Abgeordnetenhaus BERLIN

Drucksache 19 / 10 943
Schriftliche Anfrage

19. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Stefan Ziller (GRÜNE)

vom 09. Februar 2022 (Eingang beim Abgeordnetenhaus am 10. Februar 2022)

zum Thema:
IT-Sicherheitsvorfälle in Berlin 2021

und **Antwort** vom 25. Februar 2022 (Eingang beim Abgeordnetenhaus am 03. März 2022)

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. 19/10 943
vom 09.02.2022
über IT-Sicherheitsvorfälle in Berlin 2021

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

1. Wie viele IT-Sicherheitsvorfälle wurden 2021 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 sicherheitsrelevante Vorfälle unverzüglich zu melden.
Im Zeitraum vom 01.01.2021 – 31.12.2021 erfolgten gem. § 23 Abs. 2 EGovG Bln insgesamt 18 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 2021 durch landeseigene Betriebe gem. § 23 II EGovGBln oder ggf. anderer Rechtsgrundlagen gemeldet?

Zu 2.:
Im Zeitraum 01.01.2021 – 31.12.2021 wurden zwei IT-Sicherheitsvorfälle durch landeseigene Betriebe gem. § 23 Abs. 2 EGovG Bln gegenüber dem Berlin-CERT gemeldet.
Ein IT-Sicherheitsvorfall wurde durch das ITDZ Berlin (Anstalt öffentlichen Rechts) gemeldet. Ein weiterer sicherheitsrelevanter Vorfall wurde bei den Kindertagesstätten Berlin Süd-West (Eigenbetrieb von Berlin) gemeldet. Alle restlichen Meldungen stammten von den Senatsverwaltungen, deren nachgeordneten Behörden oder den Bezirksämtern. 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.:
Es erfolgt keine Erfassung der an die Berliner Beauftragte für Datenschutz und Informationsfreiheit gemeldeten IT-Sicherheitsvorfälle. Die Anzahl der nach § 51 BlnDSG gemeldeten Verletzungen des Schutzes personenbezogener Daten an die Berliner Beauftragte für Datenschutz und Informationsfreiheit betrug insgesamt 137.

4. Wie viele IT-Sicherheitsvorfälle wurden 2021 bekannt, die nicht durch die betroffenen Institutionen oder Unternehmen gemeldet wurden? Welche Konsequenzen hatte ein Ausbleiben von Meldungen?

Zu 4.:
Aufgrund von Hinweisen durch das Berlin-CERT wurden zwei Meldungen durch die betroffenen Institutionen zu IT-Sicherheitsvorfällen nachträglich erstellt, da diese erst durch die gegebenen Hinweise als solche erkannt werden konnten. Die nachträgliche Erstellung hatte keine negativen Auswirkungen und erforderte kein erweitertes Handeln des Berlin-CERT.

5. Welche Empfehlungen hat das CERT des ITDZ in 2021 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 01.01.2021 – 31.12.2021 insgesamt 63 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 und wird vom Berlin-CERT nicht kontrolliert. Aufgrund der heterogenen Systemlandschaft in den Verwaltungen ist eine Betroffenheit nur durch die jeweilige Stelle festzustellen und zu bewerten. Das entspricht der Vorgehensweise nach den BSI-Standards für das Informationssicherheitsmanagement.

Folgende Meldungen sowie Aktualisierungen, Warnungen und Informationen wurden 2021 vom Berlin-CERT veröffentlicht:

Datum	Berlin-CERT-Meldung bzw. Aktualisierung
23.12.2021	Schwachstellen im Active Directory von Microsoft und gefährliche Windows Treiber_CERT-M_2021_63V01
13.12.2021	Kritische Schwachstelle in log4j veröffentlicht_CERT-M_2021_61V04
08.12.2021	BSI-Maßnahmenkatalog zu Ransomware_CERT-M_2021-60V01
02.12.2021	Erneuter Versand von Emotet-Spam_CERT-M_2021-56V02

