Abgeordnetenhaus BERLIN

19. Wahlperiode

Plenar- und Ausschussdienst

Inhaltsprotokoll

Öffentliche Sitzung
Teilweise nichtöffentlich zu TOP 3 – neu –

Ausschuss für Digitalisierung und Datenschutz

76. Sitzung
24. August 2026

Beginn: 14.05 Uhr
Schluss: 17.46 Uhr
Vorsitz: Johannes Kraft (CDU);
zeitweise Carsten Schatz (LINKE)

Vor Eintritt in die Tagesordnung

Siehe Beschlussprotokoll.

Punkt 1 der Tagesordnung

Aktuelle Viertelstunde

Vorsitzender Johannes Kraft schlägt vor, die schriftlich eingereichte Frage der Fraktion Die Linke unter dem TOP 3 zu behandeln.

Der **Ausschuss** beschließt entsprechend.

Carsten Schatz (LINKE) fragt spontan, wie der am 11.08. vom Senat beschlossene Digitalcheck zukünftig umgesetzt werden könne. Werde einem Gesetzestext ein Text vorangestellt, der die aktuelle Situation darstelle, oder werde der Senat im Vorfeld eines Gesetzesbeschlusses Hindernisse beseitigen?

Staatssekretär Florian Hauer (Skzl) antwortet, dass beides gemacht werden könne. Es sei sinnvoll, die vorangegangenen Überlegungen zur Digitaltauglichkeit zu dokumentieren. Er erwarte aber auch, dass die Überlegungen im Vorfeld zu einer besseren Digitaltauglichkeit führten.

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

Punkt 2 der Tagesordnung

Bericht aus der Senatskanzlei

Staatssekretär Florian Hauer (Skzl) berichtet, dass am 25.06. eine Verwaltungsratssitzung des ITDZ Berlin stattgefunden habe, wo der Jahresabschluss 2025 festgestellt und ein Nachtragswirtschaftsplan für 2026 beschlossen worden sei. – Die Zuständigkeitsverordnung sei am 19.07. in Kraft getreten. Die Datenbank zum Zuständigkeitskatalog sei am 07.08. gestartet. Es gebe noch technische Schwierigkeiten, die behoben würden. Es gebe kein Schlagwortverzeichnis, aber eine KI-gestützte Suchfunktion sei geplant, um den Bürgern und Bürgerinnen eine leichte Ermittlung der Zuständigkeit zu ermöglichen. – Der Digitalcheck sei am 11.08. im Senat behandelt worden. Es werde mit Nachdruck an einer Bestands- und Planungsübersicht für den IT-Bereich gearbeitet. Der IT-Sicherheitsvorfall zeige die Notwendigkeit der Beschleunigung. – Zur noch aus der letzten Sitzung offenen Frage zur Unit GovTech Berlin berichte er, dass es einen intensiven Austausch mit den Bedarfsträgern gebe, weil die Bedarfe weiterhin sehr hoch seien. Diese würden nun priorisiert und Pilotprojekte zur KI-basierten Sitzungsprotokollierung und Audiotranskription angestoßen.

Meike Kamp (Berliner Beauftragte für Datenschutz und Informationsfreiheit) berichtet, dass es einen massiven Anstieg an Datenschutzbeschwerden in den Mitgliedsstaaten der EU gebe. – Die deutschen Datenschutzbeauftragten hätten ein Impulspapier zur Modernisierung des Datenschutzes veröffentlicht. Dies sei ein Beitrag zur Diskussion, die auch die föderale Struktur der Datenschutzaufsicht betreffe. Bis Mitte September könnten Stellungnahmen eingereicht werden, über die auf einer Veranstaltung diskutiert werden solle. – Der Europäische Datenschutzausschuss habe im Juli Leitlinien zur Anonymisierung veröffentlicht, an denen Berlin stark mitgewirkt habe. Diese Leitlinien seien nun in Konsultation.

Der **Ausschuss** schließt den Tagesordnungspunkt ab.

Punkt 3 der Tagesordnung – neu –

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 bittet, dass angesichts der Tagesordnung die Begründungen kurzgehalten würden, da der Anlass bekannt sei.

