BREMISCHE BÜRGERSCHAFT **Drucksache 21/1115**
Landtag (zu Drs. 21/1020)
21. Wahlperiode 01.04.2025

Mitteilung des Senats vom 1. April 2025

Bremer Behörden mit DoS-Angriff erneut lahmgelegt – Was ist über den Cyberangriff vom 12. Februar 2025 bekannt?

Die Fraktion der CDU hat unter Drucksache 21/1020 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 haben der zentrale IT-Dienstleister Dataport, die Kompetenzstelle CMS und Internet beim Senator für Finanzen sowie die Zentralstelle Cybersicherheit beim Senator für Inneres erstmals Kenntnis vom Cyberangriff auf Bremer Behörden am 12. Februar 2025 erlangt?

   Die Mitarbeiter:innen der Kompetenzstelle CMS und Internet stellten am Morgen des 12. Februar 2025 gegen 07:15 Uhr fest, dass die Webseiten der Bremer Verwaltung nicht erreichbar waren.

   Eine erste telefonische Meldung erfolgte am 12. Februar 2025 circa 08:00 Uhr von der Zentralstelle für Cybersicherheit beim Senator für Inneres an die Zentralstelle Informationssicherheit und der zuständigen Stelle für das Content Management System 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?

   Durch die sofortige Alarmierung des zuständigen Dienstleisters durch die Mitarbeiterinnen der Kompetenzstelle CMS und Internet konnte durch die Auswertung der Logfiles beziehungsweise der Serverlast erkannt werden, dass es sich um einen gezielten Angriff auf die Webseite der Polizei Bremen (www[.]polizei.bremen[.]de) (Stand 1. April 2025) handelte. Bedrohungshinweise wurden zudem gegen circa 09:00

Uhr vom Nationalen IT-Lagezentrum im Bundesamt für Sicherheit in der Informationstechnik (BSI) übermittelt.

Die Zentralstelle Cybersicherheit wurde durch einen Mitarbeiter einer nachgeordneten Dienststelle informiert. Im Vorfeld lagen der Zentralstelle Cybersicherheit 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)?

   Durch den stattgefundenen schweren Distributed Denialof-Service-Angriff (DDoS-Angriff) auf die Webseite der Polizei Bremen und die damit verbundene große Serverlast gab es einen kurzfristigen Ausfall der Systeme, sodass die Webseiten der Verwaltung am Morgen des 12. Februar 2025 für circa 1,5 Stunden teilweise nicht erreichbar waren.

   Andere Systeme oder Funktionen waren davon nicht betroffen.

4. Wie genau erfolgte der Angriff und inwiefern unterschied er sich von dem Angriff am 17. Dezember 2024?

   Bei dem Angriff vom 17. Dezember 2024 handelte es sich um sogenanntes BotNet-Spamming. Hierbei wurden durch das Manipulieren der einfachen Kontaktformulare auf den betroffenen Websites große Mengen Spam versendet. Spam steht als Sammelbegriff für alle Formen von massenhaft versandten, unerwünschten E-Mails, elektronischen Kettenbriefe oder Werbeposts in sozialen Netzwerken.

   Bei dem Angriff vom 12. Februar 2025 handelte es sich um einen DDoS-Angriff. Bei einem DDoS-Angriff werden gezielt so viele Anfragen an einen Server gestellt, dass dieser – so wie am 12. Februar 2025 geschehen – die Anzahl der Anfragen nicht mehr bewältigen kann. An die Website www[.]polizei.bremen[.]de (Stand 1. April 2025) wurden bis zu 18 000 Anfragen pro Minute gestellt. Die dadurch entstandene Last beeinträchtigte die Performance in der Art, dass es zu einer Nicht-Erreichbarkeit der Systeme führte.

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

   Der Angriff dauerte bis in die Abendstunden an, bevor er schließlich abebbte. Aufgrund der eingeleiteten Gegenmaßnahmen konnte der Angriff aber durch die Identifikation des Angriffsvektors – die massenhafte Abfrage der auf der Website vorhandenen Suchfunktion – und die Deaktivierung dieser Suchfunktion bereits am frühen Vormittag

erfolgreich abgewehrt werden, sodass die Systeme nach circa 1,5 Stunden wieder erreichbar waren.

6. Welchen Zusammenhang gab es zwischen dem Angriff am 12. Februar 2025 beziehungsweise dessen Bekämpfung und dem laut Auskunft des Senats „geplanten Betriebssystem-Update“ am Abend desselben Tages?

