Abgeordnetenhaus BERLIN

Drucksache 19/3519
09.09.2026

19. Wahlperiode

Dringlicher Antrag

der Fraktion Bündnis 90/Die Grünen und der Fraktion Die Linke

Nach dem größten Cyberangriff auf Berlin: Transparenz schaffen, aufklären und IKT neu ordnen

Das Abgeordnetenhaus wolle beschließen:

Der Senat wird aufgefordert, die unmittelbare Aufklärung und Bearbeitung des schlimmsten Cyberangriffs in der Geschichte Berlins in folgenden Punkten zu intensivieren:

- Der Senat muss schnellstmöglich Transparenz über Betroffenheiten schaffen. Die Betroffenengruppen außerhalb der Verwaltung müssen zumindest nach eingrenzbaren Kategorien benannt werden.
- Die verwaltungsübergreifende Zusammenarbeit im Krisenmanagement muss institutionalisiert sichergestellt werden.
- Eine umfassende Überprüfung der Speicherung sicherheitskritischer Dokumente in allen Ressorts ist durchzuführen. Die Überprüfung umfasst insbesondere: eine Bestandsaufnahme, wo und in welcher Form sicherheitskritische Dokumente sowie Zugangsdaten und Passwörter derzeit gespeichert werden, wie die Speicherung erfolgt und der Schutzbedarf sichergestellt wird (Orte, Rolle-Rechte-Konzepte, Verschlüsselung) und die Identifikation und Priorisierung von Verwaltungsbereichen mit erhöhtem Handlungsbedarf.
- Eine TaskForce „Passwortnutzung“ ist einzusetzen, die einen systematischen Scan sämtlicher Fileserver nach Dateinamen und -inhalten, insbesondere nach Dateien mit Bezeichnungen wie „passwort.docx“, „passwörter.xlsx“, „logins.txt“, „zugangsdaten.*“ o. Ä. durchführt und mit Personalvertretungen dafür Sorge trägt, dass Passwörter im Landesnetz nicht mehr im Klartext auf welchem File-Server auch immer liegen.

Darüber hinaus wird der Senat aufgefordert, unverzüglich, spätestens bis zum **1. Oktober 2026**, eine Expert*innengruppe zu berufen, die den Auftrag erhält, einen Vorschlag für eine Überarbeitung der Berliner IKT-Architektur zu erarbeiten. Dabei gelten folgende Leitplanken:

- Grundlage bilden die bisherigen Vorarbeiten in den Senatsverwaltungen. Die Expert*innengruppe soll explizit auch das geltende EGovG Bln und seine universelle Abnahmepflicht hinterfragen und die Weiterentwicklung zum Digitalgesetz als Chance begreifen, die IKT-Architektur Berlins zukunftsfest zu machen und die Rolle des ITDZ neu zu definieren.
- Verbindliche und durchsetzbare Standards und Schnittstellen für die ganze Verwaltung, solange die Bündelung der Betriebsverantwortung für sicherheitskritische IKT in einer Hand nicht erfolgt ist.
- Die Schaffung einer digitalen Geheimschutzstruktur, die landesweit eine einheitliche und sichere digitale Umgebung für alle als Verschlusssachen behandelten Dokumente umsetzt.
- Die Anschlussfähigkeit der künftigen Architektur an Systeme, die im nationalen oder europäischen Verbund entwickelt wurden, wie die Deutsche Verwaltungscloud, Deutschland- oder Euro-Stack, mit einer klaren Positionierung, welche Komponenten dadurch perspektivisch ersetzt, ergänzt oder eigenständig weiterbetrieben werden sollen.
- Die konsequente Überprüfung und Umsetzung der Regelungen des KRITIS-Dachgesetzes und NIS-2-Richtlinie.

Zusammensetzung der Expert*innengruppe: Der Senat stellt sicher, dass die folgenden Perspektiven in der Expert*innengruppe vertreten sind:

- Die Leitungen bzw. benannten Vertretungen der IT-Stellen der Bezirke, Senatsverwaltungen und Landesämter, der Beschäftigtenvertretung sowie der Landesbeauftragten für Datenschutz und Informationsfreiheit,
- Vertreter*innen von CityLab und ITDZ,
- Externe Sachverständige aus Wissenschaft oder aus anderen Ländern/Kommunen mit erfolgreich umgesetzter IT-Konsolidierung, um Betriebsblindheit vorzubeugen,
- eine Vertretung des IT-Planungsrats bzw. der Bund-Länder-Koordination, insbesondere im Hinblick auf die Deutsche Verwaltungscloud sowie
- die Einbindung zivilgesellschaftlicher Akteur*innen im Bereich der IT-Sicherheit und unabhängiger, wissenschaftlicher Expertise.

