BREMISCHE BÜRGERSCHAFT **Drucksache 21/1093**
Landtag (zu Drs. 21/1008)
21. Wahlperiode 25.03.2025

Mitteilung des Senats vom 25. März 2025

Bremer Behörden mit Spammails lahmgelegt – Was ist über den Botnet-Angriff vom 17. Dezember 2024 bekannt?

Die Fraktion der CDU hat unter Drucksache 21/1008 eine Kleine Anfrage zu obigem Thema an den Senat gerichtet.

Der Senat beantwortet die vorgenannte Kleine Anfrage wie folgt:

Kenntnisstand und Ablauf des Angriffs

1. Wann genau hat der der zentrale IT-Dienstleister Dataport und wann genau hat der Senat erstmals Kenntnis vom Angriff auf die Formulare und Postfächer Bremer Behörden vom 17. Dezember 2024 erlangt?

   Die Kompetenzstelle CMS und Internet (KOGIS) beim Senator für Finanzen wurde am Morgen des 17. Dezember 2024 durch mehrere betroffene Stellen über ein erhöhtes Spam-Aufkommen informiert. Eine erste Meldung erfolgte durch die IT-Fachabteilung der Polizei Bremen um 07:10 Uhr an KOGIS. Aufgrund dieser Hinweise wurde seitens KOGIS durch die zuständigen Mitarbeiter:innen eine erste Überprüfung dieser Feststellung eingeleitet. Da der massenhafte Versand von Spammails keinerlei Beeinträchtigungen auf den Servern zur Folge hatte, konnte der Angriff nicht sofort eindeutig mittels Log-Dateien identifiziert werden.

   Teilweise hatten die betroffenen Stellen parallel hierzu bereits Störungstickets beim zentralen IT-Dienstleister Dataport eröffnet und sich telefonisch und per Mail an das Computer Emergency Response Team (CERT Nord) gewendet. Gleichzeitig erging eine Meldung an das CERT Nord durch das Zentrale Informationssicherheitsmanagement (ISM) beim Senator für Finanzen.

2. Über welche Indikatoren wurde der Angriff entdeckt (zum Beispiel auffällige Serverlast, interne Meldungen, Security-Monitoring)? Inwiefern gab es im Vorfeld konkrete Bedrohungshinweise und, wenn ja, von wem an wen?

Es konnte festgestellt werden, dass die E-Mails über die (Kontakt-) Formulare der KOGIS-Webseiten versendet wurden. Die hohe Anzahl an Anfragen über das Kontaktformular an sich stellte keine auffällige Serverlast für die bremischen Systeme dar. Die Feststellungen in den betroffenen Ressorts beziehungsweise Dienststellen erfolgten durch die für die Verwaltung der betroffenen Funktionspostfächer zuständigen Sachbearbeiter:innen. Nach Kenntnis des Senats lagen im Vorfeld lagen keine konkreten Bedrohungshinweise vor.

3. Welche Fachressorts, Einrichtungen, Systeme und Funktionen waren konkret davon betroffen und in welchem Umfang (zum Beispiel Anzahl betroffener E-Mail-Postfächer, Kontaktformulare)?

   Nach Kenntnis des Senats waren die folgenden Ressorts beziehungsweise Dienststellen betroffen:

   — Die Senatorin für Bau,Mobilität und Stadtentwicklung,

   — Die Senatorin für Gesundheit, Frauen und Verbraucherschutz,

   — Die Senatorin für Umwelt, Klima und Wissenschaft,

   — Die Senatorin für Arbeit, Soziales, Jugend und Integration

   — das Amt für Versorgung und Integration (AVIB),

   — die Polizei Bremen,

   — die Zentrale Antikorruptionsstelle Bremen (ZAKS),

   — der Teilhabebeirat Bremen.

   Betroffen waren jeweils das Kontaktformular sowie ein (Funktions-) Postfach der oben genannten Stellen.

