Abgeordnetenhaus BERLIN

Drucksache 19 / 17 898
Schriftliche Anfrage

19. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Stefan Ziller (GRÜNE)

vom 18. Januar 2024 (Eingang beim Abgeordnetenhaus am 18. Januar 2024)

zum Thema:

IT-Sicherheitsvorfälle in Berlin 2023

und **Antwort** vom 6. Februar 2024 (Eingang beim Abgeordnetenhaus am 7. Februar 2024)

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. 19/17 898
vom 18. Januar 2024
über IT-Sicherheitsvorfälle in Berlin 2023

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

1. Wie viele IT-Sicherheitsvorfälle wurden 2023 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 Landesnetzwerk angeschlossenen Behörden und Einrichtungen haben dem Berlin-CERT gemäß dem festgelegten Meldeprozess sicherheitsrelevante Vorfälle unverzüglich zu melden. Im Zeitraum vom 01.01.2023 – 31.12.2023 erfolgten gem. § 23 Abs. 2 EGovG Bln insgesamt 15 Meldungen von Senatsverwaltungen, Landesämtern oder Bezirksämtern an das Berlin-CERT. Eine

Meldung von IT-Sicherheitsvorfällen durch Behörden und Institutionen nach anderen Rechtsgrundlagen erfolgte nicht.

2. Wie viele IT-Sicherheitsvorfälle wurden 2023 durch landeseigene Betriebe gem. § 23 II EGovGBln oder ggf. anderer Rechtsgrundlagen gemeldet?

Zu 2.:
Im Zeitraum 01.01.2023 – 31.12.2023 wurden zwei IT-Sicherheitsvorfälle durch landeseigene Betriebe gem. § 23 Abs. 2 EGovG Bln gegenüber dem Berlin-CERT gemeldet. Eine Meldung von IT-Sicherheitsvorfällen durch Behörden und Institutionen nach anderen Rechtsgrundlagen erfolgte nicht.

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. Nach Mitteilung der Berliner Beauftragten für Datenschutz und Informationsfreiheit wurden im Jahr 2023 insgesamt 1.188 Vorgänge angelegt zu Meldungen an die Berliner Beauftragte für Datenschutz und Informationsfreiheit nach Artikel 33 Datenschutzgrundverordnung (DSGVO) zu Verletzungen des Schutzes personenbezogener Daten. Darunter fallen 180 Vorgänge auf Stellen im öffentlichen Bereich (darunter jedoch keine zum Anwendungsbereich des § 51 Berliner Datenschutzgesetz (BlnDSG)) und 1.008 Vorgänge auf nichtöffentliche Stellen.

4. Wie viele IT-Sicherheitsvorfälle wurden 2023 bekannt, die nicht durch die betroffenen Institutionen oder Unternehmen gemeldet wurden? Welche Konsequenzen hatte ein Ausbleiben von Meldungen?

Zu 4.:
In drei Fällen erfolgte eine nachträgliche Meldung zu IT-Sicherheitsvorfällen:

- Die Sicherheitssysteme des ITDZ Berlin lösten einen Alert (technisch basierte Sicherheitsereignisalarmierung) aus, woraufhin das Berlin-CERT Kontakt zur betroffenen Dienststelle aufnahm und über den Vorfall informierte.
- Eine Dienststelle wurde durch den Landesbevollmächtigten für Informationssicherheit zur Meldung eines IT-Sicherheitsvorfalls an das Berlin-CERT aufgefordert.

- Ein Sicherheitsvorfall wurde auf Basis der Hinweise des Berlin-CERT als solcher erkannt, woraufhin die betroffene Behörde umgehend Meldung erstattete.

Die nachträgliche Meldung hatte in allen Fällen keine Konsequenzen von Seiten des Berlin-CERT.