Zeitplan: Die Expert*innengruppe wird gebeten

- bis zum **9. November 2026** einen ersten Zwischenbericht mit Bestandsaufnahme, ersten Leitlinien und Arbeitsplan für die weiteren Schritte bzw.
- bis zum **31. Dezember 2026** den finalen Vorschlag zur Überarbeitung der IKT-Architektur vorzulegen.

Berichtspflicht: Der Senat berichtet dem Abgeordnetenhaus zu beiden Terminen über den Stand der Arbeiten und legt den finalen Bericht unmittelbar nach Fertigstellung vor.

Begründung

Im August 2026 wurde die Berliner Verwaltung Opfer des bisher schlimmsten Cyberangriffs ihrer Geschichte. In Anbetracht der globalen sicherheitspolitischen Lage sowie den anstehenden Wahlen im September 2026 bedarf es daher politischer Konsequenzen.

In den Sitzungen des Innen- und des Digitalisierungsausschusses vom 24.08. und 07.09.2026 wurde deutlich, dass der Senat bemüht ist, die Folgen der Netzkompromittierung und der Datenveröffentlichung in den Griff zu bekommen. Bei der Darstellung dieser Bemühungen wurde auch deutlich, dass die systematischen Probleme nicht kurzfristig überwunden werden können. Jedoch ist es dem Senat bisher nicht ansatzweise gelungen, „vor die Lage“ zu kommen. Stattdessen ist das Agieren von Hilflosigkeit geprägt. Die Auswirkungen der mangelhaft organisierten IKT-Steuerung erfordern umso mehr eine ergebnisorientierte, transparente und wahrheitsgetreue Kommunikation, die nicht darauf ausgelegt ist, die Auswirkungen des Cyberangriffs kleinzureden.

In der Sitzung des Digitalausschusses vom Montag, den 07.09. wurde bekannt, dass es auch nach dem Hackerangriff kein Umdenken beim Senat gibt und weiter auf den zähen Weg des OneIT@Berlin bestanden wird. Schlimmer noch, offenbar ist nicht mal die vertragliche Grundlage mit dem ITDZ für die Verantwortungsübernahme abgeschlossen. Dabei hatte die CDO Klement diese bereits zum 01.01.2026 angekündigt. Damit hat der Senat die überfällige Neuordnung der Berliner IKT-Architektur verschleppt, was nicht nur angesichts des Hackerangriffs eine Katastrophe ist.

Hinzu kommt: Der Senat hat bereits im vergangenen Jahr im Einzelplan 25 bei der Digitalisierung den Rotstift angesetzt. Nach dem schwersten Cyberangriff der Berliner Verwaltung wirkt diese Prioritätensetzung umso verantwortungsloser. Wer bei der IT-Infrastruktur spart und gleichzeitig die notwendige Neuordnung der Berliner IKT verschleppt, gefährdet die digitale Handlungsfähigkeit Berlins. CDU und SPD reden ständig von mehr Sicherheit und sicherheitspolitischer Aufrüstung. Gleichzeitig setzt die Politik des Senats bisher auf das Offenhalten von Sicherheitslücken statt auf konsequente Penetrationstests und die Schließung von bekannt gewordenen Schwachstellen. Dabei muss gerade in einer digitalisierten Gesellschaft die kritische Infrastruktur des Landes, die Bevölkerung und die Berliner Verwaltung vor dem Ausnutzen von Sicherheitslücken geschützt werden. Zusammen mit den Kürzungen bei der IT-Sicherheit und der verschleppten Neuordnung der Landes-IT ist das eine gefährliche Ausrichtung. Sicherheit beginnt bei resilienten digitalen Strukturen. Wer dort kürzt, Zuständigkeiten verschleppt und Sicherheitslücken offen lässt, wird selbst zum Sicherheitsrisiko für diese Stadt.