   Wie alle IT-Systeme müssen auch die Webserver, auf denen die Websites der öffentlichen Verwaltung zur Verfügung gestellt werden, regelmäßig gewartet und geupdatet werden. Dieses reguläre und vollständig angekündigte Betriebssystem-Update war für den 6. Februar 2025 und den 12. Februar 2025 langfristig im Vorfeld angekündigt. Es bestand kein Zusammenhang zwischen dem Angriff vom 12. Februar 2025 sowie dem geplanten Betriebssystem-Update.

   a) Welche Websites, Systeme und Programme betraf das Update?

      Das Update betraf alle von KOGIS verwalteten Internet- und Intranetauftritte.

   b) Welche funktionalen Einschränkungen waren damit verbunden?

      Für das Update werden die Server heruntergefahren, sodass die KOGIS-Auftritte in den jeweils vorher genannten Zeiträumen nicht erreichbar sind (weder im Front- noch im Backend).

Schadensausmaß und Folgen

7. Welche konkreten Auswirkungen hatte der Angriff auf den Betriebsablauf in den betroffenen Behörden (zum Beispiel verzögerte Bearbeitungen, zeitweilige Ausfälle, eingeschränkte Erreichbarkeit)?

   Konkrete Auswirkungen auf die Betriebsabläufe sind nicht bekannt geworden.

8. Hat es im zeitlichen Zusammenhang mit der DoS-Attacke weitere, komplexere Angriffe auf die andere IT gegeben beziehungsweise inwiefern wurde dies geprüft?

   Gemäß Ziffer 5.4. der Informationssicherheitsleitlinie der Freien Hansestadt Bremen (IS-LL FHB) sind relevante Sicherheitsvorfälle dem CERT Nord zu melden.

   Im Zeitraum September 2024 bis Februar 2025 sind dem CERT Nord neben den bekannten Vorfällen vom 17. Dezember 2024 sowie dem 12. Februar 2025 die folgenden Sicherheitsvorfälle gemeldet worden:

— Ereignis: DDoS-Angriff auf die Website der Senatorin für Gesundheit, Frauen und Verbraucherschutz (gesundheit.bremen.de).

  Zeitraum: 13. Januarn2025.

  Keine Auswirkungen.

— Ereignis: Nicht autorisierte Verbindungsversuche mittels Brute-Force-Angriff, hierbei werden unzählige Zeichenfolgen als Kombinationen aus Nutzernamen und Kennwort verwendet bis eine solche Kombination Zugriff auf den Dienst gewährt, auf ein durch die BREKOM betriebenes Mail-Relay (ein Mail-Server, der E-Mails von einem Sender annimmt und an Dritte weiterleitet).

  Zeitraum: 22. Januar bis 24. Januar 2025.

  Keine Kompromittierung des Dienstes feststellbar.

— Ereignis: DDoS-Angriff auf die Websites der Wirtschaftsförderung Bremen (wfbbremen.de).

  Zeitraum: 28. Januar bis 29. Januar 2025.

  Keine Auswirkungen.

— Ereignis: Phishing-Angriff auf Mitarbeiter:innen der Schulverwaltung Bremen

  Zeitraum: 25. Februar bis 26. Februar 2025.

  Erfolgreiche Kompromittierung von zwei Accounts des durch die-Schulverwaltung betriebenen Mailsystems mit anschließendem SPAM-Versand aus der Absenderdomäne @schulverwaltung.bremen.de.

9. Inwiefern mussten neben dem Trennen der betroffenen Websites von Internet weitere Systeme heruntergefahren oder geschützt werden? Wenn ja, welche?

   Es mussten keine weiteren Systeme heruntergefahren werden. Durch die Deaktivierung des Kontaktformulars sowie der lokalen Suche auf der Website der Polizei Bremen konnten die Auswirkungen des Angriffs ausreichend abgemildert werden.

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

    Der Kompetenzstelle CMS und Internet sind keine Schäden bekannt geworden.

11. 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 weder zu einem Datendiebstahl noch zu einem Datenverlust, es wurden keine Informationen kompromittiert.

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

    Es wird auf die Antwort zu Frage 11 Bezug genommen.

