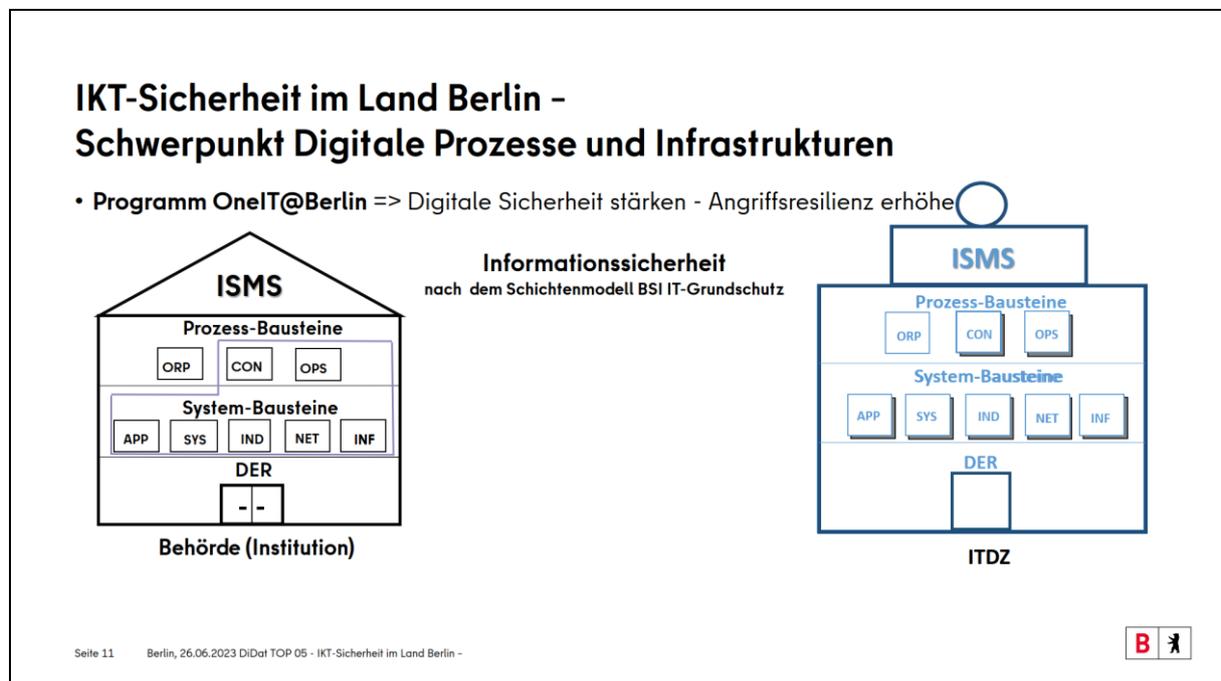
- Mit der Ablösung des dezentralen IT-Betriebes kann eine teilweise Entlastung des Informationssicherheitsmanagements in dezentralen Bereichen erreicht werden.