Zum einzuberufenden Expert*innengremium: Mit der Expertise der verschiedenen Expert*innen des nunmehr einzuberufenden Gremiums kann der neuen Regierung ein praxistauglicher Plan mit auf den Weg gegeben werden. Klar ist: Die Betriebsverantwortung für sicherheitskritische IKT muss eindeutig geregelt sein. Solange die künftige Rolle des ITDZ und die Aufgabenverteilung zwischen ITDZ und anderen Akteur*innen nicht geklärt ist, braucht es klare Verantwortlichkeiten. Das Expert*innengremium soll deshalb erarbeiten, wie eine sichere und praxistaugliche Aufgaben- und Verantwortungsverteilung zwischen allen Akteur*innen aussehen kann. Angesichts der aktuellen Bedrohungslage können wir damit jedoch nicht bis zur Konstituierung des neuen Parlaments warten.

Die Erfahrungen mit der Umsetzung des EGovG und der aktuellen Berliner IKT-Landschaft haben deutlich gemacht, dass bei einer Weiterentwicklung auch externe Expertise und neue Ideen Eingang finden sollten. Die breite Beteiligung und externe Begleitung des

Strategieprozesses „Gemeinsam, Digital:Berlin“ können auch für die Operationalisierung dieser Strategie hilfreich sein.

Der Zwischenbericht und die Berichtspflicht sollen sicherstellen, dass Fortschritt messbar und kontrollierbar bleibt, ohne den Zeitdruck angesichts der Bedrohungslage aus den Augen zu verlieren.

Im Übrigen: Aktuell läuft Crowdstrike Falcon – wie jede Virusbekämpfungs- oder Angriffsabwehrsoftware – mit vielen Privilegien auf den IT-Systemen des Berliner Landesnetzes. Hierdurch entstehen auch neue Sicherheitsrisiken. Crowdstrike unterfällt als US Unternehmen dem Cloud-Act und muss notfalls auch Daten von Kund*innen an US-Geheimdienste ausleiten. Es muss sichergestellt werden, dass keine Berliner Verwaltungsdaten in den USA landen oder weitere Sicherheitslücken durch ihren Einsatz entstehen. Der Senat muss eine Risikobewertung des beauftragten US-Unternehmens und der eingesetzten Software vornehmen und veröffentlichen.

Dem Senat sind mittlerweile mindestens die Datenquellen bekannt. Aus diesen muss sich abstrakt-generell ableiten lassen, welche Personengruppen außerhalb der Verwaltung von der Veröffentlichung betroffen sein können. Diese Erkenntnisse müssen veröffentlicht werden.

In den Behörden sind in der Regel viele Unterlagen und Vorgänge, die über die eigene Zuständigkeit hinausgehen. Bisher wurde versichert, dass keine sicherheitsrelevanten Bundesbehörden betroffen sind, weil deren Informationen nicht digital vorhanden seien. Es ist noch unklar, wie es um Informationen anderer Verwaltungen (z.B. Justizgebäude oder Schulbauoffensive) steht. Der Senat muss die betroffenen Verwaltungen umfassend informieren und behörden- und ebenenübergreifend Lösungen für mögliche Gefahren erarbeiten.

Ein besonders großes Risiko stellt der Abfluss sensibler und sicherheitsrelevanter Daten dar. Hier besteht zwar weiterhin kein Gesamtüberblick. Der Cyberangriff hat aber deutlich vor Augen geführt, dass Berlin bisher nicht über eine digitale Geheimschutzstruktur verfügt. Dabei geht es sowohl um Speicherung als auch Kommunikation entsprechend eingestufter Informationen, Notfallpläne für den Katastrophenschutz, Mängellisten kritischer Infrastruktur und Datenbestände im Kontext ziviler Verteidigung. Dabei handelt es sich auch um eine essenzielle und grundsätzliche Struktur zum Schutz sensibler und personenbezogener Daten.

Es ist höchste Zeit die IT-Struktur des Landesnetzes ins digitale Zeitalter zu holen.

Berlin, den 9. September 2026

Jarasch Graf Ziller Ahmadi
und die übrigen Mitglieder der Fraktion
Bündnis 90/Die Grünen

Helm Schulze Schrader
und die übrigen Mitglieder der Fraktion
Die Linke