Abgeordnetenhaus BERLIN

Drucksache 18 / 28 131
Schriftliche Anfrage

18. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Sebastian Schlüsselburg (LINKE)

vom 09. Juli 2021 (Eingang beim Abgeordnetenhaus am 09. Juli 2021)

zum Thema:

Cyber-Angriffe auf das Land Berlin seit 2016

und **Antwort** vom 23. Juli 2021 (Eingang beim Abgeordnetenhaus am 27. Juli 2021)

Die Drucksachen des Abgeordnetenhauses sind bei der Kulturbuch-Verlag GmbH zu beziehen.
Hausanschrift: Sprosserweg 3, 12351 Berlin-Buckow · Postanschrift: Postfach 47 04 49, 12313 Berlin, Telefon: 6 61 84 84; Telefax: 6 61 78 28.

Senatsverwaltung für Inneres und Sport

Herrn Abgeordneten Sebastian Schlüsselburg (LINKE)
über
den Präsidenten des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 18/28131
vom 09.07.2021
über Cyber-Angriffe auf das Land Berlin seit 2016

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

1. Wie viele Angriffe durch welche Schadprogramme und welche übrigen Gefahren für die Kommunikationstechnik (sog. Cyberangriffe) auf das Land Berlin gab es seit dem 1.1.2016 (bitte aufschlüsseln nach Jahren sowie a) Hauptverwaltungen einschl. nachgeordneter Bereiche, b) Bezirksverwaltungen, c) der Anstalten BSR, BVG, BWB, d) der öffentlichen Universitäten und Hochschulen des Landes Berlin einschließlich der Charité, e) bei Vivantes sowie f) sämtlichen jeweils einzeln aufzuschlüsselnden vom Land Berlin beherrschten Unternehmen und g) sämtlichen vom Land Berlin beherrschten Stiftungen)?

Zu 1. a und b:
Jährlich wird ein vertraulicher Bericht zur Informationssicherheit vom Senat erstellt und in einer Mitteilung zur Kenntnisnahme an das Abgeordnetenhaus übermittelt. In diesem jährlichen erfassten Bericht werden im Kapitel zum Berliner Computer-Ereignis-Reaktions-Team (Berlin-CERT) die Anzahl der Angriffe aufgelistet. Zusätzlich liegt dem Bericht ebenfalls der vertrauliche Jahresbericht des CERT Berlin bei, der die wesentlichen Volumina der Angriffe nach Behörden aufschlüsselt. Darüberhinausgehende Informationen zu den unter 1c bis 1g genannten Institutionen liegen nicht vor. Durch das EGovG Bln wird nur den Stellen nach 1a und 1b eine Meldepflicht auferlegt.

2. In welchen der vorgenannten Angriffsfälle wurde insbesondere versucht, jeweils welche kritische Infrastruktur des Landes anzugreifen?

Zu 2.:
Auf Basis der Aufzeichnungen der erkannten Angriffsversuche ist die Feststellung eines gezielten Angriffs auf eine spezielle und/oder bestimmte Infrastruktur oder Infrastrukturkomponente nicht möglich. Die erkannten Ereignisse wurden im vom ITDZ Berlin betriebenen Berliner Landesnetz detektiert. Eine Anschlussverpflichtung an das Berliner Landesnetz besteht für die Stellen nach 1a und 1b. Stellen, welche unter den Anwendungsbereich der KRITIS Verordnung fallen, haben eine Berichtspflicht gegenüber dem BSI.

3. Wie viele dieser Angriffe konnten durch welche zuständige Stelle rechtzeitig erkannt und abgewehrt werden (Aufschlüsselung bitte analog zu Frage 1)?

Zu 3.:
Hierzu liegen dem Senat keine dedizierten Informationen vor. Der jährliche Bericht zur Informationssicherheit gibt einen Überblick über die statistischen Gesamtmeldungen zu Sicherheitsvorfällen aus den zu 1a und 1b gehörenden Behörden. Danach konnten alle Angriffe erfolgreich erkannt und abgewehrt werden. Ausnahmen bilden die auch öffentlich bekannten Vorfälle beim Berliner Kammergericht und der TU Berlin. Darüber hinausgehende Informationen zu den unter 1c bis 1g genannten Institutionen liegen nicht vor.

4. Bei wie vielen dieser Angriffe ist es jeweils ggf. zu welchen Teilerfolgen und jeweils welchen Schäden in welcher Gesamtsumme gekommen (Aufschlüsselung bitte analog zu Frage 1)?

