BREMISCHE BÜRGERSCHAFT **Drucksache 21/1020**
Landtag
21. Wahlperiode **18. Februar 2025**

Kleine Anfrage der Fraktion der CDU

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

Am 12. Februar 2025 wurden Bremer Behörden erneut Opfer eines orchestrierten Cyberangriffs, zu dem sich nach Auskunft der Zentralstelle Cybersicherheit beim Senator für Inneres eine russische Hackergruppe bekannt hat. Betroffen waren laut Presseberichten die Polizei, die Senatskanzlei sowie das Finanz-, Sozial- und Bildungsressort, deren Internetseiten aufgrund eines Denial-of-Service-Angriffs (DoS-Angriff) auf die Website der Polizei Bremen am besagten Tag für mehrere Stunden nicht erreichbar waren. Nach dem Angriff am 17. Dezember 2024 ist dies nun der zweite, aus Sicht der Angreifer erfolgreich verlaufene Angriff auf Bremer Behörden innerhalb kurzer Zeit. Die in der Kleinen Anfrage der Fragesteller aus Drs. 21/1008 vom 11.02.2025 aufgeworfenen Fragen nach den verwendeten Sicherheitsvorkehrungen und Präventionsmaßnahmen, Überwachungssystemen und Notfallmaßnahmen stellen sich daher erneut und mit erhöhter Dringlichkeit. Offenbar waren die Lehren und Konsequenzen, die nach dem Angriff am 17. Dezember gezogen wurden, unzureichend und nicht geeignet, um weitere Angriffe auf bremische Behörden im Vorfeld abzuwehren. Dies ist bedenklich, wirft kein gutes Licht auf den Senat und die für IT-Sicherheit zuständigen Stellen und verlangt nach wirksamen Konsequenzen.

Wir fragen den Senat:

Kenntnisstand und Ablauf des Angriffs

1. Wann genau haben der 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 12.02.2025 erlangt?
2. Über welche Indikatoren wurde der Angriff entdeckt (z.B. auffällige Serverlast, in-terne Meldungen, Security-Monitoring)? Inwiefern gab es im Vorfeld konkrete Be-drohungshinweise und, wenn ja, von wem an wen?
3. Welche Fachressorts, Einrichtungen, Systeme und Funktionen waren konkret da-von betroffen und in welchem Umfang (z.B. Anzahl betroffener E-Mail-Postfächer)?
4. Wie genau erfolgte der Angriff und inwiefern unterschied er sich von dem Angriff am 17.12.2024?
5. Wie lange dauerte der Angriff und die Schadensbehebung? Wann waren alle Systeme wieder sicher und in vollem Umfang funktionsfähig?
6. Welchen Zusammenhang gab es zwischen dem Angriff am 12.02.2025 bzw. dessen Bekämpfung und dem laut Auskunft des Senats „geplanten Betriebssystem-Update“ am Abend desselben Tages?
a. Welche Websites, Systeme und Programme betraf das Update?
b. Welche funktionalen Einschränkungen waren damit verbunden?

Schadensausmaß und Folgen

7. Welche konkreten Auswirkungen hatte der Angriff auf den Betriebsablauf in den betroffenen Behörden (z.B. verzögerte Bearbeitungen, zeitweilige Ausfälle, eingeschränkte Erreichbarkeit)?
8. Hat es im zeitlichen Zusammenhang mit der DoS-Attacke weitere, komplexere An-griffe auf die andere IT gegeben bzw. inwiefern wurde dies geprüft?
9. Inwiefern mussten neben dem Trennen der betroffenen Websites von Internet weitere Systeme heruntergefahren oder geschützt werden? Wenn ja, welche?
10. Welche Schäden (z.B. Sachschäden oder sonstige wirtschaftliche Schäden) hat der Angriff bei wem verursacht?
11. Inwiefern kam es bei dem Angriff zu einem Datenverlust oder Datendiebstahl? Wurden personenbezogene Daten (z.B. aus Formularen) oder andere sensible In-formationen kompromittiert?
12. Welche davon betroffenen Personen und Institutionen wurden wann informiert?

IT-Sicherheitsmaßnahmen

13. Welche präventiven Maßnahmen waren vor dem Vorfall in Kraft (z.B. Firewall- und Spam-Filter-Systeme, Intrusion-Detection-Systeme, Load-Balancer, CDN) und inwiefern haben diese wie erwartet funktioniert?
14. Inwiefern setzt der Senat zur Absicherung gegen DoS-Attacken spezialisierte Anti-Dos-Dienstleister ein?
a. Wenn ja, warum konnten diese Vorkehrungen bei dem Angriff am 12.02.2025 überwunden werden?
b. Wenn nein, warum nicht? Plant er, dies zukünftig zu tun? (bitte begründen)
15. Warum konnten Angreifer die vorhandenen Sicherheitsvorkehrungen bei dem An-griff am 12.02.2025 erneut „erfolgreich“ überwinden? Inwiefern gab es bekannte Schwachstellen (z.B. Captcha, Rate Limits) bzw. Sicherheitslücken? Unterschieden sich diese von den im Zuge des Angriffs am 17.12.2024 identifizierten Schwachstellen?
a. Wenn ja, worin?
b. Wenn nein, warum wurden die Sicherheitslücken nach dem Angriff am 17.12.2024 nicht geschlossen?
16. Inwiefern wurden nach dem Vorfall zusätzliche Sofortmaßnahmen oder Verbesse-rungen an den Sicherheitssystemen vorgenommen?
17. Inwiefern kann der Senat ausschließen, dass es in Zukunft zu weiteren „erfolgreichen“ Angriffen auf bremische Behörden kommt, die mit den Angriffen vom 17.12.2024 und 12.02.2025 vergleichbar sind?