Stefan Ziller (GRÜNE) bittet, dass der Senat den aktuellen Sachstand zu dem Vorfall darlege.

Jan Lehmann (SPD) bittet um Erläuterung, wie die Arbeit der Senatsverwaltungen während des Vorfalls habe fortgeführt werden können und wie mit anderen Behörden wie der Datenschutzbeauftragten zusammengearbeitet worden sei.

Staatssekretär Florian Hauer (Skzl) erläutert, dass am Abend des 14.08. ein erheblicher Cyberangriff auf das Berliner Landesnetz festgestellt worden sei. Die Senatsverwaltungen SenMVKU und SenStadt seien aufgrund des großen Gefährdungspotenzials vom Netz genommen worden. Da nicht ausgeschlossen werden könne, dass weitere Teile des Netzes betroffen seien, sei der IKT-Notfallstab aktiviert worden, der nun täglich tage.

Als weitere Maßnahme sei eine externe Firma für Scans und eine forensische Untersuchung der Systeme, die als potenzial betroffen identifiziert worden seien, beauftragt worden. Bei einem Fund gebe es eine genauere Analyse. – Es sei Stand jetzt nur ein Datenabfluss von Geodaten festgestellt worden, die im Open-Data-Bereich zugänglich gewesen seien. Es gebe im Moment keine weiteren Hinweise auf Datendiebstahl und Manipulationen. Nach den aktuellen Erkenntnissen seien die Wahlen im September nicht gefährdet. Für die punktuellen Ausfälle bei der Beantragung der Briefwahl gebe es keine Hinweise auf einen Zusammenhang mit dem IT-Vorfall. Alle gegebenen Informationen seien in der dynamischen Situation nur als vorläufig zu betrachten.

Aktuell sei es gelungen, den Angriff so weit wie möglich zu isolieren. Um auszuschließen, dass es noch Schläfer im System gebe, würden die Scans fortgesetzt und ausgeweitet. Die Scans seien auf einem hohen Niveau aktiv, sodass bei einem erneuten Angriff schnell reagiert werden könne. Die Schutzmaßnahmen sowie der IKT-Notfallstab würden bis auf Weiteres aufrechtgehalten. Daher sei nach einer Risikoabwägung beschlossen worden, die betroffenen Senatsverwaltungen wieder ans Netz zu nehmen, weil diese die Sicherheitsstandards erheblich erhöht hätten, und die Verwaltung ihre Arbeit fortsetzen müsse. – Die Fachpolitiker, die Öffentlichkeit, der Senat und die Bezirke über den Rat der Bürgermeister seien zeitnah informiert worden. Es gebe einen Austausch mit der Datenschutzbeauftragten, dem BSI und den Ermittlungsbehörden wie dem LKA Berlin. Der Fokus liege aber bei der akuten Gefahrenabwehr.

Es sei absehbar, dass die Ursachen strukturelle Defizite in der IT-Sicherheit seien. Die Politik müsse die notwendigen Ressourcen bereitstellen und die IT-Sicherheit langfristig stärken. Es brauche strukturelle Reformen hinsichtlich der Zentralisierung der IT und Investitionen in Hardware. Das nächste Parlament und die nächste Regierung müssten diese Aufgabe im Blick behalten.

Staatssekretär Stephan Machulik (SenStadt) ergänzt, dass sofort nach Entdeckung des Vorfalls der Notfallstab der Senatsverwaltung einberufen worden sei. Die Hauptanliegen waren, die Gefahr einzudämmen und den Dienstbetrieb aufrechtzuerhalten. Zwischen dem 14.08. und der Wiederankopplung an das Netz seien die SenStadt sowie für SenMVKU mit Einschränkungen arbeitsfähig gewesen. Die Fachverfahren seien einsatzfähig geblieben, und es habe keinen Datenverlust gegeben. Die Hauptproblematik habe in der externen Kommunikation gelegen. Daher seien Prioritäten wie das Wohngeld gesetzt und für alle Fachanwendungen

