

19. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Stefan Ziller (GRÜNE)

vom 6. Oktober 2026 (Eingang beim Abgeordnetenhaus am 7. Oktober 2026)

zum Thema:

**Ausbringung eines Eindringungserkennungssystems für die Berliner
Verwaltung**

und **Antwort** vom 21. Oktober 2026 (Eingang beim Abgeordnetenhaus am 22. Oktober 2026)

Der Regierende Bürgermeister von Berlin
Senatskanzlei

Herrn Abgeordneten Stefan Ziller (GRÜNE)
über
die Präsidentin des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 19/27250
vom 06.10.2026
über Ausbringung eines Eindringungserkennungssystems für die Berliner Verwaltung

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

1. Welchen Stand hat die Ausbringung eines (flächendeckenden) Eindringungserkennungssystems für die IT der Berliner Verwaltung?

Zu 1.: Die Maßnahmen zur Gefahrenabwehr, im Rahmen des kürzlich stattgefundenen Cyberangriffs auf die IT-Infrastruktur des Landes Berlin, werden durch den Senat weiter konsequent umgesetzt. Um Angreifern keine potentiellen Angriffsvektoren zu bieten, wird auf konkrete Angaben zur Ausbringung des Eindringungserkennungssystems verzichtet.

2. Welche Maßnahmen wurden nach dem Hackerangriff in Sachen Eindringungserkennungssystems in die Wege geleitet und umgesetzt? (Bitte für alle dezentralen IT-Stellen der Senatsverwaltung sowie das ITDZ angeben und unterscheiden, zwischen „in die Wege geleitet“ und „umgesetzt“?)

Zu 2.: In die Aufklärung und Eindämmung des kürzlich erfolgten Cyberangriffs auf die IT-Infrastruktur des Landes Berlin wurden die zuständigen Sicherheitsbehörden, die Berliner Beauftragte für Datenschutz und Informationsfreiheit sowie insgesamt 3 externe Forensikdienstleister eingebunden. Die Dienstleister nahmen die aktive Vorfallsbearbeitung (Incident-Response-Einsatz im 24/7-Betrieb) auf. Der Einsatz umfasste insbesondere forensische Untersuchungen, die Rekonstruktion von Angriffswegen, die Suche nach weiteren

Kompromittierungen, Tor-Netzwerk-Monitoring und die Installation sowie Auswertung von Detektionssensorik. Nach der Phase der akuten Gefahrenabwehr bleiben für die anschließende Absicherung die Überwachung der betroffenen Infrastruktur, die Bewertung sicherheitsrelevanter Ereignisse und die Fähigkeit zur zeitnahen Einleitung von Gegenmaßnahmen maßgeblich. Umfang und Intensität dieser Leistungen richten sich nach dem aktuellen Bereinigungsstand und der fortgeschriebenen technischen Lagebewertung. Um Angreifern keine potentiellen Angriffsvektoren zu bieten, wird auf konkrete Angaben zur Ausbringung des Eindringungserkennungssystems sowie auf eine diesbezüglich detaillierte Aufstellung über die Einleitung und Umsetzung von Maßnahmen in allen Behörden und Einrichtungen des Landes Berlin verzichtet.

Berlin, den 21. Oktober 2026

Der Regierende Bürgermeister von Berlin
In Vertretung

Florian Graf
Chef der Senatskanzlei
für den Staatssekretär für Digitalisierung
und Verwaltungsmodernisierung / CDO (m.d.W.d.G.b.)