   Nach Auswertung der vorliegenden Informationen wurde festgestellt, dass der massenhafte Spamversand am 16. Dezember 2024 gegen 22:00 Uhr mit dem Versand von bis circa 300 E-Mails pro Stunde (zusammengerechnet für alle Webseiten betroffener Stellen) begann. In der Spitze des Spamversands wurden bis zu 4 500 E-Mails pro Stunde an die betroffenen Postfächer versandt. Durch das Deaktivieren der betroffenen Formulare sank die Zahl der eingehenden E-Mails am 17. Dezember 2024 auf etwa 2 800 pro Stunde (zusammengerechnet für alle Webseiten betroffener Stellen) ab. Die eingeleiteten Abschwächungsmaßnahmen („Mitigation“) führten dazu, dass die Zahl der eingehenden Spammails kontinuierlich sank. Sie lag am 18. Dezember 2024 noch bei zusammen circa 800 E-Mails pro Stunde. Am 19. Dezember 2024 wurden die Mitigationsmaßnahmen abgeschlossen und die Rate der festgestellten Spamails sank wieder auf den Normalwert vor dem Vorfall.

4. Wie lange dauerte der Angriff und die Schadensbehebung? Wann waren alle Systeme wieder sicher und in vollem Umfang funktionsfähig?

   Nach Kenntnis des Senats dauerte der Angriff insgesamt vier Tage an (16. Dezember 2024 bis 19. Dezember 2024).

   Als Sofortmaßnahme wurden am 17. Dezember 2024 zunächst die betroffenen Kontaktformulare auf Empfehlung der Kompetenzstelle CMS und Internet durch die Ressortansprechpersonen deaktiviert. Dies führte unmittelbar zu einer deutlichen Verbesserung der Situation. Hiernach wurden die eingehenden Spamails auf vorliegende Gemeinsamkeiten analysiert. Die gewonnenen Erkenntnisse wurden genutzt, um die Spammails automatisiert zu filtern und zu löschen, was zu einer weiteren Verbesserung der Situation am 18. Dezember 2024 führte. In der Nacht vom 18. Dezember 2024 auf den 19. Dezember 2024 wurde das Angriffsmuster durch die Angreifer verändert, um weiterhin Spammails versenden zu können. Diese Änderung des Angriffsmusters wurde am Morgen des 19. Dezember 2024 identifiziert und die eingeleiteten Mitigationsmaßnahmen angepasst. Im Laufe des 19. Dezember 2024 wurden weitere Maßnahmen ergriffen, um die Kontaktformulare mittelfristig zu schützen. Die Umsetzung langfristiger Schutzmaßnahmen ist aktuell Gegenstand weiterer Prüfungen (vergleiche hierzu die Antwort zu Frage 12).

   Weitere IT-Systeme waren durch den Spam-Versand nicht beeinträchtigt. Die Websites der betroffenen Stellen und alle zugehörigen Funktionen liefen zu jedem Zeitpunkt stabil.

Schadensausmaß und Folgen

5. Welche konkreten Auswirkungen hatten die Angriffe auf den Betriebsablauf in den betroffenen Behörden (zum Beispiel verzögerte Bearbeitungen, zeitweilige Ausfälle, eingeschränkte Erreichbarkeit)?

   Nach Kenntnis des Senats kam es durch den massenhaften Spam-Versand nicht zu wesentlichen Beeinflussungen der Betriebsabläufe in den betroffenen Stellen. Einzig das Sichten und Sortieren der im betroffenen Zeitraum eingegangenen E-Mails hatte bei einzelnen betroffenen Stellen einen kurzfristigen Arbeitsmehraufwand zur Folge.

6. Inwiefern mussten neben dem Abschalten der Kontaktformulare weitere Systeme heruntergefahren oder geschützt werden? Wenn ja, welche?

   Es waren keine weiteren IT-Systeme betroffen.

7. Welche Schäden (zum Beispiel Sachschäden oder sonstige wirtschaftliche Schäden) hat der Angriff bei wem verursacht?

Nach Kenntnis des Senats sind keine Schäden verursacht worden. Es kam zu einer zeitweisen Einschränkung der Verfügbarkeit durch das Abschalten der Kontaktformulare.

