Abgeordnetenhaus BERLIN

Drucksache 19 / 23 630
Schriftliche Anfrage

19. Wahlperiode

Schriftliche Anfrage

der Abgeordneten Gollaleh Ahmadi (GRÜNE)

vom 19. August 2025 (Eingang beim Abgeordnetenhaus am 20. August 2025)

zum Thema:

Cyberangriffe auf die Berliner Verwaltung – die Justiz im Visier

und **Antwort** vom 4. September 2025 (Eingang beim Abgeordnetenhaus am 5. September 2025)

Senatsverwaltung für Justiz
und Verbraucherschutz

Frau Abgeordnete Gollaleh Ahmadi (Bündnis 90/Die Grünen)
über
die Präsidentin des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

A n t w o r t
auf die Schriftliche Anfrage Nr. 19 / 23 630
vom 19. August 2025
über Cyberangriffe auf die Berliner Verwaltung – die Justiz im Visier
---

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

1. Welche konkreten personenbezogenen Daten sind nach jetzigem Stand vom Angriff betroffen? Bitte legen Sie dar, ob insbesondere folgende Kategorien erfasst wurden, z. B. dienstliche Kommunikation (E-Mails, Kalenderinhalte, Gesprächsnotizen), Daten aus Strafverfahren oder Ermittlungsakten (laufende Verfahren, sensible staatsanwaltschaftliche Vorgänge), Daten zu Gefangenen oder Haftangelegenheiten sowie personalbezogene Daten von Mitarbeiter:innen der Justizverwaltung (Bewerbungsunterlagen, Personalvorgänge, dienstliche Beurteilungen).

Zu 1.: Nach derzeitigem Stand der Untersuchungen beschränkt sich die Datenexfiltration auf den Arbeitsplatzrechner eines Mitarbeitenden aus dem Leitungsbereich der Senatorin. Bei den betroffenen personenbezogenen Daten handelt es sich um Daten der Senatorin und E-Mails nebst Kalendereinträgen von und an Personen, die mit dem Leitungsbereich der Senatorin seit dem 1. Februar 2023 in Kontakt standen. Zudem sind Namen in allgemeinen dienstlichen Schreiben und Vermerken auf exfiltrierten Dokumenten ersichtlich.

Daten aus Straf- und Ermittlungsverfahren, Daten zu Gefangenen oder Haftangelegenheiten und Personalunterlagen sind dem Arbeitsplatzrechner nicht zugänglich gewesen und nach derzeitigem Untersuchungsstand deshalb nicht vom Datenabfluss betroffen.

2. Um welchen konkreten Rechner handelte es sich, das Arbeitsgerät der Senatorin, des Staatssekretärs oder eines Mitarbeiters im Leitungsbereich?

Zu 2.: Nach derzeitigem Untersuchungsstand ist lediglich ein Arbeitsplatzrechner eines Mitarbeitenden des Leitungsbereichs der Senatorin betroffen.

3. Seit wann war der Rechner kompromittiert, über welchen Zeitraum erstreckte sich der unbefugte Zugriff, und wann genau wurde der Angriff erstmals festgestellt?

Zu 3.: Die Aufklärung der genannten Fragestellungen ist Gegenstand laufender Untersuchungen. Belastbare Feststellungen zum Zeitpunkt des Angriffs liegen derzeit nicht vor.

4. Wie genau wurde der Angriff entdeckt, z. B. durch ausbleibende Antwort des vermeintlichen Absenders, interne Sicherheitsmechanismen, externe Hinweise, und wann wurden LKA, ITDZ, CERT und CDC informiert?

Zu 4.: Am 31. Juli 2025 stellte die Senatsverwaltung für Justiz und Verbraucherschutz im Zusammenhang mit einer E-Mail-Korrespondenz Unstimmigkeiten fest, die Zweifel an der Authentizität des Absenders aufkommen ließen. Noch am selben Tag wurde das Landeskriminalamt durch die Senatsverwaltung für Justiz und Verbraucherschutz informiert.