IT-Sicherheitsmaßnahmen

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

    Die Websysteme werden durch ein umfangreiches System verschiedener IT-Sicherheitsmaßnahmen geschützt. So findet bei den durch die Kompetenzstelle CMS und Internet verwalteten Systemen eine intelligente Lastverteilung zwischen den eingesetzten Servern statt. Die bestehenden Sicherheitsmaßnahmen arbeiten erwartungsgemäß, sodass diverse Angriffe in der Vergangenheit abgewehrt werden konnten. Als Beispiel sei hier ein groß angelegter DDoS-Angriff im Frühjahr 2023 genannt, bei dem es zu einer Vielzahl an Ausfällen kam. Die Websites der Freien Hansestadt Bremen wurden hierbei ebenfalls angegriffen, jedoch konnten die bestehenden Sicherheitsmaßnahmen diese Angriffe erfolgreich abwehren, sodass es bei diesem Angriff zu keinen Beeinträchtigungen gekommen ist.

14. Inwiefern setzt der Senat zur Absicherung gegen DoS-Attacken spezialisierte Anti-Dos-Dienstleister ein?

    Die Kompetenzstelle CMS und Internet bezieht diverse Services bei unterschiedlichen Dienstleistern. Hierunter sind auch Dienstleister, die sich auf Cyber Security und Cyber Defense spezialisiert haben. Die dort vorhandene Expertise erstreckt sich hierbei über ein breites Themenfeld, zu dem nicht nur die Abwehr von DDoS-Attacken, sondern über den gesamten facettenreichen Bereich der Abwehr von Cyberkriminalität.

    a) Wenn ja, warum konnten diese Vorkehrungen bei dem Angriff am 12. Februar 2025 überwunden werden?

       Cyberkriminalität stellt aufgrund der sich permanent entwickelnden technischen Möglichkeiten die dynamischste Form von Kriminalität im digitalen Raum dar. Die Techniken und Taktiken der Angreifer

entwickeln sich permanent weiter, mit dem Ziel bestehende und wirksame Sicherheitsmaßnahmen zu umgehen. Ebenso werden diese Sicherheitsmaßnahmen permanent weiterentwickelt. Die aus den Angriffen gewonnenen Erkenntnisse fließen hierbei in die Weiterentwicklung ein. IT-Sicherheit ist ein fester Bestandteil der alltäglichen Arbeit der Kompetenzstelle CMS und Internet.

b) Wenn nein, warum nicht? Plant er, dies zukünftig zu tun (bitte begründen)?

Es wird auf die Antworten 14 und 14a Bezug genommen.

15. Warum konnten Angreifer die vorhandenen Sicherheitsvorkehrungen bei dem Angriff am 12. Februar 2025 erneut „erfolgreich“ überwinden? Inwiefern gab es bekannte Schwachstellen (zum Beispiel Captcha, Rate Limits) beziehungsweise Sicherheitslücken? Unterschieden sich diese von den im Zuge des Angriffs am 17. Dezember 2024 identifizierten Schwachstellen?

Wie dargestellt, handelte es sich bei den Angriffen vom 17. Dezember 2024 und vom 12. Februar 2025 um völlig unterschiedliche Angriffsarten beziehungsweise auch um unterschiedliche Ziele. Während bei einem Spam-Angriff das Ziel ist, Spam zu verteilen, ist bei einem DDoS-Angriff das Ziel, einen Server mit einer hohen Anzahl an Anfragen zu überlasten und hierdurch ausfallen zu lassen.

a) Wenn ja, worin?

Es wird auf die Antwort 15 Bezug genommen.

b) Wenn nein, warum wurden die Sicherheitslücken nach dem Angriff am 17. Dezember 2024 nicht geschlossen?

Da es sich bei den Angriffen vom 17. Dezember 2024 und vom 12. Februar 2025 um gänzlich unterschiedliche Angriffe handelte, für die unterschiedliche Angriffsvektoren genutzt wurden, besteht kein Zusammenhang zwischen den jeweiligen Schutzmaßnahmen. Sowohl im Nachgang zum Angriff vom 17. Dezember 2024 wie auch im Nachgang zum Angriff vom 12. Februar 2025 wurden die bestehenden Schutzmaßnahmen geprüft und angepasst.

16. Inwiefern wurden nach dem Vorfall zusätzliche Sofortmaßnahmen oder Verbesserungen an den Sicherheitssystemen vorgenommen?