5. Welche Empfehlungen hat das CERT des ITDZ in 2023 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 01.01.2023 – 31.12.2023 insgesamt 89 CERT-Meldungen (Aktualisierungen eingeschlossen, 74 ohne Aktualisierungen) im Intranet veröffentlicht und die Informationssicherheitsbeauftragten der Behörden der Berliner Landesverwaltung auf die Meldungen hingewiesen. Über den vom Berlin-CERT betriebenen Warn- und Informationsdienst zu Schwachstellen in IKT-Systemen wurden 4.024 Meldungen bereitgestellt. Zugriff auf dieses Portal haben alle an das Berliner Landesnetzwerk 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 2023 vom Berlin-CERT veröffentlicht:

Datum	Berlin-CERT-Meldung bzw. Aktualisierungen
11.01.2023	CERT-M_2023-1V01_Patchdays_von_Microsoft_Adobe_SAP_und_Fortinet_schliessen_z_T_kritische_Sicherheitsluecken
16.01.2023	CERT-M_2023-02V01_Kritische_Sicherheitsluecke_in_Control_Web_Panel_wird_aktiv_ausgenutzt
19.01.2023	CERT-M_2023-04V01_Cisco-VPN-Schluesselmaterial_im_Klartext_auslesbar
19.01.2023	CERT-M_2023-03V01_Welle_erpresserischer_Sextortion-Mails
20.01.2023	CERT-M_2023-05V01_Welle_von_Phishing-E-Mails

25.01.2023	CERT-M_2023_06V1 Apple schließt Zero-Day-Sicherheitslücke
26.01.2023	CERT-M_2023-05V02_Welle_von_Phishing-E-Mails
01.02.2023	CERT-M_2023-07V01 Diskussion um die Sicherheit von KeePass
06.02.2023	CERT-M_2023-08V01 Weltweit massive Angriffe auf Schwachstelle in VMware ESXi
07.02.2023	CERT-M_2023-09V01 Business Email Compromise (BEC): eine anhaltende Bedrohung
07.02.2023	CERT-M_2023-08V02_Weltweit_massive_Angriffe_auf_Schwachstelle_in_VMware_ESXi
08.02.2023	CERT-M_2023-08V03_Weltweit_massive_Angriffe_auf_Schwachstelle_in_VMware_ESXi
09.02.2023	CERT-M_2023-07V02 Diskussion um die Sicherheit von KeePass
14.02.2023	CERT-M_2023-10V01 Apple veröffentlicht Patch für aktiv ausgenutzte Schwachstelle in WebKit
15.02.2023	CERT-M_2023-11V01 Microsoft Patch Tuesday: Mehrere kritische Sicherheitslücken geschlossen
16.02.2023	CERT-M_2023-12V01 Cyber-Angriff auf den WISAG-Konzern: Handlungsempfehlungen
20.02.2023	CERT-M_2023-13V01 Intel - Kritische Lücke in BMC-Firmware geschlossen
09.03.2023	CERT-M_2023-0309-14V01_Proof-of-Concept-Code_fuer_kritische_Schwachstelle_in Microsoft_Word_veroeffentlicht
15.03.2023	CERT-M_2023-15V01_Microsoft_Patchday_Aktive_Ausnutzung_einer_Schwachstelle_in_Microsoft_Outlook
30.03.2023	CERT-M_2023-16V01_Cyberangriff auf IT-Dienstleister Materna – Handlungsempfehlungen
31.03.2023	CERT-M_2023-17V01_Apple_schliesst-viele-Sicherheitsluecken_mit_iOS_16-4_und_15-7-4_sowie_iPadOS_16-4_und_15-7-4
03.04.2023	CERT-M_2023-18V01_Telefonie-Software_von_3CX_mit_Schadcode_infiziert
05.04.2023	CERT-M_2023-16V02_Cyberangriff auf IT-Dienstleister Materna – Handlungsempfehlungen
06.04.2023	CERT-M_2023-18V02_Telefonie-Software_von_3CX_mit_Schadcode_infiziert
06.04.2023	CERT-M_2023-19V01_Vergabe neuer Passwörter notwendig wegen Änderungen im Windows Kerberos Protokoll
11.04.2023	CERT-M_2023-17V02_Apple_schliesst-viele-Sicherheitsluecken_mit_iOS_16-4_und_15-7-4_sowie_iPadOS_16-4_und_15-7-4