Im Rahmen anschließender interner Überprüfungen der dienstlichen Kommunikation ergaben sich Anhaltspunkte für einen möglichen Cyberangriff. Daraufhin wurde umgehend das IT-Dienstleistungszentrum Berlin (ITDZ) unterrichtet. Zudem wurden durch die Senatsverwaltung und das IT-Dienstleistungszentrum Berlin (ITDZ) unverzüglich weitere zuständige Stellen, darunter das Computer Emergency Response Team (CERT) und das Cyber Defense Center (CDC), in die Abstimmungen einbezogen, und die erforderlichen Sicherheitsmaßnahmen eng koordiniert.

5. Welche konkreten Ursachen sieht der Senat als Gründe für das Eindringen in das System – technische Defizite in der Justiz-IT (fehlende Sicherheitsupdates, Firewalls, E-Mail-Filter), menschliches Fehlverhalten (Klick auf Phishing-Link) oder eine Kombination aus beidem?

Zu 5.: Die Aufklärung der genannten Fragestellung ist Gegenstand laufender Untersuchungen. Belastbare Feststellungen liegen derzeit nicht vor.

6. Welche IT-Sicherheitsprotokolle, Filtermechanismen und Abwehrmaßnahmen waren zum Zeitpunkt des Angriffs implementiert, und warum konnten diese den Angriff nicht verhindern? Wurden dabei die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bzw. einschlägige ISO-Normen eingehalten?

Zu 6.: Es wird auf die Antwort zu Frage 5 verwiesen.

7. Wie bewertet der Senat den Charakter des Angriffs in Bezug auf mögliche politische Motivation?

8. Welche denkbaren Motive jenseits des bloßen Datendiebstahls werden in Betracht gezogen, z. B. Einschüchterung von politischen Entscheidungsträger:innen, gezielte Einflussnahme auf Debatten, Sammlung kompromittierender Informationen, und inwiefern ordnet der Senat den Angriff in den größeren Kontext von Cyberoperationen gegen staatliche Stellen in Deutschland ein?

9. Welche Erkenntnisse liegen der Senatsverwaltung bislang zur mutmaßlichen Täterschaft vor, insbesondere in Bezug auf die Hackergruppe „Charming Kitten“ und deren mögliche Verbindung zu staatlichen Akteuren?

Zu 7-9.: Die strafrechtlichen Ermittlungen zu Motivation, Kontext und Täterschaft dauern noch an und bleiben abzuwarten. Eine abschließende Bewertung ist derzeit nicht möglich.

10.Sind dem Senat in den vergangenen drei Jahren weitere ähnliche Angriffe auf die Berliner Verwaltung oder andere deutsche Behörden bekannt geworden, und wenn ja, wie viele Fälle gab es, in welchen Ressorts oder Bereichen traten sie auf, von welchen Angreifergruppen oder Staaten gingen sie nach derzeitiger Kenntnis aus, und welche konkreten Konsequenzen wurden aus diesen Vorfällen gezogen, um die Berliner Verwaltung besser zu schützen?

Zu 10.: Vergleichbare Cyberangriffe im genannten Zeitraum im Land Berlin sind dem Senat nicht bekannt. Die IKT-Steuerung des Landes Berlin steht – unabhängig von den aktuellen Ereignissen – in einem ständigen Austausch mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

11.Welche Maßnahmen wurden nach der Entdeckung des Angriffs bereits umgesetzt, z. B. Passwortänderungen, Sperrung von Benutzerkonten, forensische Sicherung der betroffenen Daten, Überprüfung weiterer Endgeräte, Sensibilisierung der Mitarbeiter:innen?

Zu 11.: Unmittelbar nach Entdeckung des Angriffs wurden der betroffene Arbeitsplatzrechner sowie vorsorglich weitere Geräte vom Netzwerk getrennt, die Netzwerküberwachung intensiviert und zusätzliche technische Schutzmaßnahmen umgesetzt. Betroffene IT-Systeme wurden für forensische Analysen und strafrechtliche Ermittlungen gesichert, eine forensische Untersuchung wurde beauftragt. Darüber hinaus wurde eine aktualisierte Dienstanweisung zur Sensibilisierung der Mitarbeitenden erlassen; begleitende Informationsveranstaltungen sind in Vorbereitung.