8. Inwiefern kam es bei dem Angriff zu einem Datenverlust oder Datendiebstahl? Wurden personenbezogene Daten (zum Beispiel aus Formularen) oder andere sensible Informationen kompromittiert?

   Es kam zu keinem Datenverlust. Es wurden keinerlei Daten kompromittiert.

9. Welche davon betroffenen Personen und Institutionen wurden wann informiert?

   Da es nicht zu einem Datenverlust oder einer Kompromittierung von Daten kam, mussten keine Personen oder Institutionen informiert werden.

IT-Sicherheitsmaßnahmen

10. Welche präventiven Maßnahmen waren vor dem Vorfall in Kraft (zum Beispiel Firewall- und Spam-Filter-Systeme, Intrusion-Detection-Systeme), und inwiefern haben diese wie erwartet funktioniert?

    Zum Schutz der IT-Systeme werden umfangreiche präventive Maßnahmen betrieben. Um zu verhindern, dass diese Maßnahmen umgangen werden, kann eine einzelne Auflistung dieser Schutzsysteme und der entsprechenden Funktionsweise nicht öffentlich gemacht werden. Die in Betrieb befindlichen Maßnahmen funktionierten auch am 17. Dezember 2024 erwartungsgemäß. Trotz des erhöhten Mail-Aufkommens funktionierten die Server einwandfrei.

11. Warum konnten die Botnets die Kontaktformulare innerhalb kurzer Zeit derart massiv ausnutzen? Inwiefern gab es bekannte Schwachstellen (zum Beispiel Captcha, Rate Limits) beziehungsweise Sicherheitslücken?

    Kontaktformulare werden als Online-Dienste für den Bereich der öffentlichen Verwaltung grundsätzlich möglichst niedrigschwellig angeboten. Für den Prozess der Kontaktaufnahme erfolgt somit stets eine Abwägung zwischen einem hinnehmbaren Risiko derartiger Angriffe auf der einen und Barrierefreiheit, Datenschutz, Nutzer:innenzentrierung und Informationssicherheit auf der anderen Seite (vergleiche hierzu die Antwort zu Frage 12).

12. Inwiefern wurden nach dem Vorfall Sofortmaßnahmen oder Verbesserungen an den Sicherheitssystemen vorgenommen, zum Beispiel zusätzliche Sicherheits-Features auf Kontaktformularen oder strengere Zugangsbeschränkungen?

Es wird auf die Antwort zu Frage 4 Bezug genommen, in der die unmittelbar eingeleiteten Mitigationsmaßnahmen beschrieben werden.

Bisher wurden die E-Mail-Schnittstellen des Kontaktformulars via XSRF-Token abgesichert. Hierbei handelt es sich um einen Sicherheitsmechanismus, der entwickelt wurde, um Cross-Site-Request-Forgery (CSRF)-Angriffe zu verhindern. Bei diesen Angriffen wird das Vertrauen, das eine Webseite in den Browser eines Benutzers setzt, ausgenutzt. Angreifer:innen versuchen, Benutzer:innen zu ungewollten Aktionen zu verleiten. Als Cookie implementiert, bietet der XSRF-Token eine zusätzliche Sicherheitsebene, indem er sicherstellt, dass Anfragen von der legitimen Webseite und nicht von einer bösartigen Drittseite stammen. Dieser Schutz hat beim vorliegenden Angriff erstmalig keine Wirkung gezeigt.

Aktuell wird der Einsatz von CAPTCHA-Lösungen vorbereitet. Hierbei handelt es sich um sogenannte Challenge-Response-Tests, bei denen die interagierende Person eine Aufgabe (Challenge) lösen und das Ergebnis (Response) zurückschicken muss; hierdurch sollen Menschen von Computern unterschieden werden („Bist du ein Mensch?“). Da diese CAPTCHA-Lösungen in der Regel nicht barrierefrei sind, wird derzeit zwischen barrierefreier und sicherer Funktionalität abgewogen und eine nachhaltige Lösung erarbeitet. So ist vorgesehen, dass im Falle eines erneuten Angriffs den Kontaktformularen CAPTCHA-Lösungen temporär vorgeschaltet werden, um eine automatisierte Ausnutzung der Kontaktformulare zu verhindern.

