AfD | Alternative Hauptstadtfraktion

Zuerst Bürger und Mitarbeiter, dann die Systeme, dann die Verantwortung.

Zehn Forderungen nach dem Cyberangriff auf das Berliner Landesnetz

09. September 2026

Positionspapier
der AfD-Fraktion
im Abgeordnetenhaus von Berlin

Seit dem 4. September 2026 liegen rund 1,44 Millionen Dateien aus der Berliner Verwaltung im Darknet. Nach Angaben der Täter und Stichproben der Presse darunter über 5.000 Personalakten, Gehaltsabrechnungen, Atteste, Ausweiskopien, Passwörter im Klartext, rund 80.000 Bußgeldvorgänge, Schwachstellenanalysen zur Trinkwasserversorgung und als Verschlusssache eingestufte Unterlagen. In der Nacht zum 6. September folgte ein zweites Datenpaket mit Zugangsdaten. Die Erpressergruppe Rhysida hatte zuvor 30 Bitcoin verlangt.

Der Senat hat das Abgeordnetenhaus am 24. August falsch informiert. Im Ausschuss für Digitalisierung und Datenschutz erklärte der Chief Digital Officer, es seien nur offene Geodaten abgeflossen, sensible Daten seien „logisch" ausgeschlossen. Am 7. September räumte der Senat im selben Ausschuss ein, dass zu den bekannten Abflüssen keine Protokolldaten vorliegen und von gelöschten Spuren auszugehen ist. Wer keine Protokolle hat, kann nichts „logisch" ausschließen. Die ersten Unstimmigkeiten traten Ende Juli auf, ein Forensik-Unternehmen war da schon beauftragt, der Abfluss lief vom 7. bis zum 12. August, die Netztrennung kam erst am 14. August.

Wir als AfD-Hauptstadtfraktion sagen: Erst die Bürger, dann die Systeme, dann die Verantwortung. Wer heute nicht weiß, ob sein Ausweis, sein Konto oder seine Krankenakte im Netz liegt, braucht eine Nummer, die er anrufen kann, und keine Debatte über Personalfragen. Deshalb stehen die Betroffenen am Anfang dieses Papiers. Danach kommen die Systeme: gesperrte Zugänge, geschützte Verschlußsachen, eine unabhängige Ursachenanalyse und eine Landes-IT, die einen Angriff wie diesen nicht mehr so leicht zulässt. Die Verantwortungsfrage folgt am Ende, und sie folgt zwingend: in der Sondersitzung am 28. September und in einem Untersuchungsausschuss des neuen Abgeordnetenhauses.

AfD-Fraktion im Abgeordnetenhaus von Berlin
Margot-Friedländer-Platz, 10117 Berlin
+49 30 2325 2622 info@afd-fraktion.berlin
afd-fraktion.berlin

WAS DER AUSSCHUSS AM 7. SEPTEMBER ERGAB

Die Präsidentin des BSI: „Die Angreifer hatten es hier immer noch zu leicht." Netzsegmentierung und Zugriffsmanagement seien nicht auf dem nötigen Niveau, das Datenvolumen belege das. Der Staatssekretär der Stadtentwicklungsverwaltung erklärte in derselben Sitzung, Hard- und Software seien aktuell und die BSI-Vorgaben eingehalten.

Einfallstor war eine Täuschung, danach kamen die Angreifer mit Passwörtern voran, die unverschlüsselt in Dokumenten lagen. Nach Angaben von Senat und BSI klickte ein Mitarbeiter auf einen Link in einer Phishing-Mail und führte auf einer gefälschten Sicherheitsabfrage einen Befehl aus (Methode „TerminalFix"). Beschäftigte, darunter Administratoren von Fachverfahren, hatten Zugangsdaten entgegen den Vorschriften im Klartext gespeichert. Diese Dateien sind abgeflossen. Das IT-Dienstleistungszentrum betreibt 21 Verfahren mit fest hinterlegtem Passwort.

Der Vorstand des IT-Dienstleistungszentrums: keine Planung, kein Vertrag, kein Rollout-Plan, keine Finanzierung für die Migration der beiden betroffenen Häuser. Das Security Operations Center werde nur für Lageberichte genutzt, dem Cyber Defense Center sei untersagt worden, fremde Domänen zu untersuchen, die Indikatoren des Angriffs seien erst Anfang September freigegeben und ein Darknet-Monitoring erst am 3. September beauftragt worden.

