Abgeordnetenhaus BERLIN

Drucksache 19 / 25 094
Schriftliche Anfrage

19. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Tommy Tabor (AfD)

vom 2. Februar 2026 (Eingang beim Abgeordnetenhaus am 3. Februar 2026)

zum Thema:

IT-Sicherheits- und Resilienzlage im Bezirk Berlin-Spandau und seinen nachgeordneten Behörden, Einrichtungen und Eigenbetrieben

und **Antwort** vom 17. Februar 2026 (Eingang beim Abgeordnetenhaus am 18. Februar 2026)

Der Regierende Bürgermeister von Berlin
Senatskanzlei

Herrn Abgeordneten Tommy Tabor (AfD)
über
die Präsidentin des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 19/25094
vom 02. Februar 2026
über IT-Sicherheits- und Resilienzlage im Bezirk Berlin-Spandau und seinen nachgeordneten Behörden, Einrichtungen und Eigenbetrieben

---

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

Vorbemerkung der Verwaltung:
Die Schriftliche Anfrage betrifft (zum Teil) Sachverhalte, die der Senat nicht aus eigener Zuständigkeit und Kenntnis beantworten kann. Er ist gleichwohl um eine sachgerechte Antwort bemüht und hat daher das Bezirksamt Spandau um Stellungnahme gebeten, die bei der nachfolgenden Beantwortung berücksichtigt ist.

1. Welche Ämter, Eigenbetriebe, Zweckverbände, Schulen, sozialen Einrichtungen, IT-Dienstleister und ausgelagerten Organisationseinheiten des Bezirks Spandau fallen derzeit unter:
- das IT-Sicherheitsgesetz,
- landesrechtliche IT-Sicherheitsvorgaben des Landes Berlin,
- die NIS-2-Richtlinie (direkt oder mittelbar),
- KRITIS-ähnliche Einstufungen oder Sonderregelungen?

Zu 1.: Der Geltungsbereich des IT-Sicherheitsgesetzes betrifft die Bundesverwaltungen, daher unterliegt das BA-Spandau diesem nicht. Dagegen gelten die Rechtsvorschriften des

Landes Berlin für das Bezirksamt Spandau einschließlich der aufgeführten verbindlich. Unter Verwendung des Identifizierungskonzeptes des BSI wurde das Bezirksamt Spandau als wesentliche Einrichtung im Sinne der NIS-2-Richtlinie bewertet.
KRITIS ähnlichen Einstufungen oder Sonderregelungen bestehen derzeit nicht.

2. Welche Einrichtungen des Bezirks Spandau werden als besonders schutzwürdig oder betriebskritisch eingestuft (z. B. Bürgerdienste, Katastrophenschutz, Gesundheits- oder Ordnungsbereiche)?

Zu 2.: Um keine zusätzlichen Bedrohungsvektoren zu geben, wird zur Risikominimierung hier auf eine Aufstellung der schutzbedürftigen bzw. betriebskritischen Einrichtungen verzichtet.

3. Welche konkreten technischen, organisatorischen und personellen Maßnahmen zur IT-Sicherheit sind im Bezirk Spandau aktuell umgesetzt (z. B. Netzsegmentierung, Backup-Konzepte, Notfallarbeitsplätze, Zero-Trust-Ansätze, SOC-Anbindung)?

Zu 3.: Die durch den BSI IT-Grundschutz geforderten technischen Maßnahmen werden umgesetzt.
Um keine Bedrohungsvektoren zu geben, wird zur Risikominimierung hier auf eine weitere Aufstellung der einzelnen Maßnahmen verzichtet.

4. Existiert für den Bezirk Spandau ein Informationssicherheits-Managementsystem (ISMS)? Falls ja: Nach welchem Standard (z. B. BSI IT-Grundschutz, ISO 27001)? Seit wann ist dieses implementiert? Welche Organisationseinheiten sind vollständig integriert, welche nicht?

Zu 4.: Mit Inkrafttreten des EGovG Bln wurde im Bezirksamt Spandau gemäß § 23 ein Informationssicherheits-Managementsystem-System nach dem BSI-Standard 200-x etabliert.

5. Welche Risiko-, Schwachstellen- oder Penetrationstests wurden in den letzten fünf Jahren durchgeführt? Zu welchen Ergebnissen kam der Bezirk Spandau? Welche Maßnahmen wurden daraus abgeleitet und umgesetzt?

Zu 5.: Schwachstellenscans in der Infrastruktur des Bezirksamts Spandau finden und fanden statt. Um keine Angriffsvektoren zu nennen, wird auf die Nennung konkreter Zeitpunkte wird an dieser Stelle verzichtet. Für die erkannten Schwachstellen wurde ein Realisierungsplan erarbeitet und umgesetzt. Die Wirksamkeit der durchgeführten Maßnahmen wurde mittels eines Wiederholungsscans geprüft und bestätigt.

6. Welche IT-Notfall-, Krisen- und Wiederanlaufpläne bestehen im Bezirk Spandau?

Zu 6.: Für das Bezirksamt Spandau gilt das „IKT-Notfallhandbuch, IT-Sicherheitsvorfall und IT-Notfall“, welches die Anforderungen des BSI-Standards 200-4 umsetzt.

7. In welchen zeitlichen Abständen werden diese Pläne: aktualisiert, getestet (z. B. Übungen, Simulationen), extern oder intern auditiert?

Zu 7.: Das IKT-Notfallhandbuch wird regelmäßig evaluiert und aktualisiert. Darüber hinaus werden Änderungen anlassbezogen vorgenommen.