Koordinierung der Gegenmaßnahmen und Krisenkommunikation

13. Welche Stellen innerhalb der Verwaltung waren für die Koordinierung der Gegenmaßnahmen zuständig, und wie lief die Entscheidungsfindung und interne (Krisen-)Kommunikation dazu ab?

Zuständig für das Content Management System und die dazugehörigen Webdienste inklusive der Kontaktformulare, über die die Spammails versandt wurden, ist die Kompetenzstelle CMS und Internet der Abteilung 4 beim Senator für Finanzen. Der Mailserver wird durch den zentralen IT-Dienstleister Dataport betrieben. Es fand eine Abstimmung zwischen der Kompetenzstelle CMS und Internet sowie dem zentralen Informationssicherheitsmanagement beim Senator für Finanzen statt.

Betroffenen Dienststellen wurde nach Eingang ihrer Meldung als Sofortmaßnahme die Deaktivierung ihres Kontaktformulars empfohlen. Zudem wurden nach Bekanntwerden des Angriffs die zuständigen Ressortansprechpersonen über den Angriff informiert. Hierbei handelt es sich um die für die Webseiten der Ressorts und zugeordneten Dienststellen zuständigen Ansprechpersonen. Im weiteren Verlauf der

Vorfallsanalyse wurden die genannten Ressortansprechpersonen über wesentliche Entwicklungen informiert. Zudem wurden weitere Stellen wie das CERT Nord, die Zentralstelle Cyber-Sicherheit beim Senator für Inneres und Sport sowie das zentrale Informations-sicherheitsmanagement informiert.

14. Wie erfolgte die externe (Krisen-)Kommunikation?

    Für die Krisenkommunikation bestehen je nach Bewertung der Sicherheitsereignisse Kommunikationsprozesse innerhalb und außerhalb der jeweiligen Organisation. Die externe Kommunikation findet hierbei insbesondere über die jeweils zuständigen Pressestellen sowie über das CERT Nord im Verwaltungs-CERT-Verbund (VCV) statt.

15. Inwiefern wurden das Bundeskriminalamt oder andere Stellen (zum Beispiel das Bundesamt für Sicherheit in der Informationstechnik [BSI] und das Nationale Cyber-Abwehrzentrum) beziehungsweise andere externe Stellen in die Koordinierung der Gegenmaßnahmen eingebunden? Wenn ja, in welcher Form?

    Das Sicherheitsereignis wurde nicht als zentraler Sicherheitsvorfall eingestuft. Ungeachtet dessen wurde der Sachverhalt im Verwaltungs-CERT-Verbund bekanntgegeben. Eine Einbindung weiterer Stellen war nicht erforderlich.

16. Gibt es eine einheitliche Notfall- und Krisenkommunikation für Cyber-Attacken auf die bremische IT-Infrastruktur, und wenn ja, wie ist diese strukturiert?

    Die bestehende Notfall- und Krisenkommunikation befindet sich aufgrund der geteilten Zuständigkeit in dem Gesamtkomplex der IT-Sicherheit, Informationssicherheit und Cyber-Sicherheit zwischen dem Senator für Finanzen, welcher für die Informationssicherheit in der öffentlichen Verwaltung zuständig ist, sowie dem Senator für Inneres und Sport, welcher für den Themenbereich Cyber-Sicherheit im Übrigen verantwortlich ist, derzeit in der Überarbeitung.

