19. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Stefan Ziller (GRÜNE)

vom 16. Januar 2025 (Eingang beim Abgeordnetenhaus am 17. Januar 2025)

zum Thema:

IT-Sicherheitsvorfälle in Berlin 2024

und **Antwort** vom 3. Februar 2025 (Eingang beim Abgeordnetenhaus am 5. Februar 2025)

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. 19/21360
vom 16. Januar 2025
über IT-Sicherheitsvorfälle in Berlin 2024

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

1. Wie viele IT-Sicherheitsvorfälle wurden 2024 durch Behörden und Institutionen der Berliner Verwaltung gem. § 23 II EGovGBln oder ggf. anderer Rechtsgrundlagen gemeldet?

Zu 1: Das IT-Dienstleistungszentrum Berlin (ITDZ Berlin) betreibt als zentraler IKT-Dienstleister zur Unterstützung und Beratung der Behörden der Berliner Verwaltung bei sicherheitsrelevanten Vorfällen in IKT-Systemen ein Computersicherheits-Ereignis- und Reaktionsteam (Berlin-CERT). Die an das Berliner Landesnetz angeschlossenen Behörden und Einrichtungen haben dem Berlin-CERT gemäß dem festgelegten Meldeprozess sicherheitsrelevante Vorfälle unverzüglich zu melden. Im Zeitraum vom 01.01.2024 bis 31.12.2024 erfolgten gem. § 23 Abs. 2 EGovG Bln insgesamt 8 Meldungen von Senatsverwaltungen, Landesämtern oder Bezirksämtern an das Berlin-CERT. Darüber hinaus erfolgte keine Meldung von IT-Sicherheitsvorfällen durch Behörden und Institutionen nach anderen Rechtsgrundlagen. Sofern Meldepflichten für IT-Sicherheitsvorfälle im Sinne der NIS2-Richtlinie für den Sektor öffentliche Verwaltung bestehen, sind diese gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) durchzuführen.

2. Wie viele IT-Sicherheitsvorfälle wurden 2024 durch landeseigene Betriebe gem. § 23 II EGovGBln oder ggf. anderer Rechtsgrundlagen gemeldet?

Zu 2.: Im Zeitraum 01.01.2024 bis 31.12.2024 wurden dem Berlin-CERT zwei IT-Sicherheitsvorfälle durch landeseigene Betriebe gem. § 23 Abs. 2 EGovG Bln gemeldet. Darüber hinaus erfolgte keine Meldung von IT-Sicherheitsvorfällen nach anderen Rechtsgrundlagen. Sofern Meldepflichten für landeseigene Betriebe für IT-Sicherheitsvorfälle im Sinne der NIS2-Richtlinie bestehen, sind diese gegenüber dem BSI durchzuführen.

3. Wie viele der gemeldeten IT-Sicherheitsvorfälle wurden auch an die Berliner Beauftragte für Datenschutz und Informationsfreiheit nach § 51 BlnDSG oder ggf. anderer Rechtsgrundlagen gemeldet?

Zu 3.: Seitens des Senats erfolgt keine Erfassung der an die Berliner Beauftragte für Datenschutz und Informationsfreiheit gemeldeten IT-Sicherheitsvorfälle.

4. Wie viele IT-Sicherheitsvorfälle wurden 2024 bekannt, die nicht durch die betroffenen Institutionen oder Unternehmen gemeldet wurden? Welche Konsequenzen hatte ein Ausbleiben von Meldungen?

Zu 4.: Keine.

5. Welche Empfehlungen hat das CERT des ITDZ in 2024 an betroffene Behörden, Institutionen und Unternehmen ausgesprochen? Wie viele der Empfehlungen wurden umgesetzt und in welchem Zeitraum? (Antwort bitte tabellarisch darstellen)

Zu 5.: Das Berlin-CERT hat im Zeitraum 01.01.2024 bis 31.12.2024 insgesamt 122 CERT-Meldungen (Aktualisierungen eingeschlossen, 98 ohne Aktualisierungen) im Intranet veröffentlicht und die Informationssicherheitsbeauftragten der Behörden der Berliner Landesverwaltung auf die Meldungen hingewiesen. Über das vom Berlin-CERT betriebene Warn- und Informationsdienstportal zu Schwachstellen in IKT-Systemen wurden 4.468 Meldungen bereitgestellt. Zugriff auf dieses Portal haben alle an das Berliner Landesnetz angeschlossenen Stellen. Auf Anfrage werden personalisierte Zugänge hierzu eingerichtet, womit die Möglichkeit besteht, sich per E-Mail zu Schwachstellen in vorausgewählten Produkten informieren zu lassen. Die im Tagesgeschäft des Berlin-CERT erhaltenen 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.