12.Welche zusätzlichen Schritte sind kurzfristig und mittelfristig geplant, um die IT-Sicherheit in der Berliner Justizverwaltung insgesamt zu erhöhen? Wie wird dies im Haushaltsplan abgebildet, und hält der Senat die bisherigen Mittel für ausreichend angesichts der bekannten Gefährdungslage?

Zu 12.: Die Senatsverwaltung für Justiz und Verbraucherschutz setzt die geplante IT-Betriebstransition zum IT-Dienstleistungszentrum Berlin (ITDZ) fort. Ein zentraler Bestandteil ist die Einführung des Berlin-PC, die mit Unterstützung des ITDZ kurzfristig beschleunigt und bereits weiteren Organisationseinheiten bereitgestellt werden konnte. Die flächendeckende Einführung des Berlin-PC in der Senatsverwaltung für Justiz und Verbraucherschutz ist für dieses Jahr vorgesehen. Die hierfür entstehenden Mehrbedarfe im Einzelplan 25 werden derzeit finanziell abgestimmt.

13.Welche Senatsverwaltung ist nach Auffassung des Senats federführend für die Abwehr von Cyberangriffen auf die Berliner Verwaltung zuständig, und wie bewertet der Senat selbst die Angemessenheit dieser Verantwortungszuordnung?

Zu 13.: Die Informationssicherheit für den Sektor öffentliche Verwaltung im Sinne der NIS-2-Richtlinie ist derzeit beim Landesbeauftragten für Informationssicherheit verortet. Grundlage hierfür sind die Regelungen zur Informationssicherheit im E-Governmentgesetz Berlin (EGovG Bln). Im Übrigen ist der Bereich der Cybersicherheit für die 17 weiteren Sektoren im Sinne der NIS-2-Richtlinie bei der Senatsverwaltung für Inneres und Sport angesiedelt. Die Aufteilung der Zuständigkeiten wird im Rahmen der Verwaltungsreform evaluiert.

14.Existieren für Berliner Verwaltungsbehörden standardisierte Notfallpläne bzw. eine einheitliche Verfahrenskette für den Umgang mit Cyberangriffen und politisch motivierten Angriffen aus dem Ausland, und inwiefern wurden diese im aktuellen Fall umgesetzt? Falls keine solchen Notfallpläne existieren, aus welchen Gründen wurde bislang auf deren Erstellung verzichtet?

Zu 14.: Gemäß EGovG Bln sind alle Behörden der Berliner Verwaltung dazu verpflichtet, ein den Vorschriften entsprechendes Informationssicherheitsmanagementsystem (ISMS) nach den Standards des BSI und des IT-Grundschutzkompendiums in der jeweils gültigen Fassung aufzubauen und kontinuierlich weiterzuentwickeln. Dabei sind Festsetzungen zur IKT-Sicherheitsarchitektur und den IKT-Sicherheitsstandards des Landes Berlin einzuhalten. Der Aufbau und die Weiterentwicklung des ISMS erfolgen anhand eines kontinuierlichen ISMS-Prozesses, bei dem regelmäßig die Aktualität und Wirksamkeit der Sicherheitsmaßnahmen überprüft und bei Bedarf angepasst werden. Dazu gehören nach dem BSI-Standard 200-4 unter anderem standardisierte Wiederanlauf- und Wiederherstellungspläne sowie der etablierte Meldeprozess über das Berlin-CERT. Das dezentrale ISMS in den Behörden und Einrichtungen der Berliner Verwaltung ist Bestandteil des landesweiten ISMS.

Im aktuellen Fall wurden die etablierten Meldewege über das Berlin-CERT in Gang gesetzt und ein Krisenstab gebildet.

15.Wurden die Erkenntnisse aus dem Angriff und die eingeleiteten Maßnahmen auch an andere Senatsverwaltungen bzw. Ministerien in Bund und Ländern weitergeleitet, um dort präventive Schutzmaßnahmen zu ermöglichen?