Aufklärung und Ermittlung

17. Inwiefern liegen bereits Erkenntnisse über die Hintermänner und Motive der Angriffe am 17. Dezember 2024 vor?

    Die eingegangenen Spammails waren in kyrillischer Schrift verfasst und verwiesen auf Glücksspiele und weitere Websites. Nähere Erkenntnisse über die Motive oder Täterhinweise liegen nicht vor.

18. Welche Sicherheitsbehörden (zum Beispiel Polizei Bremen oder Landeskriminalamt) haben dabei die Federführung?

Die deliktische Zuständigkeit für die Strafverfolgung bei Cyber-Angriffen in der Stadt Bremen liegt bei der Polizei Bremen.

19. Ist bereits ein Strafverfahren eingeleitet worden oder sind Strafanzeigen gestellt worden und, wenn ja, richten sich diese gegen Unbekannt oder gibt es konkrete Hinweise auf Verdächtige?

Von Amts wegen wurde durch die Polizei Bremen ein Ermittlungsverfahren eingeleitet. Zur Prüfung, ob es sich auf Grundlage der Gesamtumstände um ein strafrechtlich relevantes Verfahren handelt, wurde der Vorgang der Staatsanwaltschaft Bremen vorgelegt.

Langfristige Maßnahmen und Strategie

20. Welche Lehren zieht der Senat aus diesem Vorfall, um zukünftig ähnliche oder noch umfangreichere Angriffe auf die bremische IT-Infrastruktur erfolgreich abwehren und einen Ausfall von Systemen und Funktionen durch Redundanzen vermeiden zu können?

Die Angriffe auf bremische IT-Infrastrukturen sind, wie bei allen IKT-Infrastrukturen, anhaltend und unterliegen einer hohen Dynamik. Maßnahmen zur Verbesserung der Abwehrfähigkeit werden kontinuierlich und anlassunabhängig überprüft und bei erkannten Defiziten weiterentwickelt. Zur effektiven Bewältigung eines Vorfalls sind eine übergreifende Koordination von Maßnahmen sowie die Lagebilderstellung und Informationssteuerung von herausragender Bedeutung. Hierzu bedarf es einer übergeordneten und auf die an der Vorfallsbewältigung beteiligten Stellen abgestimmten Organisations- und Kommunikationsstruktur, die zuvörderst außerhalb eines Vorfalls Anwendung findet und in der Konsequenz im Ereignisfall routiniert bedient werden kann.

Die am 14. Januar 2025 erlassene Verwaltungsvorschrift zur Umsetzung der NIS-2-Richtlinie in der Freien Hansestadt Bremen (VV NIS2Ums FHB) sieht unter anderem vor, Meldevoraussetzungen sowie bestehende Meldewege zu überprüfen und zu optimieren. Dies entspricht der Zielrichtung der im April 2023 durch den Senat beschlossenen Bremischen Cyber-Sicherheitsstrategie, welche eine sinnvoll aufeinander abgestimmte Koordinierung der verschiedenen zuständigen Stellen im Rahmen einer harmonisierten und langsam aufwachsenden Cyber-Sicherheitsarchitektur verlangt. Der Zentralstelle Cyber-Sicherheit fällt hierbei eine koordinierende Funktion zu. Ihre übergeordnete Steuerung entlastet perspektivisch die für die Fachverfahren zuständigen Stellen, welche sich im Rahmen der Vorfallsbewältigung dann auf ihre Kernaufgaben konzentrieren und Ressourcen so noch effizienter nutzen können.

21. Welche Pläne gibt es, um die IT-Infrastruktur und Sicherheitskonzepte der Stadt Bremen zu modernisieren und zu stärken? Falls ja, wie sehen diese konkret aus (zum Beispiel Maßnahmen, Budget, Zeithorizont)?