Folgende Meldungen sowie Aktualisierungen, Warnungen und Informationen wurden im Jahr 2024 vom Berlin-CERT veröffentlicht:

Datum	Berlin-CERT-Meldung bzw. Aktualisierungen
05.01.2024	CERT-M 2024-01V01 Android Patchday schließt kritische Schwachstellen neueren Versionen
08.01.2024	CERT-M 2024-02V01 Kritische Sicherheitslücke in Ivanti Endpoint Manager
11.01.2024	CERT-M 2024-03V01 Zero Day Schwachstellen bei Cyber Angriffen auf verschiedene Ivanti Produkte genutzt
15.01.2024	CERT-M 2024-04V01 Kritische Sicherheitslücken in GitLab
16.01.2024	CERT-M 2024-03V02 Zero Day Schwachstellen bei Cyber Angriffen auf verschiedene Ivanti Produkte genutzt
17.01.2024	CERT-M 2024-05V01 Schwachstellen Citrix NetScaler ADC Netscaler
19.01.2024	CERT-M 2024-06V01 Kritische Sicherheitslücke in Junipers Junos OS
23.01.2024	CERT-M 2024-07V01 Apple Warnung Schwachstellen in Geräten bedrohen Nutzerdaten
26.01.2024	CERT-M 2024-08V01 Erneut Sicherheitslücken in Junos OS geschlossen
31.01.2024	CERT-M 2024-03V03 Zero-Day-Schwachstellen in Ivanti-Produkten
05.02.2024	CERT-M 2024-09V01 Sicherheitsempfehlungen und Maßnahmen für den Umgang mit Software-Updates in AnyDesk
07.02.2024	CERT-M 2024-10V01 Android Patchday Februar schließt Sicherheitslücken
08.02.2024	CERT-M 2024-11V01 Kritische Schwachstellen in Canon Multifunktions- und Laserdruckern
09.02.2024	CERT-M 2024-03V04 Zero-Day-Schwachstellen in Ivanti-Produkten
09.02.2024	CERT-M 2024-12V01 CERT-M 2024-12V01 Kritische Schwachstellen in FortiOS aktiv ausgenutzt
13.02.2024	CERT-M 2024-12V02 Kritische Schwachstellen in FortiOS aktiv ausgenutzt
14.02.2024	CERT-M 2024-13V01 Kritische Sicherheitslücken in Linux Systemen
14.02.2024	CERT-M 2024-14V01 Kritische Sicherheitslücken in QNAP NAS Betriebssystemen aufgedeckt
15.02.2024	CERT-M 2024-15V01 Adobe Patchday - kritische Schwachstellen in mehreren Produkten
15.02.2024	CERT-M 2024-16V01 Microsoft Patchday Februar verschiedene kritische Sicherheitslücken

15.02.2024	CERT-M 2024-16V02 Microsoft Patchday Februar verschiedene kritische Sicherheitslücken
01.03.2024	CERT-M 2024-03V05 Zero-Day-Schwachstellen in Ivanti-Produkten
05.03.2024	CERT-M 2024-17V01 Apple öffnet mit iOS 17 4 Zugang zu alternativen App Stores
06.03.2024	CERT-M 2024-18V01 Kritische Schwachstellen in Android 12 bis 14 gefixt
06.03.2024	CERT-M 2024-19V01 Wichtige Sicherheitsupdates für iPhone und iPad iOS 17.4 und iOS 16.7.6 veröffentlicht
07.03.2024	CERT-M 2024-20V01 JetBrains schließt Zeroday-Schwachstelle in TeamCity
14.03.2024	CERT-M 2024-21V01 Microsoft Patchday März 2024 kritische Lücken geschlossen
18.03.2024	CERT-M 2024-22V01 Sicherheitslücke im System-BIOS von HP-Produkten geschlossen
21.03.2024	CERT-M 2024-21V02 Microsoft Patchday März 2024 kritische Lücken geschlossen
25.03.2024	CERT-M 2024-21V03 Microsoft Patchday März 2024 kritische Lücken geschlossen
26.03.2024	CERT-M 2024-23V01 Tausende Microsoft Exchange Server in Deutschland verwundbar
26.03.2024	CERT-M 2024-24V01 Wichtige Sicherheitsupdates für iPhone und iPad 17.4.1 und 16.7.7 veröffentlicht
02.04.2024	CERT-M 2024-25V01 kritische Lücke (Hintertür) in XZ für Linux
04.04.2024	CERT-M 2024-25V02 kritische Lücke (Hintertür) in XZ für Linux
05.04.2024	CERT-M 2024-26V01 Adroid Patchday April 2024
05.04.2024	CERT-M 2024-27V01 Sicherheitsupdates für Ivanti Connect Secure und Policy Secure
09.04.2024	CERT-M 2024-28V01 Microsoft Patchday April 2024 Behebung von 150 Sicherheitslücken
12.04.2024	CERT-M 2024-29V01 Palo Alto Networks Firewalls Aktive Ausnutzung einer ungepatchten Schwachstelle
15.04.2024	CERT-M 2024-29V02 Palo Alto Networks Firewalls Aktive Ausnutzung einer ungepatchten Schwachstelle
16.04.2024	CERT-M 2024-30V01 Schwachstelle in PuTTY erlaubt Extraktion von privaten Schlüsseln