Datum	Berlin-CERT-Meldung bzw. Aktualisierung
01.12.2021	Schwachstellen in HP Multifunktionsdruckern_CERT-M_2021-59V01
26.11.2021	Schwachstelle im Modul mod_proxy von Apache HTTP-Server_CERT-M_2021-58V01
25.11.2021	Versuchter BEC-Betrug in der Berliner Verwaltung_CERT-M_2021-57_57V01
16.11.2021	DDos-Entwicklungen vor Black Friday und Cyber Monday_CERT-M_2021-55V01
12.11.2021	Kompromittierte Exchange-Server - Zunahme von Angriffen per Mail_CERT-M_2021-54V01
11.11.2021	Schwachstellen in Exchange Server und Excel werden aktiv ausgenutzt_CERT-M_2021_53V01
10.11.2021	Mehrere Schwachstellen im Netzwerkstack Nucleus 13_CERT-M_2021-52V01
02.11.2021	Viele Sicherheitslücken in Nvidia, Cisco-Produkten und Windows_CERT-M_2021-51V01
08.10.2021	Aktualisierung Aktiv ausgenutzte Sicherheitslücken in Apache Webserver_CERT-M_2021-50V02
01.10.2021	Achtung Phishing-Mails mit Bezug zu deutschen Banken_CERT-M_2021-49V01
28.09.2021	Aktualisierung Mehrere kritische Sicherheitslücken in Cisco-Geräten_CERT-M_2021_48V02
27.09.2021	Aktualisierung: Microsoft Exchange Autodiscover legt Windows-Anmeldedaten offen_CERT-M_2021-47V02
23.09.2021	Kritische Schwachstelle in VMware vCenter Standard Server Installation_CERT-M_2021-46V01
14.09.2021	Aktualisierung: Sicherheitslücke in Microsoft Office erlaubt Code-Ausführung aus der Ferne_CERT-M_2021_44V03
10.09.2021	Zeitsprung durch Fehler in GPSd_CERT-M_2021_45V02
03.09.2021	Kritische Schwachstelle in Cisco Enterprise NFV Infrastructure Software_CERT-M_2021_43V01
30.08.2021	Kritische Lücke in Wiki-Software Confluence_CERT-M_2021_42V01
30.08.2021	Sicherheitslücken in Microsoft Azure Cosmos Datenbanken_CERT-M_2021_41V01
27.08.2021	Mehrere Schwachstellen in F5-Produkten_CERT-M_2021_40V01
25.08.2021	Aktualisierung: Razer-Maus ermöglicht Privilegieneskalation in Windows 10 und 11_CERT-M_2021_39V02
23.08.2021	Aktualisierung: Microsoft Exchange Server Lücken werden aktiv ausgenutzt_CERT-M_2021_36V02
19.08.2021	Sicherheitslücke in Fortinet FortiWeb OS_CERT-M_2021-38V01
18.08.2021	Sicherheitslücke in BlackBerry QNX-Produkten_CERT-M_2021-

Datum	Berlin-CERT-Meldung bzw. Aktualisierung
	37V01
18.08.2021	INFRA HALT - Mehrere Schwachstellen im NicheStack Aktualisierung_CERT-M_2021_35V02
28.07.2021	Smartphones weltweit von Pegasus überwacht_CERT-M_2021_34V01
26.07.2021	Neue Angriffsmethode PetitPotam macht Windows Netze für Relay-Angriff verwundbar_CERT-M_2021_33V01
14.07.2021	Zeroday-Schwachstelle in SolarWinds Serv-U FTP Software_CERT-M_2021_32V01
13.07.2021	Kaseya - Angriff durch Supply-Chain-Attacke mit REvil-Ransomware trifft hunderte Unternehmen_CERT-M_2021_30V03
13.07.2021	SMS-Spam mit Schadsoftware_CERT-M_2021_31V01
07.07.2021	Kritische Schwachstelle in Druckerspooler auf Microsoft Systemen_CERT-M_2021_29V03
01.07.2021	Bezahlterminals über NFC manipulierbar_CERT-M_2021_28V01
29.06.2021	Anhaltend erhöhtes Aufkommen von Phishing E-Mails mit Schadsoftware Qakbot_CERT-M_2021_21V02
23.06.2021	Update SonicWall Network Security Appliance Pufferüberlauf-Schwachstelle_CERT-M_2021_27V01
09.06.2021	Aktive Attacken auf Windows-Sicherheitslücken_CERT-M_2021_26V01
03.06.2021	Ransomware_Kampagne nimmt VMware ESXi Server ins Visier_CERT-M_2021_25V01
18.05.2021	Sicherheitslücken in Windows IIS_CERT-M_2021_24V01
14.05.2021	FragAttacks - Neue WLAN-Schwachstellen [Update]_CERT-M_2021_23V02
12.05.2021	FragAttacks - Neue WLAN-Schwachstellen_CERT-M_2021_23V01
05.05.2021	Erhöhtes Aufkommen von Qakbot Phishing E-Mails_CERT-M_2021_21V01
06.05.2021	Schwachstellen in Exim bedrohen Unix-Mailserver_CERT-M_2021_22V01
22.04.2021	Zero-Day-Schwachstelle in SonicWall Email Security Appliance_CERT-M_2021_20V01
21.04.2021	Remote-Code-Schwachstelle in PulseConnect Secure SSL-VPN-Gateway_CERT-M_2021_19V01
20.04.2021	Schwachstelle NAMEWRECK betrifft mehrere DNS-Implementierungen_CERT-M_2021_18V01
16.04.2021	Angriffsaktivitäten gegen Netzwerkgeräte der Firma Cisco Systems Inc._CERT-M_2021_17V01
14.04.2021	Neue Schwachstellen in Microsoft Exchange Server_CERT-