    Durch die sukzessive Überführung von IKT-Infrastrukturen auf den zentralen IT-Dienstleister werden auch die relevanten Sicherheitsperimeter weiter ausgebaut, insbesondere im Bereich der Multi-Faktor-Authentifizierung und der Virtualisierung von Zugängen zu Diensten der Landesverwaltung. Sowohl die Technik als auch die konzeptionellen Arbeiten werden anhaltend in Richtung des Zero Trust-Prinzips fortgeschrieben. Ein konkreter Zeithorizont kann aufgrund der komplexen Umsetzung zurzeit nicht näher benannt werden und steht darüber hinaus unter dem Vorbehalt verfügbarer Haushaltsmittel.

    a) Welche Rolle spielt in diesem Zusammenhang die vom Senat am 14. Januar 2025 erlassene Verwaltungsvorschrift zur Umsetzung der zweiten EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2)?

       Mit der bezeichneten Verwaltungsvorschrift werden die für die Landesverwaltung zwingenden

       Bestimmungen der Richtlinie (EU) 2022/2555 in der Freien Hansestadt Bremen umgesetzt. Betroffen sind dabei ausschließlich bestimmte, aufgrund ihrer Verwaltungstätigkeiten als „kritisch“ identifizierte, Dienststellen der unmittelbaren Landesverwaltung („kritische Einrichtungen der Landesverwaltung“). Diese werden zum einen zu bestimmen Maßnahmen zur Gewährleistung ihrer IT-Sicherheit verpflichtet. Zum anderen erhält die Zentralstelle Cyber-Sicherheit beim Senator für Inneres und Sport nach der Richtlinie erforderliche neue Aufgaben, unter anderem im Bereich der Kontrolle und technischen Unterstützung bei der Bewältigung von Sicherheitsvorfällen. Die Verwaltungsvorschrift NIS2Ums FHB stellt somit einen wichtigen Schritt im kontinuierlichen Aufbau eines kohärenten Cyber-Sicherheitsrechtsrahmens in der Freien Hansestadt Bremen dar.

       Auf die Stadtgemeinde Bremen hat die Verwaltungsvorschrift NIS2Ums FHB grundsätzlich nur insoweit Einfluss, als die senatorischen Behörden in ihrer Doppelfunktion auch als Einrichtungen der Landesverwaltung unmittelbar betroffen sind.

    b) Welche wesentlichen Neuregelungen plant der Senat mit dem in Aussicht gestellten Cyber-Sicherheitsbasisgesetz (vergleiche dazu Antwort des Senats aus 21/852 vom 12. November 2024 auf eine Große Anfrage der fragestellenden Fraktion)? Wann plant er, den Gesetzentwurf zu beschließen und der parlamentarischen Beratung zuzuführen?

Mit dem Bremischen Cybersicherheitsbasisgesetz (BremCSBG) sollen – bis zur Erarbeitung eines Bremischen Cybersicherheitsgesetzes – kurzfristig erforderliche Regelungen im Bereich der Cyber-Sicherheit und IT-Sicherheit in der öffentlichen Verwaltung erlassen werden. Dabei geht es zum einen um die Verteilung von Aufgaben zwischen den fachlich zuständigen Behörden (der Zentralstelle Cyber-Sicherheit sowie dem Senator für Finanzen). Zum anderen sollen für die Fachbehörden und die Einrichtungen der öffentlichen Verwaltung bisher im Land nicht vorhandene spezifische gesetzliche Rechtsgrundlagen für bestimme Datenverarbeitungen geschaffen werden, die für die Cyber- und IT-Sicherheit erforderlich sind (etwa für den Betrieb von Angriffserkennungssystemen und weitere Maßnahmen zur Bewältigung von Sicherheitsvorfällen). Die Normierung von Verpflichtungen zu bestimmten Sicherheitsmaßnahmen ist in dem Gesetzesentwurf grundsätzlich nicht vorgesehen. Insoweit bleibt es bei den bestehenden Regelungen, etwa in der Informationssicherheitsleitlinie der Freien Hansestadt Bremen (IS-LL FHB) oder der Verwaltungsvorschrift NIS2Ums FHB. Es besteht aber insofern ein enger Zusammenhang, da mit dem Bremischen Cybersicherheitsbasisgesetz rechtssichere Grundlagen für die Wahrnehmung der verschiedenen Aufgaben und Verpflichtungen, insbesondere nach der NIS-2-Richtlinie, geschaffen werden. Der Gesetzesentwurf befindet sich momentan in der Ressortabstimmung.