17.04.2024	CERT-M 2024-29V03 Palo Alto Networks Firewalls Aktive Ausnutzung einer ungepatchten Schwachstelle
19.04.2024	CERT-M 2024-31V01 Oracle Patchday April 2024 Behebung von 441 Sicherheitslücken
23.04.2024	CERT-M 2024-32V01 Aktiv ausgenutzte Schwachstelle in CrushFTP
23.04.2024	CERT-M 2024-33V01 Firmware-Aktualisierungen für Lexmark-Drucker
25.04.2024	CERT-M 2024-29V04 Palo Alto Networks Firewalls Aktive Ausnutzung einer ungepatchten Schwachstelle
25.04.2024	CERT-M 2024-34V01 Aktiv ausgenutzte Schwachstellen in Cisco ASA geschlossen
29.04.2024	CERT-M 2024-32V02 Aktiv ausgenutzte Schwachstelle in CrushFTP
07.05.2024	CERT-M 2024-35V01 Android Patchday Mai 2024 schließt kritische Lücken
14.05.2024	CERT-M 2024-36V01 Kritische Sicherheitslücken: BSI ruft zur sofortigen Software-Aktualisierung auf
14.05.2024	CERT-M 2024-37V01 Apple veröffentlicht wichtige Sicherheitsupdates
15.05.2024	CERT-M 2024-38V01 Microsoft Patchday Schließung von zwei Zero-Day-Schwachstellen
16.05.2024	CERT-M 2024-38V02 Microsoft Patchday Schließung von zwei Zero-Day-Schwachstellen
16.05.2024	CERT-M 2024-39V01 Adobe Patchday - kritische Schwachstellen in mehreren Produkten geschlossen
17.05.2024	CERT-M 2024-40V01 CERT-M 2024-40V01 Schwachstellen in Trellix ePolicy Orchestrator
24.05.2024	CERT-M 2024-41V01 Kritische Sicherheitslücken in Produkten von Ivanti
27.05.2024	CERT-M 2024-42V01 Keine Eigentore zulassen Warnung vor aktuellen Phishing-Kampagnen
27.05.2024	CERT-M 2024-43V01 Wiederholte Sicherheitslücken Google Chrome erneut von Zero Day Exploit betroffen
03.06.2024	CERT-M 2024-44V01 Check Point meldet kritische VPN Schwachstelle
03.06.2024	CERT-M 2024-45V01 kritische Schwachstelle in vielen Versionen des Linux Kernel
04.06.2024	CERT-M 2024-44V02 Check Point meldet kritische VPN Schwachstelle
05.06.2024	CERT-M 2024-44V03 Check Point meldet kritische VPN Schwachstelle
06.06.2024	CERT-M 2024-46V01 Android Patchday Juni 2024 Aktualisierungen für mehrere Schwachstellen

