BREMISCHE BÜRGERSCHAFT Drucksache 21/
Landtag
21. Wahlperiode

Kleine Anfrage der Fraktion der CDU

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

Am 17. Dezember 2024 wurden mehrere Bremer Behörden Opfer eines groß angelegten Cyberangriffs. Betroffen waren laut Presseberichten das Gesundheitsressort, das Sozialressort, das Bauressort und die Polizei. Demnach hat ein sogenanntes Botnet, d.h. ein Zusammenschluss mehrerer autonom tätiger Programme auf miteinander vernetzten Rechnern, die Behördenpostfächer über ein interaktives Kontaktformular mit Spammails geflutet. Allein beim Gesundheitsressort gingen den Angaben zufolge innerhalb kürzester Zeit 2.000 E-Mails ein. Als Sofortmaßnahme wurden die Kontaktformulare deaktiviert, auch der Polizeinotruf war temporär nicht erreichbar.

Grundsätzlich unterliegen die im Einflussbereich der Freien Hansestadt Bremen (FHB) betriebenen IT-Systeme, sofern sie eine Schnittstelle zu öffentlichen Netzen haben, permanent der Gefahr von Cyberangriffen. Die aktuelle Bedrohungslage im Cyberraum ist bundesweit unverändert hoch. Durch geeignete Sicherheitsvorkehrungen und Präventionsmaßnahmen, Überwachungssysteme und den Einsatz von Computer Emergency Response Teams (CERT-Teams) im akuten Bedrohungsfall wird versucht, der Gefahr zu begegnen. Auch wenn es keine 100-prozentige Sicherheit gegen Cyberangriffe geben kann, stellt sich doch die Frage nach möglichen Sicherheitslücken, die den jüngsten Angriff begünstigt haben könnten, und – daraus abgeleitet – nach einer Neuordnung der Bremischen Cybersicherheitsarchitektur.

Wir fragen den Senat:

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 17.12.2024 erlangt?
2. Über welche Indikatoren wurde der Angriff entdeckt (z.B. auffällige Serverlast, interne Meldungen, Security-Monitoring)? Inwiefern gab es im Vorfeld konkrete Bedrohungshinweise und, wenn ja, von wem an wen?
3. Welche Fachressorts, Einrichtungen, Systeme und Funktionen waren konkret davon betroffen und in welchem Umfang (z.B. Anzahl betroffener E-Mail-Postfächer, Kontaktformulare)?

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

Schadensausmaß und Folgen

5. Welche konkreten Auswirkungen hatten die Angriffe auf den Betriebsablauf in den betroffenen Behörden (z.B. verzögerte Bearbeitungen, zeitweilige Ausfälle, eingeschränkte Erreichbarkeit)?
6. Inwiefern mussten neben dem Abschalten der Kontaktformulare weitere Systeme heruntergefahren oder geschützt werden? Wenn ja, welche?
7. Welche Schäden (z.B. Sachschäden oder sonstige wirtschaftliche Schäden) hat der Angriff bei wem verursacht?
8. Inwiefern kam es bei dem Angriff zu einem Datenverlust oder Datendiebstahl? Wurden personenbezogene Daten (z.B. aus Formularen) oder andere sensible Informationen kompromittiert?
9. Welche davon betroffenen Personen und Institutionen wurden wann informiert?

IT-Sicherheitsmaßnahmen

10. Welche präventiven Maßnahmen waren vor dem Vorfall in Kraft (z.B. Firewall- und Spam-Filter-Systeme, Intrusion-Detection-Systeme) und inwiefern haben diese wie erwartet funktioniert?
11. Warum konnten die Botnets die Kontaktformulare innerhalb kurzer Zeit derart massiv ausnutzen? Inwiefern gab es bekannte Schwachstellen (z.B. Captcha, Rate Limits) bzw. Sicherheitslücken?
12. Inwiefern wurden nach dem Vorfall Sofortmaßnahmen oder Verbesserungen an den Sicherheitssystemen vorgenommen, z.B. zusätzliche Sicherheits-Features auf Kontaktformularen oder strengere Zugangsbeschränkungen?

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?
14. Wie erfolgte die externe (Krisen-)Kommunikation?
15. Inwiefern wurden das Bundeskriminalamt oder andere Stellen (z.B. das Bundesamt für Sicherheit in der Informationstechnik – BSI und das Nationale Cyberabwehrzentrum) bzw. andere externe Stellen in die Koordinierung der Gegenmaßnahmen eingebunden? Wenn ja, in welcher Form?
16. Gibt es eine einheitliche Notfall- und Krisenkommunikation für Cyber-Attacken auf die bremische IT-Infrastruktur, und wenn ja, wie ist diese strukturiert?

Aufklärung und Ermittlung

17. Inwiefern liegen bereits Erkenntnisse über die Hintermänner und Motive der Angriffe am 17.12.2024 vor?
18. Welche Sicherheitsbehörden (z.B. Polizei Bremen oder Landeskriminalamt) haben dabei die Federführung?

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?

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?
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 (z.B. Maßnahmen, Budget, Zeithorizont)?
    a. Welche Rolle spielt in diesem Zusammenhang die vom Senat am 14.01.2025 erlassene Verwaltungsvorschrift zur Umsetzung der zweiten EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2)?
    b. Welche wesentlichen Neuregelungen plant der Senat mit dem in Aussicht gestellten Cybersicherheitsbasisgesetz (vgl. dazu Antwort des Senats aus 21/852 vom 12.11.2025 auf eine Große Anfrage der fragestellenden Fraktion)? Wann plant er, den Gesetzentwurf zu beschließen und der parlamentarischen Beratung zuzuführen?
22. In welcher Form ist die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter der Verwaltung vorgesehen, um bessere Reaktions- und Präventionsstrategien zu etablieren (z.B. regelmäßige Schulungen, Security-Awareness-Programme)?

Kosten und Ressourcen

23. Welche unmittelbaren Kosten sind durch die Abwehrmaßnahmen, das Abschalten von Systemen und Funktionen und mögliche Wiederherstellungs- oder Reparaturarbeiten entstanden?
24. Inwiefern sind zusätzliche Kosten für externe Dienstleister oder IT-Experten erforderlich geworden? Wenn ja, in welcher Höhe und wer trägt die Kosten?
25. Stehen ausreichend Fachpersonal und finanzielle Mittel zur Verfügung, um den wachsenden Anforderungen der Freien Hansestadt Bremen im Bereich IT-Sicherheit zu begegnen?

Zusammenarbeit mit externen Partnern

26. Welche Rolle spielen – neben Dataport – externe Provider, IT-Dienstleister oder spezialisierte Unternehmen bei der Absicherung der Bremischen Behörden-IT?
27. Inwiefern ist geplant, enger mit anderen Bundesländern oder dem Bund zu kooperieren, um gemeinsamen Cyber-Angriffen vorzubeugen bzw. bei Angriffen schneller zu reagieren?

Weiterentwicklung der Online-Angebote

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

29. Inwiefern beabsichtigt der Senat, alternative Kommunikationswege (z.B. sichere Online-Portale) zu etablieren, um Bürgeranliegen auf digitalem Weg nicht allein über E-Mail bzw. einfache Kontaktformulare abzuwickeln?
30. Welche darüberhinausgehenden neuen Online-Angebote plant der Senat, die das Niveau der IT-Sicherheit erhöhen?

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