BREMISCHE BÜRGERSCHAFT **Drucksache 21/1600**
Landtag
21. Wahlperiode **10. Februar 2026**

Große Anfrage der Fraktion der CDU

Wie gut sind die Eigen- und Beteiligungsbetriebe im Land Bremen vor Cyberangriffen geschützt?

Die Ramsomware-Attacke vom 3. Februar 2026 auf den städtischen Eigenbetrieb Werkstatt Bremen, von dem auch die Beweismittelstelle der Polizei Bremen betroffen war, verdeutlich erneut die ernste Bedrohungslage im Cyberraum für die öffentliche Daseinsvorsorge. Bereits vor einem Jahr wurden verschiedene Bremer Behörden Opfer orchestrierter Cyberangriffe. Während damals die Kernverwaltung betroffen war, wirft der aktuelle Vorfall ein Schlaglicht auf die Sicherheitsvorkehrungen, die die Eigen- und Beteiligungsbetriebe im Land Bremen gegen solche Attacken treffen. Auch wenn es keine hundertprozentige Sicherheit geben kann, sind eine gute Vorbereitung und präventive Maßnahmen im Bereich der Cybersicherheit entscheidend: Gibt es funktionierende Notfallpläne, klare Zuständigkeiten und eine professionelle IT-Überwachung?

Dabei geht es ausdrücklich nicht darum, einzelne Institutionen oder Personen „an den Pranger zu stellen“, sondern aus vergangenen Vorfällen zu lernen. Grundvoraussetzung dafür ist Transparenz: Wenn es in den letzten Jahren weitere, aus Sicht der Angreifer erfolgreiche Angriffe auf Eigen- und Beteiligungsbetriebe gab, so müssen diese benannt und systematisch ausgewertet werden, um Sicherheitslücken in Zukunft zu schließen. Cybersicherheit ist dabei eine Führungsaufgabe: Der Senat muss klar sagen, wie er in Zusammenarbeit mit den jeweiligen Geschäftsführungen und Verantwortlichen die Eigen- und Beteiligungsbetriebe im Land Bremen schützt, Sicherheitsbehörden einbindet und die Resilienz öffentlicher IT-Strukturen nachhaltig stärkt. Denn die Eigen- und Beteiligungsbetriebe sind ein unverzichtbarer Bestandteil der öffentlichen Daseinsvorsorge in Bremen und Bremerhaven.

Wir fragen den Senat:

1. Wie bewertet der Senat die aktuelle Bedrohungslage durch Cyberangriffe auf Eigen- und Beteiligungsbetriebe (direkte und indirekte Beteiligungsgesellschaften) sowie öffentlich-rechtlich verfasste Unternehmen im Land Bremen (mit Mehrheitsbeteiligung des Landes und/oder seiner beiden Stadtgemeinden) – im Folgenden als „Eigen- und Beteiligungsbetriebe“ bezeichnet?

2. Über welche verbindlichen Notfall- und Krisenpläne (z.B. Incident-Response-Pläne, Wiederanlaufpläne) verfügen diese Einrichtungen im jeweiligen Einzelfall aktuell für den Fall eines schwerwiegenden IT-Sicherheitsvorfalls und wie bewertet der Senat diese?

   a. In welchem Turnus werden diese Notfallpläne jeweils überprüft, aktualisiert und praktisch erprobt (z.B. durch Simulationen, Penetrationstests oder Notfallübungen)?
   b. Welche technischen Maßnahmen zur IT-Sicherheitsüberwachung (z.B. zentrale Log-Analyse, SIEM-Systeme, 24/7-Monitoring) werden bei den Eigen- und Beteiligungsbetrieben im Land Bremen jeweils eingesetzt?

c. Welche organisatorischen Mindeststandards zur Informationssicherheit (z.B. ISMS nach BSI-Grundschutz oder ISO 27001) sind für diese Einrichtungen verbindlich vorgeschrieben und wie wird deren Einhaltung durch wen kontrolliert?

3. Wie ist die Zuständigkeit im Krisenfall geregelt, insbesondere hinsichtlich Entscheidungsbefugnissen, Kommunikationswegen und der Einbindung der politischen Ebene? Inwiefern sieht der Senat hier vor dem Hintergrund bisheriger Erfahrungen ggf. bei der praktischen Umsetzung noch Verbesserungspotenzial?

4. Welche Rolle spielen in diesem Zusammenhang die Polizeien im Land Bremen, die Zentralstelle Cybersicherheit, der CISO und CIO bei der Prävention und Bewältigung von Cyberangriffen, insbesondere im Hinblick auf Beratung, Gefahrenabwehr, Ermittlungen und Koordination mit anderen Behörden?

5. Wie erfolgt die Zusammenarbeit zwischen den Eigen- und Beteiligungsbetrieben, der Polizei und ggf. weiteren Stellen (z.B. CERTs, Landes- oder Bundesbehörden) bei der Erkennung und Behandlung von Cyberangriffen? Inwiefern sieht der Senat hier vor dem Hintergrund bisheriger Erfahrungen ggf. bei der praktischen Umsetzung noch Verbesserungspotenzial?

6. Welche Unterstützungsangebote bestehen für betroffene Eigen- und Beteiligungsbetriebe während und unmittelbar nach einem Angriff, etwa bei forensischer Analyse, Wiederherstellung von Systemen oder rechtlicher Bewertung? Inwiefern wurden und werden diese im Krisenfall tatsächlich in Anspruch genommen?

7. Welche zusätzlichen Maßnahmen plant der Senat, um die Resilienz von Eigen- und Beteiligungsbetrieben im Land Bremen gegenüber Cyberangriffen zu stärken, insbesondere mit Blick auf Personal, Schulungen, Budget und technische Ausstattung?

8. Ist es in den vergangenen zwei Jahren bei Eigen- und Beteiligungsbetrieben im Land Bremen zu Ransomware- oder vergleichbaren Cyberangriffen gekommen, und wenn ja, wann, in welcher Form (z.B. Verschlüsselung, Datenabfluss)? Welche Auswirkungen hatten diese auf die jeweilige Einrichtung und ggf. auf Dritte? Welche Gegenmaßnahmen wurden jeweils mit welchem Erfolg ergriffen?

Beschlussempfehlung:

Simon Zeimke, Marco Lübke, Thorsten Raschen, Dr. Wiebke Winter und Fraktion der CDU