funktionierende Bypass-Strategien entwickelt worden. Die Wohngeldzahlungen hätten so durchgeführt werden können. Auch für andere Anwendungen wie dem Qualifizierten Straßennetz würden Lösungen erarbeitet, um die Anträge wiederherstellen zu können und eine externe Kommunikation zu ermöglichen. Der Vorfall sei kollegial bearbeitet worden. Der Wiederanschluss an das Netz sei vom BSI bestätigt worden. – Die Mitarbeitenden seien vor der Abkopplung informiert worden. Homeoffice sei dann entsprechend der Zielvereinbarung nicht möglich gewesen. Es seien aber individuelle Lösungen für Mitarbeitende gefunden worden.

Staatssekretär Arne Herz (SenMVKU) erläutert, dass die beiden Senatsverwaltungen seit der Aufteilung immer noch eine gemeinsame IT im Rahmen einer Servicevereinbarung hätten. Er sei dankbar dafür, da die IT-Stelle gute Arbeit geleistet habe. Gestern seien einzelne Bezirke eingebunden worden, um den bezirklichen Zugriff auf Fachverfahren wie Wohngeld und das wichtige VMS zu testen. Kleinere Probleme seien in den nächsten Tagen noch zu erwarten, aber wichtig sei, dass die Fachverfahren wieder am Netz seien und die Bezirke auf die Datenbestände zugreifen könnten.

Stefan Ziller (GRÜNE) bittet um Auskunft, wie der Ablauf des Angriffs war, um für die Öffentlichkeit Transparenz und Vertrauen herzustellen. Wann habe der Angriff gestartet und wie lange habe es bis zur Entdeckung gedauert? Es sei besorgniserregend, wenn der Zugriff länger als einen Tag gedauert habe, ohne dass es aufgefallen sei. Die Pressekonferenz des Regierenden Bürgermeisters sei daher verharmlosend gewesen. Wie sei dem Täter der Zugriff gelungen? Gebe es eine unbekannte Lücke, ein fehlendes Update oder sei es durch einen Fehler eines Mitarbeiters passiert? Er bitte um Klarstellung, ob der Angriff nur isoliert oder die Lücke geschlossen sei. Habe es mehrere Zugriffe oder einen kontinuierlichen gegeben? – Er appelliere, bereits jetzt im Krisenstab die nötigen strukturellen Entscheidungen der Zukunft festzuhalten. Die Zeitpläne etwa der Migration der Bezirke zum ITDZ müssten möglicherweise beschleunigt werden. Bei einer Zentralisierung müsse es weiterhin eine klare Trennungen zwischen den Segmenten geben, sodass ein Angriff nicht auf alles Zugriff habe. Seien weitere kritische Bereiche der Verwaltung identifiziert und Notfallpläne für einen IT-Ausfall für diese erstellt worden?

Marc Vallendar (AfD) unterstreicht, dass das Vorhaben einer volldigitalisierten Verwaltung auch besondere Risiken berge. Die Ursachen es Angriffs seien noch unklar, aber Sicherheitsleitlinien des Senats von 2017 seien als veraltet gerügt worden, und es habe seitdem keine Überarbeitung gegeben. Er bitte um Auskunft über die Schadenssumme durch die Ausfallzeiten und die Beauftragung des externen Dienstleisters. Wie seien die Mitarbeitenden über die Präsenzpflicht informiert worden, wenn E-Mails nicht hätten gesendet werden können? Gebe es ähnliche Vorfälle auch in anderen Bundesländern? Warum sei Berlin besonders betroffen? – Der Ausschuss solle einen gegebenenfalls eingestuften schriftlichen Lagebericht erhalten, der den Ablauf des Angriffs schildere.

Vorsitzender Johannes Kraft merkt an, dass es besser wäre, Fragen zurückzustellen, die erst im nichtöffentlichen Teil beantwortet werden könnten.