8. Welche maximalen Wiederanlaufzeiten (RTO) und Datenverlusttoleranzen (RPO) gelten für die wichtigsten Fachverfahren des Bezirks?

Zu 8.: Um keine Bedrohungsvektoren zu geben, wird zur Risikominimierung hier auf eine Aufstellung verzichtet.

9. Wie viele Planstellen und tatsächlich besetzte Stellen sind im Bezirk Spandau explizit für: IT-Sicherheit, Informationssicherheit, Cyber-Resilienz, Notfall- und Krisenmanagement vorgesehen? Bitte aufschlüsseln nach: Besoldungs- bzw. Entgeltgruppen, Vollzeit-/Teilzeitstellen, internen Mitarbeitenden und externen Dienstleistern.

Zu 9.: Die oben genannten Rollen sind gemäß IKT-Rollenkonzept besetzt. Auf eine detaillierte Aufstellung der Besoldungs- bzw. Entgeltgruppen, Vollzeit-/Teilzeitstellen, internen Mitarbeiter und externen Dienstleistern wird an dieser Stelle verzichtet, um keine Angriffsvektoren zu bieten.

10. Welche Qualifikationen, Zertifizierungen oder Schulungsprogramme sind für diese Funktionen vorgeschrieben oder etabliert? Bestehen Personallücken oder Kompetenzdefizite, und falls ja: wie werden diese derzeit kompensiert, welche Maßnahmen zur Personalgewinnung sind geplant?

Zu 10.: Alle Maßnahmen nach BSI 200-x wurden und werden vorgenommen. Auf weitere Ausführungen wird an dieser Stelle verzichtet, um keine Angriffsvektoren zu bieten.

11. Welche Gesamtkosten sind dem Bezirk Spandau in den letzten fünf Haushaltsjahren für: IT-Sicherheit, Cyber-Resilienz, externe Sicherheitsdienstleistungen, Schulungen und Übungen entstanden?

Zu 11.: Dem Bezirksamt Spandau sind keine Kosten in den letzten fünf Haushaltsjahren für die genannten Punkte entstanden. Durchgeführte Awareness-Veranstaltungen wurden zentral durch die Senatskanzlei aus dem Einzelplan 25 finanziert.

12. In welchen Einzelplänen, Titeln und Kapiteln des Berliner Haushalts sind diese Mittel jeweils veranschlagt?

Zu 12.: Grundsätzlich zählen sämtliche Ausgaben zur Erhöhung der IT-Sicherheit sowie hierfür notwendige Schulungen bzw. Awareness-Veranstaltungen zur Maßnahmengruppe 31, da es sich um Ausgaben für die verfahrensunabhängige IKT handelt. Diese sind im Einzelplan 25 der Senatskanzlei veranschlagt.

13. Welche zusätzlichen Mittel sind im aktuellen und in den kommenden Haushaltsjahren explizit für: die Umsetzung der NIS-2-Anforderungen, die Erhöhung der digitalen Resilienz, den Ausbau von Personalstellen vorgesehen?

Zu 13: Es wurden keine zusätzlichen Mittel im Bezirksamt Spandau für die genannten Punkte eingestellt.

14. Welche Landes-, Bundes- oder EU-Fördermittel wurden oder werden hierfür genutzt?

Zu 14.: Die Möglichkeit des Abrufs von Fördermitteln zur Umsetzung der NIS-2-Anforderungen, der Erhöhung der digitalen Resilienz bzw. dem Ausbau von Personalstellen sind dem Bezirksamt Spandau nicht bekannt.

15. Existiert für den Bezirk Spandau ein konkreter Umsetzungs- oder Maßnahmenplan zur vollständigen Erfüllung der aktuellen und absehbaren IT-Sicherheitsanforderungen? Falls ja, bitte Darstellung: der einzelnen Maßnahmen, der verantwortlichen Stellen, der geplanten Meilensteine, der vorgesehenen Fertigstellungstermine.

Zu 15.: Die BSI IT-Grundschutz-Bausteine werden bei entsprechenden Aktualisierungen des IT-Grundschutzkompendiums bzw. bei Änderungen in der IT-Infrastruktur anlassbezogen geprüft.

16. Welche politisch-administrative Stelle trägt die Gesamtverantwortung für IT-Sicherheit im Bezirk Spandau?

Zu 16.: Gemäß BSI-Standard 200-x trägt die Leitungsebene die Gesamtverantwortung für den Informationssicherheitsprozess.

17. Wie erfolgt die Koordination mit Senatsverwaltungen, dem ITDZ Berlin und externen Sicherheitsbehörden?

Zu 17.: Es erfolgt regelmäßiger Austausch mit dem Landesbevollmächtigten für Informationssicherheit des Landes Berlin (Landes-InfSiBe) bei der IKT-Steuerung in der Senatskanzlei. Das Bezirksamt arbeitet zudem eng mit dem Berlin-CERT zusammen und nutzt hier unter anderem die etablierten Meldewege.

18. Welche Berichts- und Kontrollmechanismen bestehen gegenüber dem Abgeordnetenhaus bzw. der Öffentlichkeit?

Zu 18.: Das Abgeordnetenhaus erhält jährlich den Bericht zur Informationssicherheit des Landes Berlin.

Berlin, den 17. Februar 2026

Der Regierende Bürgermeister von Berlin
In Vertretung

Martina Klement
Staatssekretärin für Digitalisierung
und Verwaltungsmodernisierung / CDO