10.06.2024	CERT-M 2024-47V01 Schwachstelle in Cisco Webex ermöglicht unautorisierten Zugriff auf Metadaten
13.06.2024	CERT-M 2024-48V01 Welle mit fraglichen Bewerbungen für Freiwilligendienste
13.06.2024	CERT-M 2024-49V01 Microsoft Patchday Juni schließt kritische Schwachstelle in Microsoft-Message-Queuing-Service
14.06.2024	CERT-M 2024-50V01 Automatisierte Angriffe gegen Windows-Systeme verteilen Ransomware über PHP-Schwachstelle
18.06.2024	CERT-M 2024-41V02 Kritische Sicherheitslücken in Produkten von Ivanti
26.06.2024	CERT-M 2024-51V01 Ausnutzung kritischer Schwachstelle in MOVEit Transfer von Progress
01.07.2024	CERT-M 2024-51V02 Ausnutzung kritischer Schwachstelle in MOVEit Transfer von Progress
04.07.2024	CERT-M 2024-52V01 Android Patchday Juli 2024 schließt kritische Lücken
12.07.2024	CERT-M 2024-53V01 Patchdays bei Microsoft, Adobe, Citrix und SAP
12.07.2024	CERT-M 2024-54V01 Warnung vor betrügerischen E-Mails zur Änderung von Kontodaten
19.07.2024	CERT-M 2024-55V01 Fehlerhaftes Update von CrowdStrike Falcon
30.07.2024	CERT-M 2024-56V01 Aktiv ausgenutzte Schwachstelle bei Acronis Cyber Infrastructure
30.07.2024	CERT-M 2024-57V01 Sicherheitsmeldung Updates für Apple Produkte
31.07.2024	CERT-M 2024-58V01 Aktive Ransomware-Angriffe auf VMware ESXi-Server
31.07.2024	CERT-M 2024-59V01 Low-Code-Plattform Intrexx - Sicherheitslücke durch Bildverlinkungen
07.08.2024	CERT-M 2024-59V02 Low-Code-Plattform Intrexx - Sicherheitslücke durch Bildverlinkungen
07.08.2024	CERT-M 2024-60V01 Aktiv ausgenutzte Schwachstelle in Android geschlossen
08.08.2024	CERT-M 2024-57V02 Sicherheitsupdates für Apple Produkte
12.08.2024	CERT-M 2024-61V01 Windows Server Angriffe auf Remote Desktop Licensing Service möglich
14.08.2024	CERT-M 2024-62V01 Microsoft Patchday August: Kritische Zero Day Schwachstellen geschlossen

15.08.2024	CERT-M 2024-63V01 Patchdays bei Adobe und SAP schließen teils kritische Lücken
29.08.2024	CERT-M 2024-64V01 Empfehlungen zur Erhöhung der Sicherheit mobiler Endgeräte
05.09.2024	CERT-M 2024-65V01 Android Patchday Google schließt mehrere Schwachstellen
06.09.2024	CERT-M 2024-66V01 Kritische Schwachstelle in SonicOS von SonicWall
12.09.2024	CERT-M 2024-67V01 Microsoft Patchday September schließt ausgenutzte Schwachstellen
12.09.2024	CERT-M 2024-68V01 Schwachstellen in Citrix Workspace App für Windows
13.09.2024	CERT-M 2024-69V01 Adobe Patchday schließt mehrere kritische Sicherheitslücken
18.09.2024	CERT-M 2024-70V01 Apple veröffentlicht neue Betriebssystemversionen und schließt Schwachstellen in bisherigen Versionen
20.09.2024	CERT-M 2024-71V01 Ivanti Cloud Services Appliance - aktive Ausnutzung von Schwachstellen
25.09.2024	CERT-M 2024-59V03 Low-Code-Plattform Intrexx - Sicherheitslücke durch Bildverlinkungen
02.10.2024	CERT-M 2024-72V01 Zimbra - aktive Ausnutzung von Schwachstellen
07.10.2024	CERT-M 2024-41V03 Kritische Sicherheitslücken in Produkten von Ivanti
08.10.2024	CERT-M 2024-73V01 Android Patchday: Google schließt mehrere Schwachstellen
09.10.2024	CERT-M 2024-74V01 Microsoft Patchday Oktober schließt ausgenutzte Schwachstellen
10.10.2024	CERT-M 2024-75V01 SAP Patchday schließt mehrere Schwachstellen
10.10.2024	CERT-M 2024-76V01 Adobe Patchday schließt mehrere Schwachstellen
14.10.2024	CERT-M 2024-77V01 Kritische Schwachstellen bei Juniper Networks, Fortinet und Palo Alto
17.10.2024	CERT-M 2024-54V02 Warnung vor betrügerischen E-Mails zur Änderung von Kontodaten
24.10.2024	CERT-M 2024-78V01 Fortinet FortiManager - aktive Ausnutzung einer Zero-Day Schwachstelle
24.10.2024	CERT-M 2024-79V01 Cisco veröffentlicht kritische Sicherheitsupdates für Firewall-Produkte