Carsten Schatz (LINKE) fragt nach, ob der veröffentliche Zero-Day des GIS-Servers involviert gewesen sei. Es habe im Vorfeld des Angriffs Auffälligkeiten gegeben. Welche Services neben dem VMS seien betroffen gewesen? Es habe auch Störungen bei anderen Senatsver-

waltungen gegeben, etwa beim Briefwahlantrag und Bildung und Teilhabe. Gebe es eine Übersicht, welche Services in dem Zeitraum insgesamt nicht erreichbar gewesen und was die Ursachen seien? Gebe es Hinweise auf weitere kompromittierte Komponenten des Landesnetzes? – Wie sei der beauftragte US-Sicherheitsdienstleister ausgewählt worden und welche Kosten verursache das? Sei das mit der Landesdatenschutzbeauftragten abgesprochen worden? Wann sei der Beauftragten der Vorfall gemeldet worden? – Wie sei die Kommunikation mit den Bezirken abgelaufen? Es habe Kritik gegeben. – Welche strukturellen Änderungen folgten aus dem Vorfall? Werde die Zentralisierung der IT der SenStadt und SenMVKU beim ITDZ vorgezogen? Welche Investitionen müssten getätigt werden? – Er bitte ebenfalls um eine detaillierte Darstellung der Ereignisse wie der Erkennung, Meldungen und Maßnahmen. Warum sei der Notfallstab erst am 17.08. eingerichtet worden, obwohl die Isolierung bereits am 14.08. erfolgt sei? – Bei den Aussagen zum Datenabfluss gebe es einen Widerspruch. Medien hätten von abgeflossenen personenbezogenen Daten gesprochen, dem der Senat widerspreche. – Habe die Risikoabwägung auch die Integrität der Systeme und Daten berücksichtigt? Welche Änderungen habe es bei der IT der betroffenen Senatsverwaltungen gegeben, die die Netzanbindung erlaubten? – Er beantrage die Vertagung des Tagesordnungspunkts. Es brauche Vorschläge, wie auch in der Zeit nach der Wahl eine parlamentarische Begleitung des Vorfalls sichergestellt werden könne, weil die nächste Sitzung des Ausschusses frühestens im Januar 2027 stattfinde.

Vorsitzender Johannes Kraft weist hin, dass es in dieser Legislaturperiode noch mindestens eine Sitzung gebe und dass Sondersitzungen möglich seien.

Jan Lehmann (SPD) bittet, dass „sensible und personenbezogene Daten“ definiert werde. Es gebe eine unklare Verwendung durch den Regierenden Bürgermeister. Sei der Vorfall als Datenschutzvorfall gemeldet worden und wenn ja wann? – Bei den Ereignissen sollten auch Uhrzeiten angegeben werden, da es sein könne, dass diese für den Ablauf relevant seien. Wann fielen erste Unstimmigkeiten auf, die rückblickend Hinweise auf den Angriff gegeben hätten? – Wer genau habe die Entscheidungen, etwa zur Abkopplung vom Netz getroffen? – Wer habe die forensische Untersuchung zu diesem frühen Zeitpunkt beauftragt? Wer sei der Dienstleister und was umfasse der Auftrag? – Hätte der Angriff genauso stattgefunden, wenn die Server der beiden Senatsverwaltungen bereits beim ITDZ angesiedelt gewesen wären? Seien andere Verwaltungen ähnlich verwundbar? Gebe es Hinweise auf das Ziel des Angriffs? Wie viele Fachverfahren seien betroffen? Was leiste das Cyber Security Operation Center bei der Organisierung der Abwehr? Wie werde die Cybersicherheit in der Berliner Verwaltung zukünftig gestärkt? Gebe es einen Austausch mit anderen Bundesländern? Sei ein gemeinsames Vorgehen mit dem Bund sinnvoll?