Datum	Berlin-CERT-Meldung bzw. Aktualisierung
	M_2021_16V01
23.03.2021	Kritische Schwachstellen der BIG-IP /BIG-IQ Produkte von F5_CERT-M_2021_15V01
23.03.2021	Aktuelle Ransomware-Angriffskampagne CERT-M_2021_14V01
19.03.2021	SMS SPAM mit Link zur Installation von Schadsoftware_CERT-M_2021_13V01
19.03.2021	Ransomware DearCry nutzt aktuelle Sicherheitslücke in Exchange Server CERT-M_2021_12V01
18.03.2021	Mehrere Schwachstellen in MS Exchange_CERT-M_2021_10V10
17.03.2021	MS Exchange Detektion und Reaktion_CERT-M_2021_10V09
12.03.2021	MS Exchange Detektion und Reaktion_CERT-M_2021_10V08
11.03.2021	Webinar Microsoft Exchange-Schwachstellen und aktuelle Lage_CERT-M_2021_11V02
10.03.2021	MS Exchange Detektion und Reaktion_CERT-M_2021_10V07
10.03.2021	Mehrere Schwachstellen in MS Exchange_CERT-M_2021_10V06
09.03.2021	MS Exchange Detektion und Reaktion_CERT-M_2021_10V05
09.03.2021	Mehrere Schwachstellen in MS Exchange_CERT-M_2021_10V04
09.03.2021	Webinar Microsoft Exchange-Schwachstellen und aktuelle Lage_CERT-M_2021_11V01
05.03.2021	Mehrere Schwachstellen in MS Exchange_CERT-M_2021_10V03
04.03.2021	Mehrere Schwachstellen in MS Exchange_CERT-M_2021_10V02
03.03.2021	Mehrere Schwachstellen in MS Exchange_CERT-M_2021_10V01
03.03.2021	Potenzieller Missbrauch der Domain labo-berlin.de_CERT-M_2021_09V02
02.03.2021	Achtung Malware Dridex_CERT-M_2021_08V01
01.03.2021	VMware vCenter Server Plugin mit kritischer RCE-Schwachstelle_CERT-M_2021_07V01
22.02.2021	0-day Schwachstelle in SonicWallSecure Mobile Access Version 10.x_CERT-M_2021_04V06
18.02.2021	Angehängte Microsoft-Office Dateien mit eingebetteten Objekten werden durch Text ersetzt_CERT-M_2021_06V01
09.02.2021	Microsoft-Patchday im Februar_CERT-M_2021_05V01
05.02.2021	Supply-Chain-Angriff über manipulierte SolarWinds Orion Software_CERT-M_2020_55V03
04.02.2021	0-day Schwachstelle in SonicWallSecure Mobile Access Version 10.x_CERT-M_2021_04V04
02.02.2021	0-day Schwachstelle in SonicWallSecure Mobile Access Version 10.x_CERT-M_2021_04V03
29.01.2021	0-day Schwachstelle in SonicWallSecure Mobile Access Version 10.x_CERT-M_2021_04V02

Datum	Berlin-CERT-Meldung bzw. Aktualisierung
29.01.2021	0-day Schwachstelle in SonicWallSecure Mobile Access Version 10.x_CERT-M_2021_04V01
26.01.2021	Achtung: Phishing E-Mails in Verbindung zu NextCloud_CERT-M_2021_03V01
25.01.2021	Veröffentlichung eines Exploit-Codes für die kritische Schwachstelle in SAPSolution Manager_CERT-M_2021_02V01
21.01.2021	Achtung Betrüger geben sich am Telefon als Mitarbeiter von Microsoft aus_CERT-M_2021_01V01

Berlin, den 25. Februar 2022

In Vertretung

Dr. Ralf Kleindiek
Senatsverwaltung für Inneres, Digitalisierung und Sport