Der Bezirk Lichtenberg verweigerte die Forensik-Software tagelang, der Senat konnte ihn nicht zwingen. Der Chief Digital Officer nannte das „grob fahrlässig" und sprach von „Gefahr im Verzug", den Bezirk nannte er nicht. Die Kosten der Forensik werden „gesammelt", haushalterische Vorkehrungen für Schadensersatz gibt es nicht. Die 1.650 Beschäftigten der Verkehrsverwaltung sind informiert, die Zahl der externen Betroffenen nennt der Senat „rein spekulativ". Die schriftliche Chronologie ist zugesagt, „so schnell wie möglich", ohne Datum.

AfD-Fraktion im Abgeordnetenhaus von Berlin
Margot-Friedländer-Platz, 10117 Berlin
+49 30 2325 2622 info@afd-fraktion.berlin
afd-fraktion.berlin

UNSERE ZEHN FORDERUNGEN NACH DEM ANGRIFF AUF DAS LANDESNETZ

1. Eine Anlaufstelle für alle Betroffenen, rund um die Uhr

Beschäftigte, Bürger und Unternehmen erhalten sofort eine zentrale Anlaufstelle mit Telefon-Hotline, Webportal und E-Mail. Die Ansprechstelle der Stadtentwicklungsverwaltung erreichte bis zum Wochenende zehn Beschäftigte mit 26 Fragen. Bürger und Unternehmen bekamen bis zum 8. September nur den Rat zur Strafanzeige. Die danach angekündigte Anlaufstelle ist ein E-Mail-Kontakt ohne Termin. **Angekündigt ist nicht eingerichtet.** Jeder muss sicher prüfen können, ob seine Daten im Leak liegen, mit klarer Antwort: betroffen, kein Treffer, Prüfung offen.

2. Jeder Betroffene wird benachrichtigt, ohne Vorauswahl

Der Senat hat seine eigenen Beschäftigten informiert, die Zahl der externen Betroffenen nennt er „rein spekulativ". Wir fordern die individuelle Benachrichtigung aller identifizierten Betroffenen, unabhängig davon, ob im Einzelfall die Schwelle des Artikels 34 der Datenschutz-Grundverordnung erreicht ist. Zuerst kommen Beschäftigte mit Sicherheitsfunktionen und Personen, deren Gesundheits-, Ausweis-, Konto- oder Zugangsdaten offenliegen, danach alle übrigen, die Bürger in 80.000 Bußgeldvorgängen und 46.500 Verträgen eingeschlossen. Bis zum 18. September nennt der Senat die Zahl der Benachrichtigten und den Termin, bis zu dem alle informiert sind.

3. Das Land trägt die Kosten, kein Betroffener zahlt für das Versagen des Senats

Identitätsschutz und Bonitätsüberwachung, Rechtsberatung, die Gebühren für neue Ausweise und Pässe, deren Kopien im Leak liegen, und der Ersatz nachgewiesener Schäden aus Identitätsmissbrauch werden vom Land getragen. Der Chief Digital Officer schließt Schadensersatz nicht aus, haushalterische Vorkehrungen gibt es keine. Antrag über die zentrale Anlaufstelle, Entscheidung binnen vier Wochen, finanziert aus einem eigenen Haushaltstitel und nicht aus dem Kassenkredit des IT-Dienstleistungszentrums.

AfD-Fraktion im Abgeordnetenhaus von Berlin
Margot-Friedländer-Platz, 10117 Berlin
+49 30 2325 2622 info@afd-fraktion.berlin
afd-fraktion.berlin

Beschäftigte beider Häuser erhalten Freistellung für Sperrungen und Behördengänge.

4. Zugänge dicht machen: Passwort-Safe und Mehrfaktor-Authentifizierung – nicht erst in drei Jahren

Alle im Leak enthaltenen Zugangsdaten werden gesperrt und neu vergeben, das zweite Datenpaket vom 6. September eingeschlossen, dazu Sitzungen, Token und Schlüssel. Passwort-Safes werden Pflicht, Klartext-Passwörter in Dokumenten enden. Jeder Fernzugang von Personen erhält bis zum 30. Juni 2027 eine Mehrfaktor-Authentifizierung, nicht erst mit der Zero-Trust-Architektur, die der Landesbeauftragte für Informationssicherheit für Ende 2029 ankündigt. Die 21 Verfahren mit fest hinterlegtem Passwort werden benannt, isoliert oder abgelöst. Für die Wahl-IT bestätigt der Landeswahlleiter vor dem 20. September schriftlich, dass Passwörter und Zertifikate getauscht sind, das BSI konnte das am 7. September nicht sagen.