Seite 10 Berlin, 26.06.2023 DiDat TOP 05 - IKT-Sicherheit im Land Berlin -



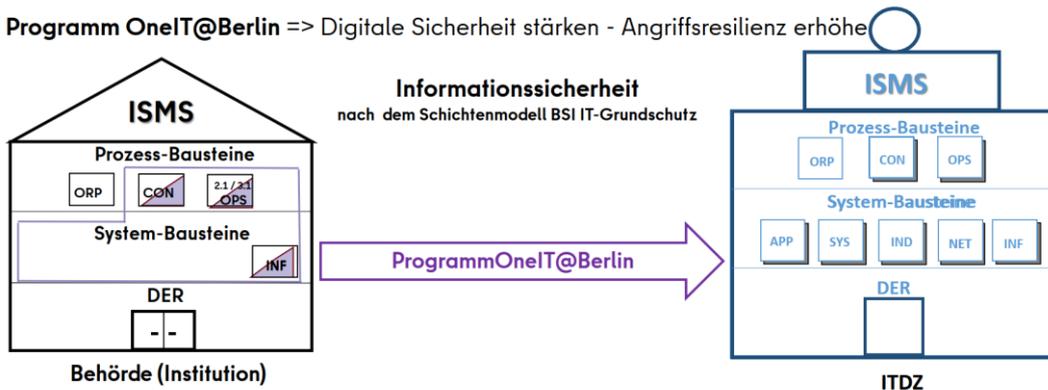
Der erste Punkt sei ein für die Verwaltung relevanter Begriff. Ein Sicherheitsbeauftragter in einer Behörde müsse Informationssicherheit nach BSI IT-Grundschutz – siehe vorherige Folie – umsetzen. Die Ressourcen dafür nähmen wegen des demografischen Wandels ab, und zudem gebe es ein Besetzungsproblem, sodass sie an dem Prozess arbeiten müssten. Mit dem Programm OneIT@Berlin sei vorgesehen, dass sie für die verfahrensunabhängige IT bestimmte Elemente zum ITDZ verlagerten, sodass einige Aufgaben, die sonst jede Behörde für sich erfüllen müsse, dort zentral gebündelt würden. Für die Behörde bleibe somit nur die rechte Seite der Folie umzusetzen.

Bei Dienstleistern müssten derzeit beide das Schichtmodell parallel machen. Wenn sich bei der Behörde der Aufwand reduziere, müsse der Dienstleister stärkere Ressourcen haben, aber er arbeite dann für alle Behörden. Es dürfe keinen Niveauunterschied zwischen Dienstleister und Behörde geben. Es dürften keine Risiken entstehen, die sich auf den Dienstleister auswirkten.



IKT-Sicherheit im Land Berlin - Schwerpunkt Digitale Prozesse und Infrastrukturen

- Programm OneIT@Berlin => Digitale Sicherheit stärken - Angriffsresilienz erhöhen



- Das erfordert eine weitere Stärkung im Bereich des beim betreibenden Dienstleister gebündelten Informationssicherheitsmanagements.

Seite 12 Berlin, 26.06.2023 DiDat TOP 05 - IKT-Sicherheit im Land Berlin -



IKT-Sicherheit im Land Berlin - Schwerpunkt Digitale Prozesse und Infrastrukturen

- Programm OneIT@Berlin => Digitale Sicherheit stärken - Angriffsresilienz erhöhen
- Mit der Ablösung des dezentralen IT-Betriebes kann eine teilweise Entlastung des Informationssicherheitsmanagements in dezentralen Bereichen erreicht werden.
- Die verbleibenden Teilprozesse sind auf gleichem Niveau wie beim Dienstleister umzusetzen. Das erfordert die äquivalente Qualifikation aller Prozessbeteiligten.
- Die Verlagerung von IT zum Dienstleister erfordert zur Erfüllung spezifischer Kundenanforderungen eine weitere Stärkung des Informationssicherheitsmanagements beim Infrastruktur betreibenden Dienstleister.
- Durch die bei den Behörden verbleibenden Teilprozessen sind Risiken für den Betrieb beim Dienstleister zu vermeiden.

Seite 13 Berlin, 26.06.2023 DiDat TOP 05 - IKT-Sicherheit im Land Berlin -



Es gebe eine Bündelung des Infrastrukturbetriebs und der Informationssicherheitsteilprozesse sowie mehr Kontinuität im Informationssicherheitsmanagement der Landesverwaltung, und es gebe nicht mehr so oft reaktives Handeln – siehe nächste Folie. Die Umsetzung müsse nahtlos sein, und sie müssten Defizite bei der Behörde, beim Dienstleister und weiteren Einrichtungen vermeiden.