Zu 4.:
Einen Aufschluss über die Anzahl der erfolgreichen Angriffe gibt der jährliche Bericht zur Informationssicherheit. Eine systematische Erfassung der Schadenshöhe erfolgt nicht, wäre aber auch aufgrund zusätzlicher Anpassungen im Rahmen der Wiederinbetriebnahme der Systeme nicht aussagekräftig. Darüber hinausgehende Informationen zu den unter 1c bis 1g genannten Institutionen liegen nicht vor.

5. Bei wie vielen dieser Angriffe ist es jeweils zu Datenabflüssen welcher Art und welchen Umfanges gekommen (Aufschlüsselung bitte analog zu Frage 1)?

Zu 5.:
Hierzu liegen dem Senat keine Informationen vor.

6. Bei wie vielen der unter 1. genannten Angriffe konnten die Angreifer:innen ermittelt werden, um wen handelte es sich und welche Strafverfolgungsmaßnahmen mit jeweils welchen Erledigungen und ggf. Verurteilungen zu welchen Geld- oder Freiheitsstrafen wurden eingeleitet?

Zu 6.:
Hierzu liegen dem Senat keine Informationen vor.

7. In welchen der unter 1. genannten Angriffsfälle wurden wie oft Daten an
   a) das Bundesamt für Sicherheit in der Informationstechnik (BSI),
   b) die Strafverfolgungsbehörden zur Verfolgung einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100a Absatz 2 der Strafprozessordnung bezeichneten Straftat,
   c) an die Polizeien des Bundes und der Länder,
   d) an die Verfassungsschutzbehörden des Bundes und der Länder sowie an den Militärischen Abschirmdienst sowie
   e) an den Bundesnachrichtendienst übermittelt?

Zu 7.:
Hierzu liegen dem Senat im Detail keine Informationen vor. Im Land Berlin sind jedoch Meldeprozesse etabliert und umgesetzt. Entsprechend werden bei Vorfällen die notwendigen Einrichtungen informiert. Dies zeigt auch der jährliche Bericht zur Informationssicherheit im Rahmen der Auswertung der bestehenden Meldeprozesse.

8. Welche kassenwirksamen Investitionen aus dem Landeshaushalt oder mit welchen anderen öffentlichen Mitteln wurden seit dem 1.1.2016 zur Verbesserung der IT-Sicherheit in welchen der unter 1. genannten Organisationseinheiten getätigt (bitte zusätzlich aufschlüsseln nach Jahren)?

Zu 8.:
Ausgaben der landesweiten IKT-Steuerung im Bereich Informationssicherheit (Senatsverwaltung für Inneres und Sport):

Jahr	Summe in T€
2016	411,00
2017	411,00
2018	1.379,00
2019	1.249,78
2020	7.108,20

Für kassenwirksame Investitionen bzw. Ausgaben aus dem Landeshaushalt, die über die Informationssicherheit der IKT-Steuerung hinausgehen, liegen dem Senat keine konsolidierten Informationen für die unter 1. genannten Organisationseinheiten vor.

9. Was sind nach Auffassung des Senats die aktuell relevanten Gefahrenquellen und Trends bei den sogenannten Cyberangriffen?

Zu 9.:
Angriffe erfolgen nach dem aktuellen Trend überwiegend durch Phishing-Mails, Social Engineering (Erschleichen von vertraulichen Informationen wie Zugangsdaten) oder dem Ausnutzen von sogenannten Zero-Day-Exploits, d.h. bisher nicht aufgedeckten oder bislang unbekannten Schwachstellen. Hauptzielsetzung ist die Verschlüsselung aller Systeme und das vorherige teilweise Kopieren von Daten unter Einsatz sog. Ransomware, um anschließend eine Geldforderung zu stellen.

10. Wie bewertet der Senat die aktuelle IT-Sicherheitsarchitektur des Landes Berlin sowie der unter 1. genannten Organisationseinheiten und welche weiteren Pläne zur Verbesserung der IT-Sicherheit plant er?

Zu 10.:
Der vertrauliche jährliche Bericht zu Informationssicherheit, der dem Abgeordnetenhaus vorliegt, gibt detailliert Aufschluss über den aktuellen Zustand der Informationssicherheit der einzelnen im Bericht erfassten Behörden des Landes Berlin. Darüberhinausgehende Informationen zu den unter 1c bis 1g genannten Institutionen liegen nicht vor.

Berlin, den 23. Juli 2021

In Vertretung

Aleksander Dzembritzki
Senatsverwaltung für Inneres und Sport