Da der für den Angriff vom 12. Februar 2025 genutzte Angriffsvektor identifiziert werden konnte – es handelte sich unter anderem um die Ausnutzung der Suchfunktion auf der Website der Polizei – wurde kurzfristig eine Drosselung für die Anzahl der Suchanfragen eingebaut. Bei einer Häufung von Suchanfragen kann die Suche automatisch

deaktiviert werden, sodass der Angriffsvektor geschlossen wird. Diese Maßnahme wurde am 21. Februar 2025 erfolgreich umgesetzt, getestet und auf allen KOGIS-Webauftritten automatisch per Hotfix – hierbei handelt es sich um ein Software-Update, das außerhalb des normalen Update-Zyklus veröffentlicht wird oder auf einem Live-System installiert wird, zum Beispiel zur Behebung eines Fehlers – verteilt.

17. Inwiefern kann der Senat ausschließen, dass es in Zukunft zu weiteren „erfolgreichen“ Angriffen auf bremische Behörden kommt, die mit den Angriffen vom 17. Dezember 2024 und 12. Februar 2025 vergleichbar sind?

    Deutschland ist Zielland unterschiedlicher Angriffsformen hybrider Art. Dabei sind Cyberangriffe ein Instrument, um einerseits tatsächliche Schäden zu verursachen und andererseits in der Bevölkerung Verunsicherung hervorzurufen. Die Abwehr von Angriffen, wie denen vom 17. Dezember 2024 und 12. Februar 2025 findet in einem Spannungsfeld statt, in dem sowohl Verteidiger als auch Angreifer die ihnen zur Verfügung stehenden Mittel und Möglichkeiten permanent weiterentwickeln. Die Kompetenzstelle CMS und Internet als zuständige Stelle für die Webseiten der Bremer Verwaltung hat im Kontext dieser Entwicklung seit Jahren in die IT-Sicherheit investiert und wird es weiter tun. Im Nachgang zu den oben genannten Angriffen wurden die bestehenden Sicherheitsmaßnahmen auf ihre Wirksamkeit überprüft und angepasst, um Angriffe, die mit vergleichbaren Techniken und Prozeduren durchgeführt werden, besser abmildern zu können.

Koordinierung der Gegenmaßnahmen und Krisenkommunikation

18. Welche Stellen innerhalb der Verwaltung waren für die Koordinierung der Gegenmaßnahmen zuständig, und wie lief die Entscheidungsfindung?

    Es waren die folgenden Stellen eingebunden:

    — die fachverfahrensverantwortliche Stelle (Kompetenzstelle CMS und Internet),

    — der zuständige IT-Dienstleister,

    — die Sicherheitsorganisation, bestehend aus dem zentralen Informationssicherheitsmanagement (CISO und CIO), der Zentralstelle Cybersicherheit, dem CERT

    — sowie der zuständigen Pressestelle beim Senator für Finanzen in Abstimmung mit der Pressestelle des Senators für Inneres und Sport.

Eine Koordinierung der Gegenmaßnahmen war bei dem Angriff vom 12. Februar 2025 nicht weiter erforderlich, da die unmittelbare Lagebewältigung durch die Kompetenzstelle CMS und Internet in Zusammenarbeit mit dem entsprechenden Dienstleister stattfand. Durch die Kompetenzstelle CMS und Internet wurden die weiteren, oben genannten Stellen über die eingeleiteten Maßnahmen und die Entwicklung des Angriffs informiert.

19. Inwiefern wurden das Bundeskriminalamt oder andere Stellen (zum Beispiel das Bundesamt für Sicherheit in der Informationstechnik – BSI und das Nationale Cyberabwehrzentrum) beziehungsweise andere externe Stellen in die Koordinierung der Gegenmaßnahmen eingebunden? Wenn ja, in welcher Form?

    Eine Einbindung von Stellen außerhalb der Freien Hansestadt Bremen war nicht erforderlich und hat nicht stattgefunden.

20. Wie genau lief die interne und externe (Krisen-)Kommunikation ab?

    Für die Krisenkommunikation bestehen je nach Bewertung des Sicherheitsereignisses definierte Kommunikationswege innerhalb und außerhalb des eigenen Ressorts, insbesondere über die zuständigen Pressestellen, sowie über das CERT-Nord im Rahmen des Verwaltungs-CERT-Verbunds an die weiteren Landes-CERT und zum CERT-Bund des BSI.