5. Verschlusssachen raus aus ungeschützten Systemen

Der Senat räumt ein, dass eingestufte Unterlagen elektronisch in einer Verwaltung lagen, die laut eigenem Vermerk keinen digitalen Geheimschutz gewährleisten kann. Auch die niedrigste Stufe VS-NfD ist eine Verschlusssache. Alle Senatsverwaltungen und Bezirke melden bis zum 30. September, wo Verschlusssachen digital abgelegt sind. Die Ablage außerhalb zugelassener Systeme endet sofort. Berlin braucht ein Geheimschutzkonzept für die digitale Verwaltung mit Geheimschutzbeauftragten, die in jeder Senatsverwaltung ein Prüfrecht haben.

6. Lagebericht bis 18. September, danach alle 14 Tage

Der Senat hat am 7. September eine schriftliche Chronologie zugesagt, „so schnell wie möglich", ohne Datum und ohne Ressourcen. Wir setzen das Datum: 18. September, vor der Wahl. Inhalt: Zeitleiste seit Ende Juli, Einfallstor, betroffene Systeme und Daten, Benachrichtigungsstand, Kosten. Fortschreibung alle 14 Tage bis zum Zusammentritt des neuen Abgeordnetenhauses, Sondersitzung am 28. September. Drei Fragen bleiben

AfD-Fraktion im Abgeordnetenhaus von Berlin
Margot-Friedländer-Platz, 10117 Berlin
+49 30 2325 2622 info@afd-fraktion.berlin
afd-fraktion.berlin

offen: Was hat das Forensik-Unternehmen zwischen Ende Juli und dem 14. August untersucht? Warum fehlen die Protokolldaten zu den bekannten Abflüssen? Warum wurde das Darknet-Monitoring erst am 3. September beauftragt?

7. Unabhängige Ursachenanalyse: Die Senatskanzlei kann sich nicht selbst prüfen

Die BSI-Präsidentin sagt, die Angreifer hatten es zu leicht. Der Senat sagt, die BSI-Vorgaben seien eingehalten. Beides zugleich geht nicht. Die technische Ursachenanalyse erfolgt unter Einbindung des BSI, beauftragt sofort, mit Zwischenbericht am 18. September und veröffentlichtem Abschlussbericht bis zum 31. März 2027. Der Rechnungshof von Berlin prüft Steuerung, Beschaffung und Mittelverwendung. Die Berliner Datenschutzbeauftragte wird gebeten, die widersprüchlichen Meldedaten aufzuklären, die Einhaltung der Melde- und Benachrichtigungspflichten zu prüfen und mitzuteilen, wann sie die Löschkonzepte beider Häuser zuletzt geprüft hat, eine Frage, die am 7. September unbeantwortet blieb.

8. Jeden Euro offenlegen: Kostenbericht jeden Monat

Der Senat berichtet dem Hauptausschuss monatlich über die Kosten des Vorfalls in fünf Blöcken: Forensik und Notbetrieb, Wiederaufbau und Härtung, Datenprüfung und Benachrichtigung, Identitätsschutz und Ansprüche Dritter, Vertrags- und Vergabeprüfung. Der Chief Digital Officer erklärte am 7. September, strukturelle Defizite aus früheren Jahren würden zutage treten und Haushaltsmittel erfordern. Ob gestrichene Mittel zu unterlassenen Maßnahmen führten, könne er nicht sagen. Genau das klärt der Bericht: Die zentralen IT-Mittel des Landes sinken laut beschlossenem Haushalt von 320,3 Millionen Euro 2025 auf 285,6 Millionen Euro 2026, der zentrale Titel für Informationssicherheit liegt 2026 mit 14,85 Millionen Euro unter dem Ansatz von 2025. Wir fordern zusätzliche Mittel für Informationssicherheit

AfD-Fraktion im Abgeordnetenhaus von Berlin
Margot-Friedländer-Platz, 10117 Berlin
+49 30 2325 2622 info@afd-fraktion.berlin
afd-fraktion.berlin

mindestens in Höhe der Absenkung, 34,6 Millionen Euro, und einen bezifferten Sofortmaßnahmen- und Personalplan.