IKT-Sicherheit im Land Berlin - Ziele

Den Reifegrad des Informationssicherheitsmanagementsystems weiter verbessern:

- Infrastrukturbetrieb und Informationssicherheitsteilprozesse bündeln
- mehr Kontinuität im Informationssicherheitsmanagement der Landesverwaltung durch weniger reaktiv geprägtes Handeln



Eine weitere große Herausforderung sei, dass die EU-Richtlinie 2022/2555 – NIS2 – hohe gemeinsame Cybersicherheitsniveau in der EU definiere und nach einem Umsetzungsgesetz unmittelbar und bis in die regionale Ebene wirksam werde – siehe nächste Folie. Die EU-Richtlinie enthalte somit Anforderungen, die das Berliner CERT und die Verwaltung des Landes Berlin umsetzen müssten. Die Länder unterhielten als Konsequenz kritische Infrastruktur im Sektor Politik und Verwaltung.

IKT-Sicherheit im Land Berlin - Ziele

- **Umsetzung der Anforderungen für ein hohes gemeinsames Cybersicherheitsniveau in der Union gemäß EU RL 2023 / 2555 NIS-2 für Berlin**
 - Fokus Berliner Verwaltung als wichtige kritische Infrastruktur des Sektors Staat und Verwaltung auf regionaler Ebene
 - Umsetzung unmittelbarer Anforderungen (Berlin-CERT und CDC-LV)
 - Umsetzung nach föderal abgestimmten Identifizierungskonzept in Bezug auf die Einrichtungen nach formellen und insbesondere funktionellen Kriterien
 - Fortschreibung der IKT-Sicherheitsarchitektur



Berlin brauche ein föderal abgestimmtes Identifizierungskonzept bezogen auf alle Einrichtungen der Verwaltung, sowohl die unmittelbare als auch nachgeordnete Berliner

Verwaltung. Dazu gehörten auch funktionelle Kriterien: Wie sei die Versorgungsbandbreite der Bevölkerung durch die Einrichtungen, und ergebe sich daraus ein Schwellwert? – Die Frist sei Oktober 2024. Weiterhin müsse es ein Dokument geben, in dem entsprechend dieser Anforderungen die IKT-Sicherheitsarchitektur fortgeschrieben werde.

Personal dafür müsse hochqualifiziert und motiviert sein und brauche ein großes Durchhaltevermögen sowie starken Fokus.

IKT-Sicherheit im Land Berlin - Herausforderungen

- **Digitale Sicherheit und demographischer Wandel**

- **Gewinnung von hochqualifiziertem und motiviertem Personal**
 - mit großem Durchhaltevermögen
 - bei hoher Belastung
 - fokussiert auf die Zielerreichung

Seite 16 Berlin, 26.06.2023 DiDat TOP 05 - IKT-Sicherheit im Land Berlin -



Stefan Ziller (GRÜNE) gibt zu bedenken, die Präsentation habe die Komplexität teilweise gezeigt, aber ein paar Dinge fehlten. So seien auch Mitarbeitende, die die Software verwendeten, ein wichtiger Punkt. Auf eine Anfrage von ihm habe es die Antwort gegeben, dass aus Gründen der Datensparsamkeit nicht gezählt werde, wie viele Mitarbeiterinnen wie regelmäßig Fortbildungen machten, was verantwortungslos wäre. Sei das der Fall?

Nutze die Berliner Verwaltung inzwischen flächendeckend eine Zwei-Faktor-Authentifizierung?

Er begrüße das Bekenntnis zu OneIT@Berlin. Eine einheitliche Verwaltung sei aus IT-Sicherheitsgründen ein Quantensprung. Da dies noch dauere: Wie könne Berlin die Anforderungen, die mit Blick auf IT-Sicherheit in den nächsten Jahren aufträten, ohne OneIT@Berlin meistern?

Die Priorität bei OneIT@Berlin sei, die Senatsverwaltungen zuerst zu behandeln, weil sie einfacher seien. Das sei zwar verständlich, aber andererseits gebe es in den Bezirken viele Daten, stellenweise besonders sensible. Wie handhabe der Senat das?