    Nachdem die Zentralstelle Cybersicherheit über die Nicht-Verfügbarkeit der Websites der öffentlichen Verwaltung informiert wurde, nahm diese sowohl Kontakt mit der Kompetenzstelle CMS und Internet sowie dem zentralen Informationssicherheitsmanagement beim Senator für Finanzen auf. Durch die Kompetenzstelle CMS und Internet wurde daraufhin mitgeteilt, dass der DDoS-Angriff bekannt ist und bereits erste Maßnahmen durch den für die Administration der Server zuständigen Dienstleister eingeleitet wurden.

    Aufgrund der geringen Ausfallzeit der Websites fand keine weitere interne und externe Kommunikation statt.

21. Wie genau waren die Zentralstelle Cybersicherheit mit ihrem Chief Cybersecurity Officer (CCSO) beim Senator für Inneres sowie die Kompetenzstelle CMS und Internet beim Senator für Finanzen in die vorstehenden Entscheidungen, Abstimmungen und Maßnahmen eingebunden?

    Die Zentralstelle Cybersicherheit wurde durch die Kompetenzstelle CMS und Internet über die weitere Entwicklung informiert. Eine Einbindung der Zentralstelle Cybersicherheit in die weiteren Entscheidungen und Maßnahmen zur unmittelbaren Abwehr des DDoS-Angriffs war nicht erforderlich. Durch die Zentralstelle Cybersicherheit

konnte im Nachgang zu dem Angriff das von den Angreifern verwendete Angriffsskript gesichert und eingesehen werden. Diese Informationen wurden daraufhin der Kompetenzstelle CMS und Internet zur Verfügung gestellt. Die Inhalte des Angriffsskripts ergaben eine Überschneidung mit den bei der Kompetenzstelle CMS und Internet ebenfalls vorliegenden Informationen und bestätigten somit den Angriffsvektor.

22. Inwiefern gab es bei den Abläufen, Entscheidungen und Maßnahmen im Zusammenhang mit dem Angriff am 12. Februar 2025 Unterschiede zu denjenigen im Zusammenhang mit dem Angriff am 17. Dezember 2024?

    Beim Angriff vom 17. Dezember 2024 waren mehrere Postfächer der senatorischen Behörden sowie weiterer Dienststellen betroffen. Die Auswirkungen waren somit unmittelbar bei den Betroffenen bemerkbar, sodass eine informatorische Einbindung dieser in die weiteren Maßnahmen erfolgte.

    Während am 17. Dezember 2024 als Sofortmaßnahme die Kontaktformulare auf den Websites der betroffenen Stellen durch die jeweiligen Ressortansprechpersonen deaktiviert wurden und im Nachgang weitere technische Maßnahmen zum Schutz der Kontaktformulare umgesetzt wurden, wurde der Angriff vom 12. Februar 2025 zentral durch die Kompetenzstelle CMS und Internet in Zusammenarbeit mit dem für die Administration zuständigen Dienstleister bewältigt.

    Eine direkte Betroffenheit weiterer senatorischer Behörden oder Dienststellen war am 12. Februar 2025 nicht gegeben.

23. Wie ist die Zentralstelle Cybersicherheit organisatorisch aufgestellt sowie personell und materiell ausgestattet? Inwiefern entspricht das dem Soll-Zustand?

    Die Zentralstelle Cybersicherheit ist innerhalb der Linienorganisation ein eigenständiges Referat in der Abteilung Öffentliche Sicherheit beim Senator für Inneres und Sport.

    Für die Aufgabenwahrnehmung ist ihr derzeit ein Personal-Soll von 3,0 Vollzeiteinheiten auf drei Funktionsstellen zugeordnet. Die Funktionsstellen sind besetzt.

    Unbeschadet ihrer Stellung in der Linienorganisation ist die Zentralstelle Cybersicherheit nach § 3 Absatz 1 Satz 1 der Verwaltungsvorschrift zur Umsetzung der NIS-2-Richtlinie in der Freien Hansestadt Bremen (VV NIS2Ums FHB) zuständige Behörde für die in der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes

gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) benannten Aufsichtsaufgaben. Hierzu ist die Leitung der Zentralstelle Cybersicherheit zur Chief Cyber Security Officer (CCSO) der Freien Hansestadt Bremen berufen. Bei Aufsichtsanordnungen nach der NIS-2-Richtlinie handelt die CCSO unabhängig.

Für die Wahrnehmung der Aufgaben nach der NIS-2-Richtlinie, insbesondere für die Einrichtung eines Computer Security Incident Response Teams (CSIRT), beabsichtigt der Senat perspektivisch eine personelle Verstärkung der Zentralstelle Cybersicherheit.