9. Landes-IT sanieren statt vertagen

Die Stadtentwicklungs- und die Verkehrsverwaltung betreiben ihre IT bis heute gemeinsam und außerhalb des IT-Dienstleistungszentrums, obwohl das E-Government-Gesetz von 2016 das ITDZ zum Pflichtdienstleister macht. Für die IT-Migration gibt es nach Auskunft des ITDZ-Vorstands weder Planung noch Vertrag noch Finanzierung. Wir fordern die Migration der IT nach einer Sicherheits- und Architekturprüfung mit Termin, Kostenrahmen und eigenem Titel, den Auftrag an Security Operations Center und Cyber Defense Center, alle Domänen des Landes zu überwachen, ein Durchgriffsrecht des Landesbeauftragten für Informationssicherheit gegenüber Bezirken bei Gefahr im Verzug, eine Leitlinie nach aktuellem BSI-Standard anstelle der Fassung von 2017, Löschkonzepte auch für Fileserver und Home-Laufwerke, ein Landes-IT-Sicherheitsgesetz mit Meldepflicht an das Parlament binnen 72 Stunden und einen Chief Digital Officer in Vollzeit mit Weisungsrecht und Digitalbudget.

10. Verantwortung nach Aufklärung: Plenum, Sondersitzungen, Untersuchungsausschuss

Der Senat lenkt die Verantwortung auf Beschäftigte, die Passwörter in Word-Dateien speicherten. Das war ein Verstoß. Die politische Verantwortung trägt, wer über zwei Jahrzehnte ohne Passwort-Safe, ohne Mehrfaktor-Authentifizierung und ohne Segmentierung arbeiten ließ. Es gab „sicher auch Fehlentscheidungen", wie der Staatssekretär der Stadtentwicklungsverwaltung einräumt. Die Steuerung der Landes-IT liegt nach dem E-Government-Gesetz in der Senatskanzlei, der Behörde des Regierenden Bürgermeisters. Personelle Konsequenzen sind unausweichlich, wenn die Aufklärung ergibt, dass Schutzvorgaben bewusst missachtet wurden oder das Parlament wissentlich falsch informiert wurde. Die AfD-Hauptstadtfraktion beantragt in der ersten Sitzungswoche des neuen Abgeordnetenhauses einen Untersuchungsausschuss „IT-Sicherheit des Landes Berlin und Cyberangriff auf das Landesnetz 2026". Der Senat sichert ab sofort alle Unterlagen und Protokolldaten gegen Löschung.

AfD-Fraktion im Abgeordnetenhaus von Berlin
Margot-Friedländer-Platz, 10117 Berlin
+49 30 2325 2622 info@afd-fraktion.berlin
afd-fraktion.berlin

AUFKLÄRUNG ENDET NICHT MIT DER WAHL

Die Aufklärungsforderungen hat unsere Fraktion am 7. September im Ausschuss vorgetragen.
Gewarnt wurde zweimal, 2023 und 2025 im Innenausschuss. Die Leitlinie zur Informationssicherheit stammt von 2017. Der Chief Digital Officer hat am 24. August eingeräumt, dass es keinen genauen Überblick über die Informationstechnik in Berlin gibt. Das ist der Zustand, in dem am 7. August ein Datenabfluss begann, den eine Woche lang niemand bemerkt hat.

Der Untersuchungsausschuss ist das Instrument, mit dem die Aufklärung die Wahl überlebt.
Er klärt die Vorgeschichte seit 2017, den Ablauf zwischen Ende Juli und dem 4. September und die Folgen für Betroffene und Landeshaushalt. Die übrigen Oppositionsfraktionen laden wir zur Mitzeichnung ein.

Die AfD-Hauptstadtfraktion steht dafür ein:
Zuerst Bürger und Mitarbeiter,
dann die Systeme,
dann die Verantwortung.

AfD-Fraktion im Abgeordnetenhaus von Berlin
Margot-Friedländer-Platz, 10117 Berlin
+49 30 2325 2622 info@afd-fraktion.berlin
afd-fraktion.berlin