22. In welcher Form ist die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter der Verwaltung vorgesehen, um bessere Reaktions- und Präventionsstrategien zu etablieren (zum Beispiel regelmäßige Schulungen, Security-Awareness-Programme)?

    Im Aus- und Fortbildungsprogramm der Freien Hansestadt Bremen werden Schulungen für IT-Sicherheitsbeauftragte und Awareness-Kampagnen angeboten. Zudem sind Online-Fortbildungen über das Intranet der öffentlichen Verwaltung der Freien Hansestadt Bremen abrufbar. Im Rahmen der Umsetzung der VV NIS2Ums FHB soll das bestehende Angebot geprüft und bei Bedarf überarbeitet werden.

Kosten und Ressourcen

23. Welche unmittelbaren Kosten sind durch die Abwehrmaßnahmen, das Abschalten von Systemen und Funktionen und mögliche Wiederherstellungs- oder Reparaturarbeiten entstanden?

    Da die eingeleiteten Mitigationsmaßnahmen unmittelbar wirkten und alle durch die Kompetenzstelle CMS und Internet betriebenen Systeme durchweg stabil betrieben werden konnten, mussten keine Systeme abgeschaltet werden. Wiederherstellungs- oder Reparaturarbeiten

waren nicht erforderlich. Alle im CMS-Kontext entstandenen Kosten sind durch die täglichen Betriebsaufgaben abgedeckt.

Weitere Kosten sind nach Kenntnis des Senats auch bei den betroffenen Stellen nicht entstanden.

24. Inwiefern sind zusätzliche Kosten für externe Dienstleister oder IT-Experten erforderlich geworden? Wenn ja, in welcher Höhe und wer trägt die Kosten?

    Es sind keine zusätzlichen Kosten entstanden.

25. Stehen ausreichend Fachpersonal und finanzielle Mittel zur Verfügung, um den wachsenden Anforderungen der Freien Hansestadt Bremen im Bereich IT-Sicherheit zu begegnen?

    Bremen, Hamburg, Schleswig-Holstein und Sachsen-Anhalt sind Trägerländer des zentralen IT-Dienstleisters Dataport (Anstalt öffentlichen Rechts). Die Weiterentwicklung des Cyber Defense Center (CDC), welches das Security Operation Center (SOC) sowie das CERT Nord umfasst, stellt einen wichtigen Schritt in der kontinuierlichen Absicherung der IT- und Cybersicherheit in der Freien Hansestadt Bremen dar und ist eng an die Verfügbarkeit vorhandener Haushaltsmittel geknüpft.

    Für die Kompetenzstelle CMS und Internet stehen ausreichend Fachpersonal und Mittel zur Verfügung.

Zusammenarbeit mit externen Partnern

26. Welche Rolle spielen – neben Dataport – externe Provider, IT-Dienstleister oder spezialisierte Unternehmen bei der Absicherung der Bremischen Behörden-IT?

    Externe Provider, IT-Dienstleister oder spezialisierte Unternehmen können eine sinnvolle Ergänzung im Gesamtgefüge der IT-Sicherheitsstruktur in der Freien Hansestadt Bremen darstellen; die Art und der Umfang ihrer Einbindung erfolgt stets nach sorgfältiger Abwägung unter Berücksichtigung vorhandener und notwendiger Kompetenzen sowie verfügbarer Haushaltsmittel.

27. Inwiefern ist geplant, enger mit anderen Bundesländern oder dem Bund zu kooperieren, um gemeinsamen Cyber-Angriffen vorzubeugen beziehungsweise bei Angriffen schneller zu reagieren?