Die materielle Ausstattung entspricht der üblichen Verwaltungsausstattung der bremischen Verwaltung, ergänzt um geheimschutzspezifische weitere Ausstattung. Die Ausstattung entspricht dem festgelegten Ausstattungs-Soll.

a) Wenn nein, worin liegen die Abweichungen zwischen Soll und Ist begründet?

Es bestehen keine Abweichungen zwischen Ist- und Soll-Zustand.

b) Wenn nein, durch welche Maßnahmen und bis wann soll der Soll-Zustand erreicht werden?

Es wird auf die Antwort zu Frage 24 Bezug genommen.

24. Wie ist die Kompetenzstelle CMS und Internet organisatorisch aufgestellt sowie personell und materiell ausgestattet? Inwiefern entspricht das dem Soll-Zustand?

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

a) Wenn nein, worin liegen die Abweichungen zwischen Soll und Ist begründet?

Es wird auf die Antwort zu Frage 24 Bezug genommen.

b) Wenn nein, durch welche Maßnahmen und bis wann soll der Soll-Zustand erreicht werden?

Es wird auf die Antwort zu Frage 24 Bezug genommen.

Aufklärung und Ermittlung

25. Welche Erkenntnisse liegen vor dem Hintergrund des Bekennerschreibens russischer Hacker über die Hintermänner und Motive des Angriffs am 12. Februar 2025 vor? Inwiefern ähneln beziehungsweise unterscheiden sich diese Hintermänner und Motive von dem Angriff am 17. Dezember 2024?

Bei dem Angriff vom 12. Februar 2025 handelt es nach derzeitigem Ermittlungsstand um einen sogenannten DDoS-Angriff, bei welchem die Erreichbarkeit der Webseite der Polizei Bremen durch Überlastungsanfragen auf den zum Hosting der Webseite genutzten Server erschwert beziehungsweise unmöglich gemacht wurde.

Der Angreifer vom 12. Februar 2025 ist gemäß Selbstbekenntnis die Gruppierung NoName057(16). Bei NoName057(16) handelt es sich um eine prorussische Hacker:innengruppe, die im Kontext des Kriegs in der Ukraine erstmals im März 2022 bekannt wurde. Die Gruppe zeichnet verantwortlich für diverse Cyberangriffe in der Ukraine, den Vereinigten Staaten von Amerika sowie einigen anderen europäischen Staaten.

Die Angriffe richten sich dabei in der Regel auf Webseiten von staatlichen Behörden, aber auch von Medien und privaten Unternehmungen. Die Gruppe veröffentlicht regelmäßig aktuelle Angriffsziele auf dem Messengerdienst „Telegram“.

Ziel der Gruppierung NoName057(16) ist es nach eigener Darstellung, Unterstützer der Ukraine zu beeinträchtigen und gleichzeitig russische Propaganda zu verbreiten. In diversen Veröffentlichungen wird darüber berichtet, dass das Ziel eine möglichst breite Berichterstattung in den Medien ist. Dies gelingt einerseits durch bekannte Opfer wie Regierungen oder große Unternehmen, andererseits durch unangenehme Störungen für viele Personen, etwa durch das Lahmlegen des Ticketverkaufs für öffentliche Verkehrsmittel.

Der Bedrohungsakteur NoName057(16) führt nach Kenntnis des Senats DDoS-Angriffe durch – der Versand von Spam-Mail ist nach vorliegenden Erkenntnissen keine Vorgehensweise des Akteurs. Über die Hinterleute, Motive und Hintergründe des Angriffs vom 17. Dezember 2024 liegen dem Senat bislang keine weiteren Erkenntnisse vor.

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

    Die deliktische Zuständigkeit für die Strafverfolgung bei Cyberangriffen in der Stadt Bremen liegt bei der Polizei Bremen.

    Aufgrund der bundesweiten Auswirkungen und bereits betroffenen Einrichtungen des Bundes (unter anderem Bundesregierung, BMVg) werden die zentralen Ermittlungen zur Gruppe NoName057(16) durch das Bundeskriminalamt im Auftrag der Generalstaatsanwaltschaft Frankfurt/Main – Zentralstelle für Internetstraftaten – geführt.

27. 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? Inwiefern führen diese Hinweise in eine ähnliche oder in eine andere Richtung wie die Hinweise zu dem Angriff am 17. Dezember 2024?

