Abgeordnetenhaus BERLIN

Drucksache 19 / 14 609
Schriftliche Anfrage

19. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Stefan Ziller (GRÜNE)

vom 17. Januar 2023 (Eingang beim Abgeordnetenhaus am 18. Januar 2023)

zum Thema:

IT-Sicherheitsvorfälle in Berlin 2022

und **Antwort** vom 26. Januar 2023 (Eingang beim Abgeordnetenhaus am 27. Januar 2023)

Senatsverwaltung für Inneres, Digitalisierung und Sport

Herrn Abgeordneten Stefan Ziller (GRÜNE)
über
den Präsidenten des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 19/14 609
vom 17. Januar 2023
über IT-Sicherheitsvorfälle in Berlin 2022

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

1. Wie viele IT-Sicherheitsvorfälle wurden 2022 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 01.01.2022 – 31.12.2022 erfolgten gem. § 23 Abs. 2 EGovG Bln insgesamt 14 Meldungen an das Berlin-CERT. Eine Meldung von IT-Sicherheitsvorfällen durch Behörden und Institutionen nach anderen Rechtsgrundlagen erfolgte nicht.

2. Wie viele IT-Sicherheitsvorfälle wurden 2022 durch landeseigene Betriebe gem. § 23 II EGovGBln oder ggf. anderer Rechtsgrundlagen gemeldet?

Zu 2.:

Im Zeitraum 01.01.2022 – 31.12.2022 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 betrug die Anzahl der nach § 51 BlnDSG gemeldeten Verletzungen des Schutzes personenbezogener Daten insgesamt 147.

4. Wie viele IT-Sicherheitsvorfälle wurden 2022 bekannt, die nicht durch die betroffenen Institutionen oder Unternehmen gemeldet wurden? Welche Konsequenzen hatte ein Ausbleiben von Meldungen?

Zu 4.:
Im Rahmen der Bereitstellung von sogenannten Indicators of Compromise durch das Berlin-CERT wurde bei der Prüfung eine Betroffenheit durch eine Institution in der Berliner Landesverwaltung festgestellt und nachträglich in Form einer Sofortmeldung gemeldet. Die nachträgliche Meldung des IT-Sicherheitsvorfalls hatte keine Konsequenzen von Seiten des Berlin-CERT.

5. Welche Empfehlungen hat das CERT des ITDZ in 2022 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 01.01.2022 – 31.12.2022 insgesamt 88 Meldungen im Intranet veröffentlicht und die Informationssicherheitsbeauftragten der Behörden der Berliner Landesverwaltung auf die Meldungen hingewiesen. Die Umsetzung der Empfehlungen liegt in der Verantwortung der jeweiligen Institution. Aufgrund der heterogenen Systemlandschaft in den Verwaltungen ist eine Betroffenheit nur durch die jeweilige Institution festzustellen und zu bewerten. Das entspricht der Vorgehensweise nach den BSI-Standards für das Informationssicherheitsmanagement.

Folgende Meldungen sowie Aktualisierungen, Warnungen und Informationen wurden im Jahr 2022 vom Berlin-CERT veröffentlicht:

Datum	Berlin-CERT-Meldung bzw. Aktualisierung
12.01.2022	CERT-M_2021_62V03_Kritische Log4Shell-Schwachstelle in Java-Bibliothek Log4j
09.02.2022	CERT-M_2022_01V01_Microsofts Patch Tuesday behebt Zero-Day-Lücke
10.02.2022	CERT-M_2022_02V01_SAP schließt mehrere kritische Sicherheitslücken
18.02.2022	CERT-M_2022_03V01_Informationssicherheitshinweise im Kontext der Ukraine-Krise
23.02.2022	CERT-M_2022_04V01_Welle von Phishing E-Mails mit HTML-Anhang
25.02.2022	CERT-M_2022_03V02_Informationssicherheitshinweise im Kontext der Ukraine-Krise
28.02.2022	CERT-M_2022_03V03_Informationssicherheitshinweise im Kontext der Ukraine-Krise
01.03.2022	CERT-M_2022_03V04_Informationssicherheitshinweise im Kontext der Ukraine-Krise
02.03.2022	CERT-M_2022_03V05_Informationssicherheitshinweise im Kontext der Ukraine-Krise
03.03.2022	CERT-M_2022_03V06_Informationssicherheitshinweise im Kontext der Ukraine-Krise
04.03.2022	CERT-M_2022_03V07_Informationssicherheitshinweise im Kontext der Ukraine-Krise
04.03.2022	CERT-M_2021-60V02_BSI-Maßnahmenkatalog zu Ransomware
07.03.2022	CERT-M_2022_03V08_Informationssicherheitshinweise im Kontext der Ukraine-Krise
09.03.2022	CERT-M_2022_03V09_Informationssicherheitshinweise im Kontext der Ukraine-Krise
10.03.2022	CERT-M_2022_05V01_Aktuelle Informationssicherheitshinweise im Kontext der Ukraine-Krise
11.03.2022	CERT-M_2022_06V01_Mehrere kritische Sicherheitslücken
14.03.2022	CERT-M_2022_05V02_Aktuelle Informationssicherheitshinweise im Kontext der Ukraine-Krise
15.03.2022	CERT-M_2022_07V01_Aktuelle Informationssicherheitshinweise im Kontext der Ukraine-Krise
16.03.2022	CERT-M_2022_07V02_Aktuelle Informationssicherheitshinweise im Kontext der Ukraine-Krise
16.03.2022	CERT-M_2022_08V01_Datenabfluss im Falle von Dateiprüfungen bei VirusTotal
16.03.2022	CERT-M_2022_09V01_Massive Phishing-Welle mit Links zu OneDrive
18.03.2022	CERT-M_2022_07V03_Aktuelle Informationssicherheitshinweise im Kontext der Ukraine-Krise