12.04.2023	CERT-M_2023-20V01 Microsoft Patchday schließt aktiv ausgenutzte Sicherheitslücke
13.04.2023	CERT-M_2023-21V01 Informationssicherheit in der Gebäudeautomation
27.04.2023	CERT-M_2023-22V01 Zero-Day-Schwachstellen in Vmware Workstation und Fusion geschlossen
16.05.2023	CERT-M_2023-23V01_Microsoft_Patchday_Mai_2023
23.05.2023	CERT-M_2023-24V01 Kritische Schwachstellen in Cisco Switches
24.05.2023	CERT-M_2023-25V01_Apple schließt viele Sicherheitslücken mit iOSiPadOS 16.5 und 15.7.6
30.05.2023	CERT-M_2023-26V01_Neue QakBot-(QBot)-Variante E-Mails mit schädlichem PDF-Anhang führen zur Installation von Malware
14.06.2023	CERT-M_2023-27V01_Kritische Schwachstelle in Microsoft SharePoint Server
14.06.2023	CERT-M_2023-28V01_Kritische Schwachstelle mit aktiver Ausnutzung in Fortinet SSL-VPN
23.06.2023	CERT-M_2023-29V01 _Apple beseitigt Zero-Day-Lücken auch in älteren Systemen
12.07.2023	CERT-M_2023-30V01_Aktive_Ausnutzung_einer_Zero-Day-Schwachstelle_in_Microsoft_Office
14.07.2023	CERT-M_2023-31V01_Apple veröffentlicht Patch für schwerwiegende Sicherheitslücke in seiner Browser-Engine WebKit
14.07.2023	CERT-M_2023-32V01_Kritische Schwachstelle mit PoC Exploit in Ghostscript
19.07.2023	CERT-M_2023-30V03_Aktive_Ausnutzung_einer_Zero-Day-Schwachstelle_in_Microsoft_Office
19.07.2023	CERT-M_2023-33V01_Sicherheitslücke in NetScaler ADC von Citrix wird aktiv ausgenutzt
20.07.2023	CERT-M_2023-34V01_Support-Ende für Windows Server 2012 R2
21.07.2023	CERT-M_2023-35V01_Sicherheitsrisiken in großen KI-Sprachmodellen
25.07.2023	CERT-M_2023-36V01_Apple schließt Sicherheitslücken mit Updates für iOS, iPadOS macOS, tvOS und watchOS
25.07.2023	CERT-M_2023-37V01_Zero-Day Schwachstelle in Ivanti Endpoint Manager Mobile geschlossen
31.07.2023	CERT-M_2023-37V02_Zero-Day Schwachstelle in Ivanti Endpoint Manager Mobile geschlossen
09.08.2023	CERT-M_2023-39V01_Microsoft Patchday schließt die Zero-Day-Schwachstelle in Office und weitere Sicherheitslücken
16.08.2023	CERT-M_2023-33V02_Sicherheitslücke in NetScaler ADC von Citrix wird aktiv ausgenutzt
22.08.2023	CERT-M_2023-40V01_Zero-Day Schwachstelle in Ivanti Sentry (MobileIron Sentry)