Dr. Matthias Kollatz (SPD) merkt an, dass es nun wichtig sei, die Maßnahmen schnell umzusetzen, und nicht auf die Konstituierung des neuen Senats zu warten. – Der Vorfall am Kammergericht sei nicht zu vergleichen, weil es dieses Mal gelungen sei, die Senatsverwaltungen nach einer Woche wieder arbeitsfähig zu bekommen. Seinerzeit habe auch das ITDZ gehandelt, obwohl es nicht sollte, weil die Justiz die Entscheidung getroffen habe, die IT nicht ins ITDZ zu migrieren. Das sei etwas, das geprüft und neu beschieden werden sollte. – Er stelle klar, dass seine Fraktion die Arbeit des aktuellen CDO unterstütze. – Es brauche eine Verbesserung der Erkennungsmechanismen, um Angriffe frühestmöglich zu erkennen. Berlin sei als Hauptstadt und durch seine weltweite Bekanntheit häufiger Ziel von Angriffen. – Das Ziel der IT in Berlin sei, dass Daten nur noch einmal eingegeben werden müssten. Das sei

gewünscht, führe aber dazu, dass Programme Zugriff auf die zentral lagernden Daten bekämen und somit die Abwehr von Angriffen besonders wichtig werde. – Gegebenenfalls müsse der Ausschuss auch nach der Wahl außerordentliche Sitzungen durchführen.

Gollaleh Ahmadi (GRÜNE) bittet um Klarstellung, dass wirklich ausgeschlossen werden könne, dass sicherheitsrelevante oder personenbezogene Daten abgeflossen seien. – Was von der vor einem Jahr beschlossenen Cybersicherheitsstrategie für Berliner Behörden sei bereits umgesetzt worden? Habe dies beigetragen, Schlimmeres zu verhindern? Könnten Maßnahmen aus dem Strategiepapier beschleunigt umgesetzt werden? Es müsse bedacht werden, dass in Berlin als Bundeshauptstadt in vier Wochen Wahlen anstünden.

Staatssekretär Florian Hauer (Skzl) erläutert, dass der Angriff sich bis zur Abschaltung des Netzzugangs der betroffenen Verwaltungen am 14.08. über mehrere Tage erstreckt habe. Die Entscheidung der Abschaltung sei von ihm als politisch Verantwortlichem in enger Abstimmung mit den Landesbevollmächtigten und den beiden Senatsverwaltungen getroffen worden. Dass der Angriff über mehrere Tage unerkannt geblieben sei, sei nicht gut, aber letztlich sei er erkannt worden, bevor größerer Schaden entstanden sei. Zur Ursache und Ausgangspunkt des Angriffs fehlten noch belastbare Erkenntnisse. Die Ermittlungen würden von der Staatsanwaltschaft und dem LKA geleitet.

Den Angriff isoliert zu haben, bedeute, dass die betroffenen Verwaltungen vom Netz genommen worden seien. Dann sei der Angreifer aus dem System entfernt worden. Die forensischen Untersuchungen würden fortgesetzt und nun auch auf andere Verwaltungen ausgeweitet. Bislang seien die Untersuchungen bei Verdachtsmomenten gestartet worden. Kurzfristige Maßnahmen würden nun vorgenommen und umfassten unter anderem das Passwortmanagement für alle Mitarbeiterinnen und Mitarbeiter. Es gebe noch Verbesserungsbedarf auf allen Ebenen. Problematisch sei auch, dass es keinen genauen Überblick über die Informationstechnik in Berlin gebe. Es werde nun die Erstellung einer Bestands- und Planungsübersicht veranlasst. Alternative Lösungswege würden geprüft und aufgesetzt, aber dennoch könnten im schlimmsten Fall bei einem großflächigen Angriff wichtige Verwaltungsleistungen nicht aufrechterhalten werden. Es sei nun politische Aufgabe, die Wahrscheinlichkeit solcher Angriffe deutlich zu minimieren, auch wenn ein absoluter Schutz nie möglich sei.

Die Schadenssumme sei noch unbekannt. Die Ermittlung der Höhe werde Teil des Ermittlungsverfahrens sein. Ihm sei nicht bekannt, ob andere Bundesländer von ähnlichen Angriffen betroffen seien. Berlin stehe im Austausch mit dem Cyber-Abwehrzentrum, anderen Sicherheitsbehörden des Bundes und dem BSI. Es sei unklar, warum Berlin angegriffen worden sei. Es gebe noch keine belastbaren Erkenntnisse zu den Tätern oder ihren Motiven. Er sichere zu, Fragen nach bestem Wissen und Gewissen zu beantworten.