21.03.2022	CERT-M_2022_07V04_Aktuelle Informationssicherheitshinweise im Kontext der Ukraine-Krise
22.03.2022	CERT-M_2022_10V01_Aktuelle Informationssicherheitshinweise im Kontext der Ukraine-Krise
23.03.2022	CERT-M_2022_10V02_Aktuelle Informationssicherheitshinweise im Kontext der Ukraine-Krise
28.03.2022	CERT-M_2022_10V05_Aktuelle Informationssicherheitshinweise im Kontext der Ukraine-Krise
24.03.2022	CERT-M_2022_10V03_Aktuelle Informationssicherheitshinweise im Kontext der Ukraine-Krise
25.03.2022	CERT-M_2022_10V04_Aktuelle Informationssicherheitshinweise im Kontext der Ukraine-Krise
28.03.2022	CERT-M_2022_10V05_Aktuelle Informationssicherheitshinweise im Kontext der Ukraine-Krise
29.03.2022	CERT-M_2022_11V01_Aktuelle Informationssicherheitshinweise im Kontext der Ukraine-Krise
30.03.2022	CERT-M_2022_11V02_Aktuelle Informationssicherheitshinweise im Kontext der Ukraine-Krise
30.03.2022	CERT-M_2022_12V01_Kritische Schwachstellen in APC Smart-USV-Geräten
31.03.2022	CERT-M_2022_11V03_Aktuelle Informationssicherheitshinweise im Kontext der Ukraine-Krise
04.04.2022	CERT-M_2022_11V04_Aktuelle Informationssicherheitshinweise im Kontext der Ukraine-Krise
04.04.2022	CERT-M_2022_13V01_Spring4Shell – Mehrere Sicherheitslücken in Spring
07.04.2022	CERT-M_2022_15V01_Maßnahmen gegen Domain-Missbrauch durch Spam- und Phishing-Akteure
07.04.2022	CERT-M_2022_14V01_Aktuelle Informationssicherheitshinweise im Kontext der Ukraine-Krise
08.04.2022	CERT-M_2022_16V01_Mehrere Schwachstellen in Produkten von FortiNet und Cisco geschlossen
14.04.2022	CERT-M_2022_17V01_Microsoft – Sicherheitsupdates für kritische Zero-Day-Sicherheitslücken die zum Teil bereits aktiv ausgenutzt werden
14.04.2022	CERT-M_2022_18V01_Framework für Angriffe auf ICS- und SCADA-Systeme
21.04.2022	CERT-M_2022_19V01_Oracle Java SE- und OpenJDK-Schwachstelle erlaubt Umgehung von ECDSA-Signaturen
22.04.2022	CERT-M_2022_20V01_Spring4Shell-Schwachstelle in Zutrittskontrollsystemen von Siemens

