In der Senatssitzung am 13. Februar 2024 beschlossene Fassung

Die Senatorin für Gesundheit, Frauen und Verbraucherschutz

Bremen, 11.02.2024

L 10

Tischvorlage für die Sitzung des Senats am 13.02.2024

„Cyber-Angriffe im Bremer Gesundheitswesen“

(Anfrage für die Fragestunde der Bremischen Bürgerschaft (Landtag))

A. Problem

Die Fraktion der FDP hat für die Fragestunde der Bürgerschaft (Landtag) folgende Anfrage an den Senat gestellt:

1. Von wie vielen Cyber-Angriffen auf Einrichtungen des Gesundheitswesens im Land Bremen hat der Senat in den letzten fünf Jahren jeweils Kenntnis erhalten?
2. Inwiefern unterstützt der Senat die Einrichtungen des Gesundheitswesens bei der Prävention vor Cyber-Attacken und welche Hilfestellungen bzw. Maßnahmen wurden in den vergangen fünf Jahren konkret umgesetzt?
3. Inwiefern hat sich nach Auffassung des Senats die Gefährdung für Einrichtungen des Gesundheitswesens Opfer von Cyber-Angriffen zu werden in den vergangenen fünf Jahren verändert, und welche Handlungsbedarfe werden für die Zukunft gesehen?

B. Lösung

Auf die vorgenannte Anfrage wird dem Senat folgende Antwort vorgeschlagen:

Zu Frage 1:

Im Ressort der Senatorin für Gesundheit, Frauen und Verbraucherschutz einschließlich aller zugeordneter Dienststellen (Gesundheitsamt Bremen, Lebensmittelüberwachungs-, Tierschutz- und Veterinärdienst, Gewerbeaufsicht des Landes Bremens, Eichamt des Landes Bremens und Landesuntersuchungsamt für Chemie, Hygiene und Veterinärmedizin) gab es in den letzten 5 Jahren keinen erfolgreichen Cyber-Angriff.

Die Kliniken berichten, dass die IT-Systeme der Kliniken täglich Angriffen unterschiedlicher Trageweite ausgesetzt sind, diese jedoch in der Regel von den IT-Sicherheitssystemen abgefangen werden. Da nicht erfolgreiche Cyber-Angriffe meist unerkannt bleiben, ist es in der Regel nicht möglich die Zahl der möglichen Angriffe zu beziffern.

Aus den vergangenen fünf Jahren sind dem Senat zwei Cyber-Angriffe auf Kliniken bekannt:

1. Im Januar 2020: Citrix-Netscaler kompromittiert, dabei handelte es sich um einen weltweiten Angriff. Eine Schwachstelle in den Produkten Netscaler ADC und Gateway des Softwareunternehmens Citrix wurde von Angreifern ausgenutzt.
2. Im Mai 2023: Der Einbruch in die IT-Infrastruktur einer Klinik und Datendiebstahl.

Laut des betroffenen Klinikbetreibers, der Gesundheit Nord - Klinikverbund Bremen, wurden beide Vorfälle den zuständigen Behörden gemeldet.

Zu Frage 2:

Bei der Beantwortung dieser Frage ist zu unterscheiden zwischen Dataport angeschlossenen Dienststellen sowie Einrichtungen, die nicht an Dataport gebunden sind.

Zu den Dataport angeschlossenen Dienststellen gehört das Ressort der Senatorin für Gesundheit, Frauen und Verbraucherschutz einschließlich aller zugeordneten Dienststellen. Der Senator Finanzen hat in seinem Geschäftsbereich die Verantwortung für zentrale Informations- und Kommunikationsinfrastrukturen der öffentlichen Verwaltung Bremens. In diesem Kontext und entlang des einschlägigen IT-Planungsratsbeschlusses aus 2013 wurde beim zentralen IT-Dienstleister Dataport ein „Computer Emergency Response Team“ (CERT) eingerichtet. Die öffentliche Verwaltung Bremens ist über die „Leitlinie für Informationssicherheit“ verpflichtet, Sicherheitsvorfälle an das CERT zu melden. Diese Organisationen sind im IT-Verbund Bremens integriert und über den zentralen IT-Dienstleister im Hinblick auf Prävention, Detektion und Reaktion involviert. Insbesondere sind in den vergangenen Jahren die Reaktionsfähigkeiten und die Systeme zur Angriffserkennung (SzA) weiter ausgebaut worden. Beim IT-Dienstleister wurde hierfür das „Security Operation Center“ (SOC) personell aufgebaut, was zusammen mit dem CERT als „Cyber Defense Center“ (CDC) unter einer Abteilungsleitung wirkt. Sofern es zu gravierenden Sicherheitsvorfällen kam, was für die benannten Organisationen nicht zutraf, sind Prozesse zur Abarbeitung bis hin zur Eskalation aufgesetzt.

