

18. Wahlperiode

Schriftliche Anfrage

des Abgeordneten **Stefan Ziller (GRÜNE)**

vom 28. Januar 2021 (Eingang beim Abgeordnetenhaus am 28. Januar 2021)

zum Thema:

IT-Sicherheitsvorfälle in Berlin 2020

und **Antwort** vom 08. Februar 2021 (Eingang beim Abgeordnetenhaus am 10. Feb. 2021)

Senatsverwaltung für Inneres und Sport

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

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 18 / 26378
vom 28. Januar 2021
über IT-Sicherheitsvorfälle in Berlin 2020

Der Senat ist sich des Stellenwerts des Fragerechts der Abgeordneten bewusst und die Beantwortung Schriftlicher Anfragen der Mitglieder des Abgeordnetenhauses nach Artikel 45 Absatz 1 der Verfassung von Berlin hat stets eine sehr hohe Priorität. Gegenwärtig konzentriert der Senat seine Arbeit und seinen Ressourceneinsatz aber auf die Bekämpfung der infektionsschutzrechtlichen Gefährdungslage für die Berliner Bevölkerung und setzt die zwischen Bund und Ländern verabredeten Maßnahmen zur Reduzierung von Kontakten um. Vor diesem Hintergrund beantworte ich Ihre Schriftliche Anfrage im Namen des Senats von Berlin wie folgt:

1. Wie viele IT-Sicherheitsvorfälle wurden 2020 durch Behörden und Institutionen der Berliner Verwaltung gem. § 23 II EGovGBln oder ggf. anderer Rechtsgrundlagen gemeldet?

Zu 1.:

In den Behörden und Institutionen sind die Prozesse zum Informationsmanagement, die auch die Behandlung von relevanten Ereignissen zur Informationssicherheit beinhalten, etabliert. Gemäß dem festgesetzten Meldeprozess übermitteln die Behörden und Institutionen halbjährlich dem CERT Vorfälle, die lokal in eigener Verantwortung bearbeitet wurden. Diese Meldungen sind im jährlichen Bericht zur Informationssicherheit enthalten. Für 2020 liegen die Angaben noch nicht vor, weil pandemiebedingt Verzögerungen festzustellen sind. Tendenziell überwiegen entsprechend dem Anstieg entsprechender CERT-Meldungen weiterhin technisch bedingte Sicherheitsereignisse (Schwachstellen) gegenüber nutzungsbedingten Ereignissen, da der Eintritt letzterer im Wege der Abwehr von Spam mittels E-Mail-Filterung und Abwehr von Verbindungen zu Bot-Netzen entgegengewirkt wird. Bei der Zählung der Abwehrmaßnahmen ist ein Anstieg vergleichbar der vom BSI veröffentlichten Cybersicherheitslage zu verzeichnen.

Ereignisse mit dem Verdacht von behördenübergreifender Wirkung sind sofort zu melden. Von Behörden und Institutionen der Berliner Verwaltung wurden gem. § 23 Abs. 2 EGovG Bln 20 Sofort-Meldungen zu IKT-Sicherheitsvorfällen im Zeitraum vom 01. Januar 2020 bis 31. Dezember 2020 gegenüber dem Berlin-CERT gemeldet.

2. Wie viele IT-Sicherheitsvorfälle wurden 2020 durch landeseigene Betriebe gem. § 23 II EGovGBln oder ggf. anderer Rechtsgrundlagen gemeldet?

Zu 2.:

Im Zeitraum 01. Januar 2020 bis 31. Dezember 2020 wurden keine IKT-Sicherheitsvorfälle durch landeseigene Betriebe gem. § 23 Abs. 2 EGovG Bln gegenüber dem Berlin-CERT gemeldet.

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.

4. Wie viele IT-Sicherheitsvorfälle wurden 2020 bekannt, die nicht durch die betroffenen Institutionen oder Unternehmen gemeldet wurden? Welche Konsequenzen hatte ein Ausbleiben von Meldungen?

Zu 4.:

Dem Berlin-CERT sind keine IKT-Sicherheitsvorfälle mit behördenübergreifenden Ausmaß bekannt, die nicht gemeldet wurden. Für den Fall, dass Hinweise zu IKT-Sicherheitsvorfällen durch andere Stellen an das Berlin-CERT erfolgen, werden die Institutionen gebeten, unverzüglich eine Sofort-Meldung für einen IKT-Sicherheitsvorfall an das Berlin-CERT zu übermitteln.

5. Welche Empfehlungen hat das CERT des ITDZ in 2020 an betroffene Behörden, Institutionen und Unternehmen ausgesprochen? Wie viele der Empfehlungen wurden umgesetzt und in welchem Zeitraum? (Antwort bitte tabellarisch darstellen)

Zu 5.:

Alle Empfehlungen und Warnhinweise des Berlin-CERT, sowie Meldungen und Hinweise des BSI werden im Landesbeschäftigtenportal der Berliner Verwaltung veröffentlicht. Neben den Veröffentlichungen werden zusätzlich über den durch das Berlin-CERT bereitgestellten Warn- und Informationsdienst zu bekannten Schwachstellen z.B. in Produkten der Firma Microsoft, in verschiedenen Linux-Distributionen oder Firmwareversionen unterschiedlichster Hardwarekomponenten informiert. Der Warn- und Informationsdienst ist für jede Behörde im Intranet der Berliner Verwaltung nutzbar.

Im Landesbeschäftigtenportal wurden in 2020 insgesamt 56 Meldungen und Hinweise veröffentlicht.

Im Warn- und Informationsdienst wurden in 2020 über 2950 Schwachstellen informiert.

Die Umsetzung der Empfehlungen kann durch das Berlin-CERT aufgrund der Heterogenität der Systemlandschaft in der Berliner Landesverwaltung nicht durchgehend überwacht werden. Bei Empfehlungen, die auch durch die IKT-Sicherheit bei SenInnDS als umzusetzende Maßnahmen für alle an des Berliner Landesnetzes angeschlossenen Einrichtungen vorgegeben werden, wird die Umsetzung durch das Berlin-CERT beobachtet.

Umsetzungen, die durch das ITDZ Berlin als Betreiber zentraler Komponenten oder Dienste, die unter anderem für die Sicherheit des Berliner Landesnetzes zuständig sind, werden dem Berlin-CERT gemeldet.

Berlin, den 08. Februar 2021

In Vertretung

Sabine Smentek
Senatsverwaltung für Inneres und Sport