Zu 15.: Durch den etablierten Meldeprozess über das Berlin-CERT wurden landesweit Informationen ausgetauscht.

16.Welche speziellen Maßnahmen sind vorgesehen, um die Sicherheit deutscher Politikerinnen und Staatsbürgerinnen zu gewährleisten, die in das Visier ausländischer Nachrichtendienste kommen könnten?

Zu 16.: Gemäß § 21 Verfassungsschutzgesetz Berlin (VSG) werden bei Vorliegen gefährdungsrelevanter Erkenntnisse des Verfassungsschutzes zu Einzelpersonen oder Institutionen in Berlin, die in den Fokus ausländischer Nachrichtendienste geraten sind, entsprechende Informationen an die Polizei Berlin übermittelt. Die betrifft nicht nur deutsche Politikerinnen und Politiker, sondern auch sonstige deutsche Staatsangehörige.

Das Portfolio von polizeilichen Maßnahmen im Sinne der Fragestellung reicht von gefahrenabwehrrechtlichen bis zu strafprozessualen Instrumenten, die individuell angewandt werden. Weitergehende Details zu konkreten Gefahrenlagen und Einsatzplanungen sind Bestandteil der polizeilichen Einsatztaktik und daher nicht für die Veröffentlichung bestimmt.

17.Welche Empfehlungen spricht der Senat an Berlinerinnen und Berliner mit iranischem Hintergrund aus, die sich öffentlich für Demokratie und Menschenrechte engagieren, um sie vor ähnlichen Angriffen zu schützen, und wenn ja, welche?

Zu 17.: In Bezug auf konkrete Notfall- oder Gefährdungssituationen, Gefährdungssachverhalte oder Verdachtsfälle im Sinne der Fragestellung wird eine Kontaktaufnahme mit der Polizei Berlin empfohlen. Im Falle von konkreten gegenwärtigen Gefährdungssituationen wird auf den Polizeinotruf unter 110 verwiesen. In konkreten Verdachtsfällen nimmt jede Dienststelle der Polizei Berlin Anzeigen entgegen. Diese können auch online über die Internetwache der Polizei Berlin erstattet werden. Bestehen andere Gefährdungssachverhalte, können sich Bürgerinnen und Bürger vertrauensvoll an die Polizeiabschnitte der Polizei Berlin bzw. an den Polizeilichen Staatsschutz des Landeskriminalamts Berlin wenden.
Der Berliner Verfassungsschutz informiert die Öffentlichkeit in seinen jährlichen Verfassungsschutzberichten über geheimdienstliche Aktivitäten fremder Mächte in Berlin, einschließlich solcher Aktivitäten, die sich gegen Dissidenten und Oppositionelle richten (sogenannte Transnationale Repression).

18.Welche Warnungen oder Handlungsempfehlungen von Sicherheitsbehörden, z. B. Bundesamt für Verfassungsschutz, Bundesamt für Sicherheit in der Informationstechnik, zu Cyberangriffen durch ausländische Nachrichtendienste lagen der Berliner Verwaltung vor, und inwiefern wurden diese vor dem aktuellen Vorfall umgesetzt?

Zu 18.: Die von den zuständigen Behörden veröffentlichten Hinweise und Warnungen zu Cyberaktivitäten ausländischer Nachrichtendienste fließen in die Sensibilisierungsmaßnahmen des Berliner Verfassungsschutzes bei gefährdeten Einzelpersonen und Institutionen ein.

Das Berlin-CERT veröffentlicht CERT-Meldungen im Intranet. Die Informationssicherheitsbeauftragten der Behörden der Berliner Landesverwaltung werden auf die Meldungen hingewiesen. Über das vom Berlin-CERT betriebene Warn- und Informationsdienstportal zu Schwachstellen in IKT-Systemen wurden allein im letzten Jahr 4.468 Meldungen bereitgestellt. Zugriff auf dieses Portal haben alle an das Berliner Landesnetzwerk angeschlossenen Stellen. Auf Anfrage werden personalisierte Zugänge hierzu eingerichtet. Damit besteht die Möglichkeit, sich per E-Mail zu Schwachstellen in vorausgewählten Produkten informieren zu lassen. Die im Tagesgeschäft an das Berlin-CERT gestellten Anfragen und deren Beantwortung werden statistisch nicht erfasst. Die Umsetzung der Empfehlungen liegt in der Verantwortung der jeweiligen Institution. Aufgrund der heterogenen Systemlandschaft in den Verwaltungen ist eine Betroffenheit durch die jeweilige Stelle festzustellen und zu bewerten.