Die Polizei Bremen leitete von Amts wegen ein Ermittlungsverfahren ein. Dieses befindet sich derzeit in Bearbeitung in der Staatsschutzabteilung der Polizei Bremen. Es wird in Kürze zur strafrechtlichen Würdigung der Staatsanwaltschaft vorgelegt werden. Hinweise oder Erkenntnisse auf einen Zusammenhang der zwei in Rede stehenden Angriffe liegen bislang nicht vor.

Langfristige Maßnahmen und Strategie

28. Welche Lehren zieht der Senat aus diesem erneuten 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 Kompetenzstelle CMS und Internet wird weiterhin einen Schwerpunkt auf die Verbesserung der IT-Sicherheit ihrer Systeme legen. Die Informations- und Kommunikationstechnologie der Freien Hansestadt Bremen wird fortwährend unter ökonomischen und ökologischen Rahmenbedingungen weiterentwickelt. Dem Senat ist bewusst, dass es keinen einhundertprozentigen Schutz geben kann, gewinnt jedoch aus jedem Vorfall Erkenntnisse zur angemessenen Fortentwicklung der Sicherheitssysteme und -konzepte.

29. Inwiefern beeinflusst der erneute Angriff am 12. Februar 2025 die Pläne des Senats zur Modernisierung der IT-Infrastruktur und Stärkung der Sicherheitskonzepte?

    Es wird auf die Antwort zu Frage 28 Bezug genommen.

30. Inwiefern beeinflusst der erneute Angriff am 12. Februar 2025 die Aktivitäten und Pläne des Senats zur Sensibilisierung der Mitarbeiterinnen und Mitarbeiter der Verwaltung, um bessere Reaktions- und Präventionsstrategien zu etablieren?

    Eine einheitliche Notfall- und Krisenkommunikation befindet sich aufgrund der geteilten Zuständigkeit zwischen dem Senator für Finanzen und dem Senator für Inneres und Sport derzeit in Überarbeitung. Da DDoS-Angriffe auf technische Systeme zielen beziehungsweise kein weiteres Zusammenwirken zwischen Menschen und Maschine hierfür erforderlich ist, besteht keine wirksame Möglichkeit DDoS-Angriffe durch die Sensibilisierung von Mitarbeiter:innen zu verhindern.

    Gleichwohl ist dem Senat bewusst, dass eine weiterführende Sensibilisierung der Mitarbeiter:innen die Cybersicherheit innerhalb der

öffentlichen Verwaltung weiter optimieren kann. 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 wird das bestehende Angebot geprüft und bei Bedarf überarbeitet werden.

Kosten und Ressourcen

31. Welche unmittelbaren Kosten sind durch die Abwehrmaßnahmen, das Abschalten von Systemen und Funktionen und mögliche Wiederherstellungs- oder Reparaturarbeiten im Zuge des Angriffs am 12. Februar 2025 entstanden?

    Es sind keine zusätzlichen Kosten angefallen.

32. 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 angefallen.

33. Inwiefern beeinflusst der erneute Angriff am 12. Februar 2025 die Einschätzung des Senats zu den Erfordernissen für IT-Fachpersonal und finanziellen Mitteln für IT-Sicherheit?

    Der Senat hat durch seine Entscheidung, den IT-Dienstleister Dataport mit wesentlichen Aufgaben der Informations- und Kommunikationstechnologie zu betrauen, eine richtungsweisende Entscheidung für professionelle IT getroffen und steuert anhaltend Ressourcen für die Fortentwicklung.

Zusammenarbeit mit externen Partnern

34. Wie bewertet der Senat vor dem Hintergrund des erneuten Angriffs am 12. Februar 2025 die Arbeit von Dataport und weiterer zuständiger bremischer Stellen sowie deren Zusammenarbeit mit externen Providern, IT-Dienstleistern und spezialisierten Unternehmen bei der Absicherung der Bremischen Behörden-IT?

    Die Zusammenarbeit der Kompetenzstelle CMS und Internet mit den eigenen Dienstleistern basiert auf gegenseitigem Vertrauen, was sich auch in der professionellen und erfolgreichen Zusammenarbeit äußert.