Es seien öffentlich zugängliche Geodaten abgeflossen, was logisch ausschließe, dass es sich um sensible Daten handele. Sensible Daten umfassten seiner Meinung nach personenbezogene Daten sowie Daten zu kritischer Infrastruktur. Das externe Sicherheitsunternehmen sehe nur Metadaten, keine Inhaltsdaten. Daher sei es datenschutzrechtlich wahrscheinlich unbedenklich. Die Kritik an einer verspäteten Kommunikation mit den Bezirken nehme er auf. In den ersten Tagen sei nach dem Need-to-know-Prinzip vorgegangen, und abgesehen vom Parlament seien vor allem Betroffene informiert worden. Der Fokus habe aber auf der Gefahren-

abwehr gelegen. Beim Wiederanschluss an das Netz sei der RdB aber proaktiv informiert worden.

Die Entscheidung, den IKT-Notfallstab einzuberufen, sei am 14.08. getroffen worden, nachdem festgestellt worden sei, dass möglicherweise der gesamte AD-Verbund betroffen sei. Rückblickend hätte dies früher geschehen können, aber zum damaligen Zeitpunkt habe sich das Ausmaß erst nach und nach offenbart. Die ersten Unstimmigkeiten seien Ende Juli aufgetreten, aber es habe noch keinen Hinweis auf einen Hackerangriff gegeben. Zu diesem Zeitpunkt sei aber bereits das Forensik-Unternehmen beauftragt worden. Die Sensibilität der Mitarbeiter habe dazu beigetragen, den Angriff frühzeitig zu erkennen und den Schaden einzudämmen.

Die Risikoabwägung für die Wiederanbindung der Verwaltungen sei in enger Abstimmung mit dem BSI erfolgt. Die Restrisiken seien gegen die Notwendigkeit abgewogen worden, wichtige Funktionen des Staates aufrechtzuerhalten. Die Sicherheitsmaßnahmen seien aktuell sehr hoch. Das Cyber Defence Center sei eingebunden und arbeite intensiv. Die Zusammenarbeit innerhalb des Senats und mit dem ITDZ funktioniere pragmatisch und sehr gut.

Es gebe in der aktuellen Situation keine hundertprozentige Sicherheit. Er könne nur den aktuellen Stand wiedergeben, dass nur öffentlich zugängliche Daten abgeflossen seien. – Aus der Cybersicherheitsstrategie sei bereits die Kooperationsvereinbarung mit dem BSI umgesetzt worden. Dieses habe hilfreiche Unterstützung leisten können. Weitere kurzfristige Maßnahmen seien das Passwortmanagement und die Umsetzung des IKT-Business-Continuity-Managements. Auch der IT-Überblick werde unverzüglich erarbeitet. Notwendige strukturelle Lösungen würden jetzt dokumentiert und anschließend umgesetzt. Der nächster Angriff komme, daher müssten auch zukünftige Regierungen in die IT-Sicherheit investieren.

Staatssekretär Stephan Machulik (SenStadt) erläutert, dass Wohngeld- und Kindergeldbezieher einen expliziten Antrag auf BuT stellten müssten, daher liege dies im Fachbereich Wohnen. – Das qualifizierte Straßennetz laufe auf den Servern von SenStadt. Beim Briefwahlantrag müsse die Anschrift verifiziert werden, was über dieses System laufe. Das LABO habe aber eine digitale Kopie des Verzeichnisses auf eigenen Servern liegen, sodass Ausfälle nichts mit dem Vorfall zu tun gehabt hätten. – Sensible Geodaten befänden sich dezentral bei einem Dienstleister und seien deutlich stärker gesichert. – Eine Informationsmail sei vor der Abschaltung an die Mitarbeitenden geschickt worden. Darin sei auf die seit Jahren existierende Notfallseite hingewiesen worden.