Speziell zu den APT-Cyberangriffen empfiehlt das BSI für die Prävention, Detektion und Reaktion eine Reihe von Maßnahmen, die zusätzlich zu den gängigen Basismaßnahmen eingeführt werden sollten. Die dafür bereitgestellten Dokumente verfolgen das Ziel, „Erste Hilfe" bei der Vorfallsbearbeitung zu leisten. Die Aufzählung der relevanten Maßnahmen für die Basis-Sicherheit ist nicht abschließend und soll auch nicht als ganzheitliches Sicherheitskonzept verstanden werden. Dabei ist der DER.2.3 des IT-Grundschutz-Kompendiums des BSI besonders zu beachten und umzusetzen.

19.Wie häufig werden in den Berliner Senatsverwaltungen verpflichtende IT-Sicherheits- und Awareness-Schulungen durchgeführt, einschließlich Phishing-Simulationen, und wurden diese auch im betroffenen Leitungsbereich vor dem Angriff umgesetzt?

Zu 19.: Gemäß der Leitlinie zur Informationssicherheit der Landesverwaltung des Landes Berlin sind alle Mitarbeiterinnen und Mitarbeiter in den Sicherheitsmanagementprozess einzubinden und regelmäßig hinsichtlich der Informationssicherheit zu schulen und zu sensibilisieren. Durch Schulungs- und Sensibilisierungsmaßnahmen wird das Problembewusstsein für IKT-Sicherheit bei den Mitarbeiterinnen und Mitarbeitern der Berliner Verwaltung aufgebaut und kontinuierlich gestärkt. Dies führt langfristig zu einem sicheren digitalen Umgang und trägt dazu bei, das Informationssicherheitsniveau im Land Berlin aufrecht zu erhalten. Mit dieser Zielstellung wurde von der IKT-Steuerung ein landesweites, zielgruppenspezifisches Awareness-Konzept zur Sensibilisierung der Beschäftigten für Informationssicherheit erstellt. Abstimmungen zur Umsetzung erfolgen derzeit mit der Verwaltungsakademie Berlin (VAk). Über die VAk-Plattform sollen künftig Module zur Informationssicherheit angeboten und allen Beschäftigten der Berliner Verwaltung in Form von Selbstlernkursen bereitgestellt werden. Es erfolgt zudem eine gesonderte Sensibilisierung der obersten Managementebene in gesonderter Form.

Die Beschäftigten der Senatsverwaltung für Justiz und Verbraucherschutz werden bereits bei Dienstantritt durch entsprechende Unterlagen zu sicherem Verhalten im digitalen Arbeitsumfeld sensibilisiert. Diese Unterlagen – darunter die Internetdienstanweisung, die Dienstanweisung zum Umgang mit elektronischer Post sowie allgemeine Hinweise zur Informationssicherheit – sind im Intranet hinterlegt und den Beschäftigten in wiederkehrenden Abständen in Erinnerung gerufen. Ergänzend gibt die IT-Stelle der Senatsverwaltung anlassbezogene Hinweise und Empfehlungen zum sicheren Umgang mit digitalen Anwendungen.

Angesichts der zunehmenden Professionalität von Cyberangriffen und der damit verbundenen steigenden Komplexität wird die Senatsverwaltung für Justiz und Verbraucherschutz die vorhandenen Unterlagen fortlaufend kritisch überprüfen und das Sensibilisierungsangebot für die Beschäftigten entsprechend weiterentwickeln.

Berlin, den 4. September 2025

In Vertretung

Dirk Feuerberg
Senatsverwaltung für Justiz
und Verbraucherschutz