29.08.2023	CERT-M_2023-41V01_Zwei Sicherheitslücken in 7-Zip ermöglichen die Ausführung beliebigen Codes
30.08.2023	CERT-M_2023-42V01 Exploit für Schwachstellen in Junos OS veröffentlicht
06.09.2023	CERT-M_2023-43V01_Cyberangriffe auf Microsoft-SQL-Server-Datenbanken
08.09.2023	CERT-M_2023-44V01_Sicherheitsupdates_fuer_Zero-Click-Exploit_bei_Apple-Betriebssystemen
11.09.2023	CERT-M_2023-45V01_Android-Patchday_schliesst_mehrere_kritische_Sicherheitsluecken
13.09.2023	CERT-M_2023-46V01_Patchdays_von_Microsoft_Adobe_Mozilla_schliessen_kritische_Sicherheitslücken
20.09.2023	CERT-M_2023-42V02 Exploit für Schwachstellen in Junos OS veröffentlicht
22.09.2023	CERT-M_2023-47V01 Sicherheitsupdates für Betriebssysteme von Apple
29.09.2023	CERT-M_2023-48V01_Mail_Transfer_Agent_Exim_mit_ungepatchten_Schwachstellen
02.10.2023	CERT-M_2023-49V01_Aktive_Ausnutzung_Schwachstelle_WS_FTP
02.10.2023	CERT-M_2023-48V02_Mail_Transfer_Agent_Exim_mit_ungepatchten_Schwachstellen
05.10.2023	CERT-M_2023-50V01_Android_Patchday_schliesst_teilweise_kritische_Schwachstellen
05.10.2023	CERT-M_2023-51V01_Aktiv_ausgenutzte_Schwachstelle_in_Atlassian_Confluence
11.10.2023	CERT-M_2023-51V02_Aktiv_ausgenutzte_Schwachstelle_in_Atlassian_Confluence
11.10.2023	CERT-M_2023-52V02_Zwei_Schwachstellen_ermoeglichen_ua_das_Ausfuehren_beliebigen_Programmcodes
17.10.2023	CERT-M_2023-54V01_Aktive Ausnutzung einer Schwachstelle in Cisco IOS XE
19.10.2023	CERT-M_2023-55V01_Aktive_Ausnutzung_einer_Schwachstelle_in_Citrix_NetScaler_ADC_und_NetScaler_Gateway
23.10.2023	CERT-M_2023-54V03_Aktive Ausnutzung einer Schwachstelle in Cisco IOS XE
25.10.2023	CERT-M_2023-54V04_Aktive Ausnutzung einer Schwachstelle in Cisco IOS XE
26.10.2023	CERT-M_2023-56V01_Kritische_Schwachstellen_in_Squid_Caching_Proxy

26.10.2023	CERT-M_2023-57V01 Sicherheitsupdates für Apple-Betriebssysteme
12.10.2023	CERT-M_2023-53V01_Microsoft_Patchday_Oktober_2023
03.11.2023	CERT-M_2023-58V01_Aktive_Ausnutzung_einer_Schwachstelle_in_Apache_ActiveMQ
03.11.2023	CERT-M_2023-59V01_Aktive_Ausnutzung_von_Schwachstellen_in_F5_BIG-IP
07.11.2023	CERT-M_2023-60V01_Scam-Mails_im_Umlauf
07.11.2023	CERT-M_2023-61V01_Sicherheitslücke in Atlassian Confluence wird aktiv ausgenutzt
08.11.2023	CERT-M_2023-62V01_Android_Patchday_Kritische_Schwachstellen_bedrohen_Android
10.11.2023	CERT-M_2023-61V02_Sicherheitslücke in Atlassian Confluence wird aktiv ausgenutzt
10.11.2023	CERT-M_2023-63V01_Erneut_kritische_Schwachstelle_in WS_FTP_Server
15.11.2023	CERT-M_2023-64V01_Microsoft_Patchday_November_2023
16.11.2023	CERT-M_2023-65V01_Adobe_Patchday_November_2023
23.11.2023	CERT-M_2023-55V02_Aktive_Ausnutzung_einer_Schwachstelle_in_Citrix_NetScaler_ADC_und_NetScaler_Gateway
01.12.2023	CERT-M_2023-66V01_Apple_Sicherheitsupdates
06.12.2023	CERT-M_2023-67V01_Android_Patchday
11.12.2023	CERT-M_2023-68V01_Mehrere_kritische_Sicherheitslücken_in_Atlassian_Software
12.12.2023	CERT-M_2023-66V02_Apple_Sicherheitsupdates
13.12.2023	CERT-M_2023-69V01_weitere_Apple_Sicherheitsupdates
20.12.2023	CERT-M_2023-70V01_Terrapin_Angriffe_können_die_Sicherheit_von_OpenSSH_Verbindungen_beeinträchtigen

6. Welche erfolgreichen Angriffe gab es in 2023 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 2023 können als (potentielle) Angriffe gewertet werden:

- Erfolgreicher Phishing-Angriff (3x)
- Interaktion mit maliziöser Mail (2x)
- Verbindungsversuch mit C2-Server
- Diebstahl dienstliches Notebook

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 CERTs und verbleibt in der Verantwortung der örtlich zuständigen IT-Sicherheits-/ Verfahrensverantwortlichen und Behördenleitungen.

Berlin, den 06. Februar 2024

Der Regierende Bürgermeister von Berlin
In Vertretung

Martina Klement
Staatssekretärin für Digitalisierung
und Verwaltungsmodernisierung / CDO