Marc Vallendar (AfD) weist darauf hin, in den letzten Jahren seien vermehrt Cyberangriffe festzustellen. Wenn Angriffe schwere Schäden verursachten, müsse ein Land sie

völkerrechtlich wie militärische Angriffe betrachten und eine diplomatische oder militärische Reaktion in Betracht ziehen. Finde mit Blick auf das Cyber-Defence-Center neben der Abwehr der Angriffe auch eine Dokumentation der Angriffe statt, auch Hinsichtlich der Ermittlung der Herkunft? Habe Berlin die technische Fähigkeit und Möglichkeit dazu?

Was passiere zudem, wenn im Land Berlin Stromknappheit bestehe? Es gebe sehr gute Sicherungssysteme der Server, aber mit Blick auf die Einführung der E-Akte bestehe das Problem, dass Behörden weitestgehend keine Dieselgeneratoren hätten, die einen Weiterbetrieb ermöglichen. Beständen Pläne zur Verbesserung?

Tobias Schulze (LINKE) erinnert, in letzter Zeit habe es schwerwiegende Angriffe gegeben, die häufig über E-Mail-Anhänge eingetroffen seien, sodass die Kompetenz der Mitarbeitenden eine große Rolle spiele. Wie sei das in die Strategie integriert?

Ein zentraler Grund für die Standardisierung im Rahmen des EGovG Bln seien Sicherheitsgründe, aber derzeit sei Technik noch sehr dezentral. Wie sicher sei die derzeitige Architektur? Sei es als größtes Netz Deutschlands mit einer Vielfalt an Strategien noch auf Dauer schützbar, oder müsse die Zentralisierung deutlich schneller vorankommen?

Angriffe seien oft auf nachgeordnete Bereiche erfolgt, die selbst für ihre IT verantwortlich seien und nicht die notwendigen Standards angewendet hätten – Kammergericht, Hochschulen und auch im Kulturbereich. Wie könne Berlin diese nachgeordneten Bereiche stärker adressieren?

Vor einem Jahr sei die Aussage des damaligen CDO gewesen, dass es eine erhöhte Angriffszahl gegeben habe, aber keine schwerwiegenden Angriffe von russischer Seite oder aus russlandnahen Kreisen. Habe sich das geändert?

Christopher Förster (CDU) interessiert sich dafür, wie umfangreich und in welchem Turnus Schulungen der Mitarbeiter stattfänden. Wie könnten Senatsverwaltungen außerdem gewährleisten, dass ihre Mitarbeiter wüssten, was sie zu tun hätten, wenn sie einen Fehler gemacht hätten?

Die Frage zum Stromausfall interessiere ihn auch, aber möglicherweise sei es aufgrund der Sensibilität erforderlich, die Öffentlichkeit auszuschließen. Er beantrage vor dem Hintergrund, dass Herr Waniek mit Blick auf seine Präsentation vielleicht mehr sagen könne, Ausschluss der Öffentlichkeit.

Dr. Matthias Kollatz (SPD) kommentiert, die Präsentation zeige, dass das Land Berlin in den letzten Jahren Fortschritte erzielt habe. Zu den letzten zwei Jahren gebe es sicherlich einen Austausch zwischen den Bundesländern. Es gebe Beispiele, in denen Berlin nicht besonders gut ausgesehen habe, z. B. beim Kammergericht. Wie sei das Berliner Sicherheitsniveau unter Berücksichtigung der bundesweit schweren Fälle der letzten zwei Jahren zu bewerten?

Gollaleh Ahmadi (GRÜNE) macht darauf aufmerksam, dass der Ausschuss InnSichO das Thema in den letzten zwei Jahren nicht ausführlich behandelt habe. Sie werde die

Präsentation im Rahmen eines Besprechungspunktes auch in diesem Ausschuss anmelden, da das Thema auch eine sicherheitspolitische Frage sei.

Stefan Ziller (GRÜNE) erinnert, er habe vor einiger Zeit abgefragt, welche Windows-Server-Versionen in der Verwaltung liefen; es habe insbesondere bei Feuerwehr und Polizei noch Windows-Server 2012 gegeben, die in diesem Jahr ihr Supportende hätten. Funktioniere der Ablösungsplan, oder bestehe vor Oktober noch Handlungsbedarf?