Nicht an Dataport gebunden sind die Krankenhäuser. Laut Auskunft der Kliniken erfolgen von den Krankenhäusern im Land Bremen eine Vielzahl an Maßnahmen zur Prävention von Cyberangriffen, dazu gehören u.a.: der Einsatz von IT-Sicherheitssystemen mit einer leistungsfähigen, mehrstufigen Sicherheitsinfrastruktur, Informations- und Schulungskonzepte, um die Awareness und Sensibilität aller Anwender:innen zu erhöhen, regelmäßige externe Penetrationstests, die Segmentierung der IT Netzwerke, um sicherzustellen, dass bei einem Angriff nur ein kleiner Bereich der IT betroffen ist, die Beschränkung der Zugriffe von Beschäftigten von außen per VPN sowie Partnerschaften in der Allianz für Cybersicherheit.

Übergreifend für alle Dienststellen und Einrichtungen im Land Bremen hat der Senat im April 2023 die Bremische Cybersicherheitsstrategie verabschiedet. Die Bremische Cybersicherheitsstrategie enthält insgesamt neun Handlungsfelder, in denen Maßnahmen zur Stärkung der Cyberresilienz im Land Bremen beschrieben sind. Als eine erste Maßnahme wurde im Mai 2023 die Zentralstelle Cybersicherheit beim Senator für Inneres und Sport eingerichtet. Perspektivisch soll diese u.a. durch die Koordinierung und Vernetzung der unterschiedlichen Akteure im Feld der Cybersicherheit, die Cyberresilienz im Land Bremen steigern.

Zu Frage 3:

Das Risiko, Opfer von Cyberangriffen zu werden, ist innerhalb der letzten fünf Jahre für Einrichtungen im Gesundheitswesen genauso wie auch für andere Einrichtungen deutlich gestiegen. So melden z.B. die Kliniken zurück, dass Cyber-Angriffe nach Schätzungen um das bis zu 20–30-fache zugenommen haben.

Die Angriffsversuche – beispielsweises durch fingierte E-Mails – wurden in den letzten Jahren immer professioneller. Es ist schwer, die genaue Entwicklung von Cyberangriffen zu antizipieren, allerdings ist davon auszugehen, dass insbesondere die voranschreitende Digitalisierung

und die zu erwartenden Entwicklungen im Bereich der künstlichen Intelligenz, Handlungsbedarfe im Zusammenhang mit Cyberangriffen auf Gesundheitseinrichtungen auslösen werden. So kann Künstliche Intelligenz z.B. durch Cyberkriminelle benutzt, aber Künstliche Intelligenz kann z.B. auch dafür eingesetzt werden, Netze und Informationstechnische Einrichtungen besser auf Anomalien zu überwachen und so Cyberangriffe frühzeitig zu detektieren und zu verhindern.

Generell ist das Risiko, Opfer von Cyberangriffen zu werden, sehr hoch, es ist nicht zu erkennen, dass speziell Gesundheitseinrichtungen gezielt angegriffen werden.

Die Gewährleistung der Cyber- und Informationssicherheit sind für den Senat und die öffentliche Verwaltung elementare Tätigkeitsbereiche der Daseinsvorsorge.

Bund und Länder sind miteinander vernetzt und tragen zum deutschen Lagebild bei. Die Freie Hansestadt Bremen ist über den Verwaltungs-CERT-Verbund (VCV) mit dem Bund und den Ländern inhaltlich und zur Abwehr von Gefahren für die öffentliche Verwaltung vernetzt. Bedrohungsvektoren werden technikunterstützt zwischen den Teilnehmenden ausgetauscht und verifiziert.

Wie schon zu Frage 2 ausgeführt, hat der Senat zudem im April 2023 die Bremische Cybersicherheitsstrategie zwecks Aufbau einer Bremen-weiten Cybersicherheitsarchitektur verabschiedet.

C. Alternativen

Werden nicht vorgeschlagen.

D. Finanzielle, personalwirtschaftliche und genderbezogene Auswirkungen

Die Beantwortung der Anfrage hat keine finanziellen oder personalwirtschaftlichen Auswirkungen. Frauen und Männer sind von den Cyberangriffen gleichermaßen betroffen.

E. Beteiligung und Abstimmung

Die Vorlage ist mit dem Senator für Inneres und Sport und dem Senator für Finanzen abgestimmt.

F. Öffentlichkeitsarbeit und Veröffentlichung nach dem Informationsfreiheitsgesetz

Einer Veröffentlichung über das zentrale elektronische Informationsregister steht nichts entgegen.

G. Beschluss

Der Senat stimmt entsprechend der Vorlage der Senatorin für Gesundheit, Frauen und Verbraucherschutz vom 11.02.2024 der mündlichen Antwort auf die Anfrage der Fraktion der FDP für die Fragestunde der Bremischen Bürgerschaft (Landtag) zu.