Staatssekretär Arne Herz (SenMVKU) ergänzt, dass die Notfallseite extern erreichbar sei, sodass der Zugriff auch bei Störungen des Netzes möglich sei. Daran sei in der E-Mail erinnert worden. Auf der Notfallseite seien dann regelmäßig Updates veröffentlicht worden, um die Mitarbeitenden intern zu informieren. – Es seien circa 40 interne und externe Fachverfahren betroffen gewesen. Da auch kein Zugriff auf Daten von außen bestand, sei auch eine interne Bearbeitung und kein Zugriff durch die Bezirke nicht möglich gewesen. Wie die Kommunikationswege mit den Bezirken zukünftig verbessert werden könnten, werde geprüft. Es müsse nun ermittelt werden, wo es weitere Redundanzen brauche.

Meike Kamp (Berliner Beauftragte für Datenschutz und Informationsfreiheit) führt aus, dass zwei Meldungen der SenStadt und dem ITDZ am 17.08. übermittelt worden seien. Das ITDZ

habe mitgeteilt, dass es noch unklar sei, ob personenbezogene Daten abgeflossen seien. Die SenStadt habe mitgeteilt, dass es nach aktuellem Stand keine Zugriffe auf personenbezogene Daten gegeben habe. Sie erwarte weitere Informationen bei Fortschreiten der Ermittlungen.

Staatssekretär Alexander Slotty (SenStadt) korrigiert, dass die SenStadt bereits am 14.08. an die Datenschutzbeauftragte gemeldet habe. Am 15.08. sei eine Nachmeldung mit dem Aktenzeichen des LKA Berlin erfolgt. Es gebe schriftliche Bestätigungen.

Meike Kamp (Berliner Beauftragte für Datenschutz und Informationsfreiheit) sichert zu, die Diskrepanz aufzuklären.

Vorsitzender Johannes Kraft empfiehlt, den TOP 5 – neu – zu vertagen.

Gollaleh Ahmadi (GRÜNE) schlägt vor, dass auch die Anhörung unter TOP 4 – neu – vertagt oder vorgezogen werden solle.

Vorsitzender Johannes Kraft wendet ein, dass eine Unterbrechung des laufenden TOP nicht sinnvoll sei.

Dr. Marco Holtz (Medienanstalt Berlin-Brandenburg) sichert zu, dass auch bei einer Verschiebung der Anhörung unter TOP 4 – neu – die Medienanstalt zur Verfügung stehe.

Vorsitzender Johannes Kraft schlägt vor, TOP 6 – neu – ohne Aussprache zu beschließen.

Der **Ausschuss** beschließt, die TOP 4 – neu – und TOP 5 – neu – zu vertagen.

Vorsitzender Johannes Kraft schlägt vor, dass für die Fortsetzung der Besprechung die Öffentlichkeit ausgeschlossen werde.

Der **Ausschuss** beschließt entsprechend.

[Fortsetzung in nichtöffentlicher Sitzung –
siehe nichtöffentliche Anlage zum Inhaltsprotokoll.]

Punkt 4 der Tagesordnung – neu –

Besprechung gemäß § 21 Abs. 3 GO Abghs 0169
Radikalisierung und Extremismusprävention im digitalen Raum DiDat
(auf Antrag der Fraktion der SPD und der Fraktion der CDU)

Hierzu: Anhörung

Vertagt.

Punkt 5 der Tagesordnung – neu –

Besprechung gemäß § 21 Abs. 3 GO Abghs 0157
Mehr Nachnutzung für die Berliner Verwaltung: Warum Berlin in Sachen IT-Fachverfahren das Rad nicht neu erfinden sollte DiDat
(auf Antrag der Fraktion Bündnis 90/Die Grünen)

Hierzu: Anhörung

Vertagt.

Punkt 6 der Tagesordnung – neu –

Antrag der Fraktion Bündnis 90/Die Grünen 0167
Drucksache 19/3309 DiDat
Digitale Verwaltung: Erst Mönchengladbach, dann Wiesbaden und jetzt Berlin: Passierschein A38

Vertagt.

Punkt 7 der Tagesordnung – neu –

Verschiedenes

Siehe Beschlussprotokoll.