Staatssekretärin Martina Klement (Skzl) begrüßt die Anregung, das Thema im Ausschuss InnSichO zu behandeln. Sie teile weiterhin die Auffassung, dass Probleme bei Anwenderinnen und Anwendern entstehen, aber ihre Mitarbeiterinnen und Mitarbeiter seien natürlich nicht das Problem. Fehler passierten auch geschulten Anwenderinnen und Anwendern, aber die Fragen nach besserer Schulung seien dennoch berechtigt.

Klaus-Peter Waniek (SenInnSport) erinnert, Mitarbeiterschulungen ständen im Gesetz, und Sicherheitsbeauftragte der einzelnen Behörden hätten die Verantwortung, Schulungen durchzuführen. Sie wollten dies durch ein landesweites Awareness- und Schulungskonzept ablösen und würden dabei den Hauptpersonalrat und die Beschäftigtenvertretungen beteiligen. Wer welche Schulung gemacht habe, sei allerdings Mitarbeiterüberwachung und sei nicht umsetzbar. Einzelne Behörden könnten aber eine statistische Zahl erheben, wie viele ihrer Mitarbeiter an Schulungen teilgenommen hätten.

Die Sicherheitsbeauftragten des CERT erhielten regelmäßig Informationen zu Phishing- und Spamwellen, die sie an Behörden weitergäben. Zudem gebe es die Verabredung, dass Empfänger von Phishing- oder Spammails sie an ihre Sicherheitsbeauftragte oder direkt an das CERT weitergeben könnten, die es dann behandelten und bei Bedarf darauf reagierten. Der Meldeprozess sei einer der besten Prozesse im Informationssicherheitsmanagement im jährlichen Sicherheitsbericht; er gehe sehr schnell und liege bei weit über 90 Prozent.

Sie versuchten die Herkunft von Spam- und Phishingmail zu identifizieren und brächten dabei zumindest die IP-Adresse in Erfahrung. Dies erlaube dem CERT, wie im EGovG Bln von 2021 vorgesehen, proaktiv entgegenzuwirken. Das CERT schlage vor, IP-Adressen und Domänen zu sperren, und er bestätige es im Anschluss. Analysen und Untersuchungen zu Cyberkriminalität oblägen der Polizei und deren Zentraler Ansprechstelle Cybercrime.

Es gebe jährliche Angebote zur Fortbildung, z. B des IT-Planungsrates und der FITKO, die sie an Behörden weitervermittelten. Bis Ende des Jahres führten sie ein Awarenesskonzept ein, das sie auch mit der VAK abstimmen würden. Das ITDZ solle zudem eine Spamanalyseplattform zur Verfügung stellen, sodass Beschäftigte verdächtige Mails direkt dort eintragen könnten. Dies sei aufgrund knapper Ressourcen beim ITDZ im Verzug, schreite aber voran.

Eine Zwei-Faktor-Authentifizierung gebe es an wenigen Stellen, vor allem im Rechenzentrumsbetrieb. Die meisten Sachen liefen über Passwörter. Medien stellten Passwörter als nicht mehr zeitgemäß dar. Der BSI-Grundschutz schreibe aber: Wenn es keine Möglichkeit gebe zu prüfen, ob ein Passwort kompromittiert sei oder an anderer Stelle registriert worden sei, müsse man weiter Passwörter für Authentifikationen einsetzen.

Für eine Zwei-Faktor-Authentifizierungs-Infrastruktur müsse Berlin alle Fachverfahren und Geräte umstellen, was ein großer Aufwand sei, den das Land mittelfristig angehen müsse.

Die behördlichen Sicherheitsbeauftragten seien verpflichtet, das ISMS umzusetzen, was ihnen mit den zur Verfügung stehenden Ressourcen mehr oder weniger gut gelinge. In den Sicherheitsberichten sei bemerkbar, wenn der Stellenanteil von Sicherheitsbeauftragten nicht 100 Prozent betrage.