Koordinierung der Gegenmaßnahmen und Krisenkommunikation

18. Welche Stellen innerhalb der Verwaltung waren für die Koordinierung der Gegenmaß-nahmen zuständig und wie lief die Entscheidungsfindung?
19. Inwiefern wurden das Bundeskriminalamt oder andere Stellen (z.B. das Bundes-amt für Sicherheit in der Informationstechnik – BSI und das Nationale Cyberabwehrzentrum) bzw. andere externe Stellen in die Koordinierung der Gegenmaß-nahmen eingebunden? Wenn ja, in welcher Form?
20. Wie genau lief die interne und externe (Krisen-)Kommunikation ab?
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?
22. Inwiefern gab es bei den Abläufen, Entscheidungen und Maßnahmen im Zusammenhang mit dem Angriff am 12.02.2025 Unterschiede zu denjenigen im Zusammenhang mit dem Angriff am 17.12.2025?
23. Wie ist die Zentralstelle Cybersicherheit organisatorisch aufgestellt sowie personell und materiell ausgestattet? Inwiefern entspricht das Soll-Zustand?
a. Wenn nein, worin liegen die Abweichungen zwischen Soll und Ist begründet?

b. Wenn nein, durch welche Maßnahmen und bis wann soll der Soll-Zustand er-reicht werden?
24. Wie ist die Kompetenzstelle CMS und Internet organisatorisch aufgestellt sowie personell und materiell ausgestattet? Inwiefern entspricht das Soll-Zustand?
a. Wenn nein, worin liegen die Abweichungen zwischen Soll und Ist begründet?
b. Wenn nein, durch welche Maßnahmen und bis wann soll der Soll-Zustand er-reicht werden?

Aufklärung und Ermittlung

25. Welche Erkenntnisse liegen vor dem Hintergrund des Bekennerschreibens russischer Hacker über die Hintermänner und Motive des Angriffs am 12.02.2025 vor? Inwiefern ähneln bzw. unterscheiden sich diese Hintermänner und Motive von dem Angriff am 17.12.2024?
26. Welche Sicherheitsbehörden (z.B. Polizei Bremen oder Landeskriminalamt) haben dabei die Federführung?
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 17.12.2024?

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?
29. Inwiefern beeinflusst der erneute Angriff am 12.02.2025 die Pläne des Senats zur Modernisierung der IT-Infrastruktur und Stärkung der Sicherheitskonzepte?
30. Inwiefern beeinflusst der erneute Angriff am 12.02.2025 die Aktivitäten und Pläne des Senats zur Sensibilisierung der Mitarbeiterinnen und Mitarbeiter der Verwaltung, um bessere Reaktions- und Präventionsstrategien zu etablieren?

Kosten und Ressourcen

31. Welche unmittelbaren Kosten sind durch die Abwehrmaßnahmen, das Abschalten von Systemen und Funktionen und mögliche Wiederherstellungs- oder Reparatur-arbeiten im Zuge des Angriffs am 12.02.2025 entstanden?
32. Inwiefern sind zusätzliche Kosten für externe Dienstleister oder IT-Experten erforderlich geworden? Wenn ja, in welcher Höhe und wer trägt die Kosten?
33. Inwiefern beeinflusst der erneute Angriff am 12.02.2025 die Einschätzung des Senats zu den Erfordernissen für IT-Fachpersonal und finanziellen Mitteln für IT-Sicherheit?

Zusammenarbeit mit externen Partnern

34. Wie bewertet der Senat vor dem Hintergrund des erneuten Angriffs am 12.02.2025 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?
35. Inwiefern beeinflusst der erneute Angriff am 12.02.2025 die Notwendigkeit und Bereitschaft des Senats, noch enger mit anderen Bundesländern oder dem Bund zu kooperieren, um gemeinsamen Cyber-Angriffen vorzubeugen bzw. schneller auf Angriffe schneller zu reagieren?

Weiterentwicklung der Online-Angebote und der IT-Infrastruktur

36. Laut Pressemitteilung des Senats hat es bei dem DoS-Angriff am 12.02.2025 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 bzw. der angegriffene Server) ausreichend dimensioniert für ihren Zweck ist?
a. Wenn ja, wie begründet er dies vor dem Hintergrund, dass 18.000 rpm bei einer größeren, optimierten Website nicht zur Überlast führen müssen?
b. Wenn nein, wie will er die Dimensionierung der IT-Infrastruktur bedarfsgerecht anpassen?
37. Wie beeinflusst der erneute Angriff am 12.02.2025 die Pläne des Senats zur Weiterentwicklung der Online-Angebote der Bremer Behörden (z.B. Überarbeitung der Kontaktformulare und Bereitstellung alternative Kommunikationswege)?

Beschlussempfehlung:

Simon Zeimke, Dr. Wiebke Winter, Frank Imhoff und Fraktion der CDU