    Die Zusammenarbeit mit Dataport wird ebenfalls positiv bewertet. Bei Dataport handelt es sich um einen professionellen IT-Dienstleister welcher über eine umfangreiche Sicherheitsorganisation verfügt. Das bei Dataport vorhandene Wissen fließt ebenfalls in die Absicherung der

bremischen Behörden IT ein. Im Rahmen der Umsetzung der VV NIS2Ums FHB innerhalb der öffentlichen Verwaltung sollen die bestehenden Strukturen und Dienstleistungen zur Absicherung der IT der öffentlichen Verwaltung analysiert werden. Hierbei sollen insbesondere die bestehenden Meldewege geprüft und mit den in der VV NIS2Ums FHB vorgesehenen Abläufen harmonisiert werden. Ebenso ist vorgesehen, dass ein CSIRT eingerichtet werden soll. Neben den bestehenden Dienstleistungen, wie dem bereits durch das CERT Nord betriebenen Warn- und Informationsdienst, soll das CSIRT präventiv und reaktiv unterstützend tätig werden. Ein Ziel ist es zum Beispiel die Fähigkeiten zur Detektion und Abwehr von Cyberangriffen auf die öffentliche Verwaltung weiter auszubauen und Dienstleistungen im Rahmen der IT-Forensik, unter der Inanspruchnahme weiterer spezialisierter Dienstleister, vorzuhalten

35. Inwiefern beeinflusst der erneute Angriff am 12. Februar 2025 die Notwendigkeit und Bereitschaft des Senats, noch enger mit anderen Bundesländern oder dem Bund zu kooperieren, um gemeinsamen Cyber-Angriffen vorzubeugen beziehungsweise schneller auf Angriffe 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 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 bundesweiten 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 Cybersicherheit steht als zentrale Koordinierungsstelle im Land zudem mit weiteren Cybersicherheitsbehörden 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 Cybersicherheit (LAG Cybersicherheit) der Innenministerkonferenz, 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 Cybercrime der Landeskriminalämter sowie ein Austausch der Landesämter für Verfassungsschutz mit dem Bundesamt für Verfassungsschutz.

Weiterentwicklung der Online-Angebote und der IT-Infrastruktur

36. Laut Pressemitteilung des Senats hat es bei dem DoS-Angriff am 12. Februar 2025 bis zu 18 000 Anfragen pro Minute (rpm) gegeben, was zur Überlast führte. Ist der Senat der Meinung, dass die bremische IT-Infrastruktur (insbesondere die angegriffene Website beziehungsweise der angegriffene Server) ausreichend dimensioniert für ihren Zweck ist?

    Die Systeme laufen stabil und leistungsfähig und sind ausreichend dimensioniert.

    a) Wenn ja, wie begründet er dies vor dem Hintergrund, dass 18 000 Anfragen pro Minute bei einer größeren, optimierten Website nicht zur Überlast führen müssen?

        Bei den genannten 18 000 Anfragen pro Minute handelt es sich um ein Beispiel, welches die Dimension des Angriffs greifbar machen sollte. Zum Ausmaß eines DDoS-Angriffs und den eventuell entstehenden Folgen und Ausfällen gehören neben den Anfragen pro Minute eine Vielzahl an weiteren Parametern. In der konkreten Konstellation des Angriffs vom 12. Februar 2025 kam es zu einem kurzfristigen Ausfall. Die erkannten Schwachstellen wurden bereits behoben. Grundsätzlich laufen die Systeme stabil und performant, zudem wird die Vielzahl der Angriffe abgewehrt. Anhand des kurzfristigen Ausfalls vom 12. Februar 2025 kann daher nicht geschlussfolgert werden, dass die bestehende IT-Infrastruktur nicht ausreichend dimensioniert ist.

    b) Wenn nein, wie will er die Dimensionierung der IT-Infrastruktur bedarfsgerecht anpassen?

        Es wird auf die Antwort zu Frage 36a Bezug genommen.

37. Wie beeinflusst der erneute Angriff am 12. Februar 2025 die Pläne des Senats zur Weiterentwicklung der Online-Angebote der Bremer Behörden (zum Beispiel Überarbeitung der Kontaktformulare und Bereitstellung alternative Kommunikationswege)?

    Für KOGIS und die zugehörigen Webdienste sind die Kommunikationswege durchweg sicher. Im Rahmen der

kontinuierlichen Verbesserung werden die Erkenntnisse dieses Angriffs wieder in die bestehenden und zu entwickelnden IT-Sicherheitsmaßnahmen des Bremer Content Management Systems KOGIS und der zugehörigen Systeme einfließen.