Die Daten der Bezirke, auch Sozialdaten, bestehe größtenteils das ITDZ. Sie setzten Fachverfahren ein, die Senatsverwaltungen bereitstellten, und Bezirke seien nur ausführende Einrichtungen, die Software verwendeten, die andere Stellen vorgäben.

Es gebe keine zentrale Erfassungsmöglichkeit für Schulungsnachweise der Dienststellen. Möglicherweise könnten sie etwas mit dem Hauptpersonalrat erreichen.

Auf Ermittlung von Angriffen wolle er im Detail im nichtöffentlichen Teil eingehen.

Der Weiterbetrieb bei Stromausfall falle in den Katastrophenschutz. Seine Dienststelle unterstützte den Katastrophenschutz, aber er falle in einen anderen Dienstbereich.

Er stimme zu, dass eine schnelle Standardisierung die Sicherheit verbessere.

Eine Großzahl der Mitarbeiter reagierten schnell und hätten Vertrauen in Sicherheitsbeauftragte, und die Meldewege funktionierten schnell. Das Cyber-Defence-Center des ITDZ fange viel auffälliges, nicht qualifiziertes Verhalten von Anwendern ab, was aber der geringste Anteil sei.

Frau Ahmadi bestätige er, dass es sich um eine sicherheitspolitische Frage handele, und sie arbeiteten mit dem Bereich Cybersicherheit von SenInnSport eng zusammen. Derzeit gehe es um die Weiterentwicklung für NIS2 des BSI zur Zentralstelle. Parallel zur Ausschusssitzung finde ein Workshop zum Thema statt, an dem ein Kollege von der Cybersicherheit das Land Berlin vertrete.

Sie hätten alle Bereiche für das Supportende von Windows-Server 2012 sensibilisiert. Sie arbeiteten intensiv an der Beseitigung. Es gebe das IKT-Management, und sie sensibilisierten noch in dieser Woche im IKT-Lenkungsrat für das Thema. Die Behörden müssten es aber in eigener Verantwortung umsetzen.

Christopher Förster (CDU) erkundigt sich, ob es korrekt zusammengefasst sei, dass das Land Mitarbeiter nicht zu Schulungen verpflichten könne, weil der Personalrat und der Datenschutz ein Problem seien. Er halte es für wichtig, in die Kommunikation mit Personalräten zu gehen. Für Mitarbeiter eines Wirtschaftskonzerns wäre es undenkbar, an Schulungen nicht teilzunehmen. Vielleicht müsse die Verwaltung dabei neue Wege finden.

Meike Kamp (BlnBDI) wirft ein, Dienstherrinnen und Dienstherrn dürften Mitarbeiterinnen und Mitarbeiter selbstverständlich anweisen, Schulungen zu machen und Vorgaben zu erfüllen, um IKT-Mittel einzusetzen. Sie habe die Aussagen so verstanden, dass nur die einzelnen Dienstherrinnen und Dienstherrn nicht gebündelt dem Landesbevollmächtigten

Informationssicherheit, Herrn Waniek, mitteilen könnten, ob individuelle Mitarbeiterinnen und Mitarbeiter die Schulung durchgeführt hätten.

Stefan Ziller (GRÜNE) fordert, es müsse im Land Berlin eine statistische Übersicht darüber geben, wie hoch der Anteil einer Verwaltung ist, die eine Schulung belegt hätten. Wenn dafür eine Gesetzesänderung nötig ist, bitte er Herrn Waniek, dies dem Ausschuss mitzuteilen.

Weitere Beratung siehe nichtöffentliche Anlage zum Inhaltsprotokoll.

Nachdem die Öffentlichkeit wiederhergestellt ist, stellt **Vorsitzender Johannes Kraft** fest, dass der Tagesordnungspunkt abgeschlossen sei.

Punkt 6 der Tagesordnung

Verschiedenes

Siehe Beschlussprotokoll.