    Dem intensiven und kontinuierlichen Austausch zwischen dem Bund und den Ländern fällt im Rahmen der Angriffsprävention und -bewältigung eine wichtige Rolle zu. Dies wurde bereits in der Bremischen Cybersicherheitsstrategie festgeschrieben. Die dort

vorgesehene angestrebte Kooperation mit dem BSI zur formalisierten vertieften Zusammenarbeit wurde im Rahmen einer Kooperationsvereinbarung am 15. August 2024 gemeinsam verwirklicht. Auf Basis dieser Vereinbarung werden perspektivisch vorbehaltlich verfügbarer Haushaltsmittel gemeinsame Anstrengungen in unterschiedlichen Handlungsfeldern umgesetzt. So sind für das 2. Quartal 2025 erste Gespräche zwischen der Freien Hansestadt Bremen und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Durchführung von Sicherheitschecks der bremischen IT-Infrastruktur terminiert.

Darüber hinaus bestehen weitere Austauschformate zwischen der Freien Hansestadt Bremen sowie den übrigen Ländern und dem Bund. So ist das CERT Nord Mitglied im Verwaltungs-CERT-Verbund, über den unter anderem relevante Informationen zu Cyber-Angriffen ausgetauscht werden, um schneller und effektiver auf diese reagieren zu können. Die Zentralstelle Cyber-Sicherheit steht als zentrale Koordinierungsstelle im Land zudem mit weiteren Cyber-Sicherheitsbehörden anderer Länder im Austausch. Ebenso nimmt die Freie Hansestadt Bremen sowohl an der Arbeitsgruppe Informationssicherheit (AG InfoSic), vertreten durch den Senator für Finanzen, als auch an der Länderarbeitsgruppe Cyber-Sicherheit (LAG Cyber-Sicherheit) der Innenministerkonferenz (IMK), vertreten durch den Senator für Inneres und Sport, teil. In diesen Gremien wird eine Vielzahl von Themen bearbeitet, um die Cyber-Resilienz aller Länder sowie des Bundes weiter zu stärken.

Zudem besteht ein Austausch zwischen den Zentralen Ansprechstellen Cyber-Crime der Landeskriminalämter sowie ein Austausch der Landesämter für Verfassungsschutz mit dem Bundesamt für Verfassungsschutz.

Weiterentwicklung der Online-Angebote

28. Wie soll sichergestellt werden, dass Kontaktformulare im Verantwortungsbereich der Freien Hansestadt Bremen zukünftig nicht mehr für Cyber-Angriffe missbraucht werden können?

    Die bei der Analyse des Vorfalls gewonnen Erkenntnisse finden Einfluss in die kontinuierliche Verbesserung der IT-Sicherheitsmaßnahmen des CMS KOGIS und der zugehörigen Systeme. Neben der Schließung erkannter Schwachstellen werden weitere präventive Maßnahmen, wie die in der Antwort zu Frage 12 genannten CAPTCHA-Lösungen, entwickelt, die eine erneute Ausnutzung der Kontaktformulare zum Versand von Spammails verhindern sollen.

29. Inwiefern beabsichtigt der Senat, alternative Kommunikationswege (zum Beispiel sichere Online-Portale) zu etablieren, um Bürgeranliegen

auf digitalem Weg nicht allein über E-Mail beziehungsweise einfache Kontaktformulare abzuwickeln?

Für KOGIS und die zugehörigen Webdienste sind die Kommunikationswege durchweg sicher. Eine Entwicklung alternativer Kommunikationswege ist zum aktuellen Zeitpunkt nicht beabsichtigt, da diese für KOGIS und die zugehörigen Webdienste als sicher angesehen werden und darüber hinaus der Versand von E-Mails an die betroffenen Stellen zu jederzeit weiterhin möglich war. Der massenhafte Versand von Spammails hatte keine negativen Auswirkungen auf die Schutzziele der Integrität, Authentizität oder Vertraulichkeit der Kommunikationswege.

30. Welche darüberhinausgehenden neuen Online-Angebote plant der Senat, die das Niveau der IT-Sicherheit erhöhen?

Es wird auf die Antworten zu den Fragen 28 und 29 Bezug genommen.