29.04.2022	CERT-M_2022_20V02_Spring4Shell-Schwachstelle in Zutrittskontrollsystemen von Siemens
06.05.2022	CERT-M_2022_21V01_DDoS-Angriffe durch pro-russische Hacktivisten
10.05.2022	CERT-M_2022-22V01_Kritische_Schwachstellen_in_BIG-IP-Systemen_von_F5
18.05.2022	CERT-M_2022-23V01_Betrügerische Anrufe im Namen verschiedener Polizeibehörden
20.05.2022	CERT-M_2022-24V01_Kombination kritischer Sicherheitslücken erlaubt Übernahme verschiedener VMware-Produkte
31.05.2022	CERT-M_2022_25V01_Zero-Day-Schwachstelle_in_Microsoft_Word_erlaubt_lokale_Code-Ausführung
01.06.2022	CERT-M_2022_25V02_Zero-Day-Schwachstelle_in_Microsoft_Word_erlaubt_lokale_Code-Ausführung
03.06.2022	CERT-M_2022_26V01_Aktive Ausnutzung einer Zeroday-Schwachstelle in Atlassian Confluence
07.06.2022	CERT-M_2022-23V02_Betrügerische Anrufe im Namen verschiedener Polizeibehörden
07.06.2022	CERT-M_2022_26V02_Aktive Ausnutzung einer Zeroday-Schwachstelle in Atlassian Confluence
15.06.2022	CERT-M_2022_27V01_Microsoft-Patchday MSDT-Lücke und weitere Schwachstellen geschlossen
16.06.2022	CERT-M_2022_25V03_Zero-Day-Schwachstelle in Microsoft Word erlaubt lokale Code-Ausführung_
24.06.2022	CERT-M_2022_09V02_Massive Phishing-Welle mit Links zu OneDrive
13.07.2022	CERT-M_2022_28V01_Microsoft-Patchday im Juli behebt 84 Sicherheitslücken
22.07.2022	CERT-M_2022_29V01_Sicherheitsupdates für z. T. kritische Sicherheitslücken in Produkten von Cisco, Oracle und Atlassian
04.08.2022	CERT-M_2022_30V01_VMware schließt mehrere Schwachstellen
10.08.2022	CERT-M_2022_31V01_Microsoft-Patchday im August schließt 121 Sicherheitslücken
19.08.2022	CERT-M_2022_32V01_Zero-Day-Schwachstellen in Apple-Produkten geschlossen
06.09.2022	CERT-M_2022_33V01_Phishing-Mails mit HTM-Anhängen im Umlauf
15.09.2022	CERT-M_2022_34V01_Microsoft-Patchday im September behebt 64 Sicherheitslücken
26.09.2022	CERT-M_2022_36V01_Kritische Schwachstelle in Sophos Firewalls wird aktiv ausgenutzt
28.09.2022	CERT-M_2022-37V01_Gezielte Phishing-Kampagne gegen die Berliner Verwaltung

04.10.2022	CERT-M_2022-38V01_Zwei neue Zero-Day Schwachstellen in Microsoft Exchange Server
05.10.2022	CERT-M_2022-38V02_Zwei neue Zero-Day Schwachstellen in Microsoft Exchange Server
06.10.2022	CERT-M_2022-38V03_Zwei neue Zero-Day Schwachstellen in Microsoft Exchange Server
10.10.2022	CERT-M_2022-39V01_Cyberangriffe auf Zimbra Collaboration Suite
11.10.2022	CERT-M_2022-40V01_Aktuelle_Phishing_Kampagne_mit_dem_Betreff_Beratungsstelle
11.10.2022	CERT-M_2022-41V01 Fortinet-Sicherheitslösungen_-_aktive_Ausnutzung_einer_kritischen_Schwachstelle
12.10.2022	CERT-M_2022-38V04_ Zwei neue Zero-Day Schwachstellen in Microsoft Exchange Server
14.10.2022	CERT-M_2022-42V01_Patchdays_von_Microsoft_Adobe_SAP_und_Fortinet_schliessen_z_T_kritische_Sicherheitsluecken
14.10.2022	CERT-M_2022-39V02_Cyberangriffe_auf_Zimbra_Collaboration_Suite
21.10.2022	CERT-M_2022-43V01_Abmahnschreiben_wegen_Google_Fonts
25.10.2022	CERT-M_2022_09V03_Massive Phishing-Welle mit Links zu OneDrive
31.10.2022	CERT-M_2022-44V01_Kritische Schwachstelle in OpenSSL 3
02.11.2022	CERT-M_2022-44V02_Kritische Schwachstelle in OpenSSL 3
09.11.2022	CERT-M_2022_45V01_Microsoft_Patchday_schliesst_Exchange-Schwachstellen_und_weitere_zT_kritische_Sicherheitsluecken
11.11.2022	CERT-M_2022_46V01_Kritische Schwachstelle in Citrix Gateway und Citrix ADC
24.11.2022	CERT-M_2022-47V01_Umgehung der Malware-Erkennung auf Cisco Secure Email Gateways
14.12.2022	CERT-M_2022-48V01_Aktive_Ausnutzung_einer_Schwachstelle_in_Fortinet_SSL-VPN
14.12.2022	CERT-M_2022-49V01_Zero-Day-Luecke_Citrix_ADC_und_Microsoft_Patchday
15.12.2022	CERT-M_2022-49V02_Zero-Day-Luecke_Citrix_ADC_und_Microsoft_Patchday
15.12.2022	CERT-M_2022-50V01_Apple_schliesst_Zero-Day-Schwachstelle_in_Betriebssystemen
15.12.2022	CERT-M_2022-51V01_VMware_schließt_teils_kritische_Schwachstellen_in_mehreren_Produkten
19.12.2022	CERT-M_2022-52V01_Vorweihnachtliches Phishing
21.12.2022	CERT-M_2022-53V01_Ungepatchte Exchange-Schwachstelle wird aktiv ausgenutzt

22.12.2022	CERT-M_2022-54V01_Spam-/Phishing-Welle mit Anhängen iCalendar-Format

Berlin, den 26. Januar 2023

In Vertretung

Dr. Ralf Kleindiek
Senatsverwaltung für Inneres, Digitalisierung und Sport