29.10.2024	CERT-M 2024-78V02 Fortinet FortiManager - aktive Ausnutzung einer Zero-Day Schwachstelle
31.10.2024	CERT-M 2024-80V01 Apple schließt kritische Sicherheitslücken in iOS iPadOS und macOS
31.10.2024	CERT-M 2024-54V03 Warnung vor betrügerischen E-Mails zur Änderung von Kontodaten
06.11.2024	CERT-M 2024-81V01 Android Patchday Mehrere Schwachstellen ermöglichen u a das Ausführen beliebigen Programmcodes
08.11.2024	CERT-M 2024-82V01 Kritische Sicherheitslücken in Cisco Produkten
13.11.2024	CERT-M 2024-83V01 Sicherheitsupdates für Produkte von Citrix
13.11.2024	CERT-M 2024-84V01 SAP Patchday November behandelt 8 neue Schwachstellen
13.11.2024	CERT-M 2024-85V01 Adobe Patchday November stellt Updates bereit
14.11.2024	CERT-M 2024-86V01 Microsoft Patchday November
14.11.2024	CERT-M 2024-87V01 Sicherheitsupdates für Produkte von Fortinet
15.11.2024	CERT-M 2024-88V01 Palo Alto Networks Firewalls Zero Day Angriffe Management Interface
19.11.2024	CERT-M 2024-88V02 Palo Alto Networks Firewalls Zero Day Angriffe Management Interface
21.11.2024	CERT-M 2024-89V01 Apple schließt zwei Zero Day Sicherheitslücken
22.11.2024	CERT-M 2024-90V01 7-Zip-Lücke ermöglicht Schadcodeausführung
22.11.2024	CERT-M 2024-91V01 Zyxel Firewalls zur Verbreitung von Ransomware missbraucht
04.12.2024	CERT-M 2024-92V01 Android Patchday Dezember
10.12.2024	CERT-M 2024-93V01 Brute-Force-Angriffe auf exponierte Systeme
11.12.2024	CERT-M 2024-94V01 SAP Patchday Dezember behandelt teils kritische Schwachstellen
11.12.2024	CERT-M 2024-95V01 Microsoft Patchday schließt aktiv ausgenutzte Sicherheitslücke
11.12.2024	CERT-M 2024-96V01 Adobe Patchday Dezember behebt mehr als 160 Schwachstellen
12.12.2024	CERT-M 2024-97V01 Apple behebt zahlreiche Schwachstellen in iOS, iPadOS und macOS
17.12.2024	CERT-M 2024-98V01 Der Katalog der aktiv ausgenutzten Schwachstellen (Known Exploited Vulnerabilities)

6. Welche erfolgreichen Angriffe gab es in 2024 auf die Behörden, Institutionen der Berliner Verwaltung und landeseigenen Betriebe und welche Konsequenzen wurden daraus gezogen? (Antwort bitte tabellarisch darstellen)

Zu 6.: Folgende dem Berlin-CERT gemeldeten Sicherheitsvorfälle aus dem Jahr 2024 können als (potentielle) Angriffe gewertet werden:

- Erfolgreicher Phishing-Angriff (2x)
- Interaktion mit maliziöser Mail (2x)

Das Berlin-CERT hat dabei Empfehlungen zur Bewältigung der Vorfälle an die betroffenen Dienststellen ausgesprochen, sofern entsprechende Maßnahmen nicht ohnehin schon durch diese ergriffen worden sind. Die Tätigkeit des Berlin-CERT hat grundsätzlich beratenden, empfehlenden und unterstützenden Charakter. Handlungsempfehlungen werden unter Berücksichtigung der Landesinteressen und der Interessen der dezentralen Behörden im Berlin-CERT abgestimmt. Die Umsetzung und Prüfung von empfohlenen Maßnahmen zählt nicht zu den Aufgaben des Berlin-CERT und verbleibt in der Verantwortung der örtlich zuständigen IT-Sicherheits-/ Verfahrensverantwortlichen und Behördenleitungen.

Berlin, den 03. Februar 2025

Der Regierende Bürgermeister von Berlin
In Vertretung

Martina Klement
Staatssekretärin für Digitalisierung
und Verwaltungsmodernisierung / CDO