BREMISCHE BÜRGERSCHAFT **Drucksache 21/31**
Landtag
21. Wahlperiode **27. Juli 2023**

Kleine Anfrage der Fraktion der CDU

Wie sorgt der Senat in seinem Verantwortungsbereich für Datensicherheit?

Vor einigen Wochen wurde bekannt, dass bei einem Cyberangriff auf Server der Gesundheit Nord gGmbH (GeNo) in umfangreichem Ausmaß Daten (Patientendaten, Beschäftigtendaten, Daten zu internen Arbeitsabläufen, interne Kommunikationsdaten usw.) kopiert und ins Ausland transferiert wurden. Bei Gesundheitsdaten handelt sich um eine besondere Kategorie von Daten gemäß Art. 9 Abs. 1 Datenschutz-Grundverordnung (DSGVO), an die hohe Schutzanforderungen gestellt werden.

Seit Inkrafttreten der Informationssicherheitsrichtlinie der Freien Hansestadt Bremen (IS-LL) bestehen verbindliche Grundsätze für die Datensicherheit im Verantwortungsbereich des Senats. Sie orientiert sich dabei insbesondere an den Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die u.a. ein IT-Sicherheitskonzept, einen IT-Notfallplan und die Benennung eines Beauftragten für IT-Sicherheit vorsehen.

Immer wieder hat der Landesrechnungshof in den vergangenen Jahren strukturelle Versäumnisse bei der Datensicherheit senatorischer Behörden oder ihrer nachgeordneten Dienststellen festgestellt, z.B. was die Erstellung von IT-Sicherheitskonzepten angeht. Betroffene Behörden waren u.a. das Amt für Straßen und Verkehr, das Statistische Landesamt sowie Immobilien Bremen. Trotz eindeutiger rechtlicher Vorgaben waren dort aufgrund mangelnder Ressourcen oder fehlender Vorgaben der Führungsebene IT-Sicherheitsplanungen nicht im notwendigen Umfang erfolgt. Es bedarf hier eines besseren Bewusstseins für Datensicherheit als Kernaufgabe einer funktionierenden staatlichen Daseinsvorsorge und einer erhöhten Aufmerksamkeit dafür, dass die Beachtung rechtlicher Vorgaben und politischer Zielsetzungen keine Beliebigkeit darstellt und mit der Zuordnung der für die Umsetzung notwendigen finanziellen und personellen Ausstattung in Verbindung stehen muss.

Die Landesdatenschutzbeauftragte mahnt seit Jahren eine Verbesserung der Datensicherheit an und hat u.a. wiederholt die Nutzung ungesicherter Faxverbindungen zur Übermittlung sensibler personenbezogener Daten bemängelt. Auch zeigen vermehrte Datenschutzverstöße im Rahmen der Verarbeitung sensibler Daten zu Impfungen und Infektionszahlen während der Corona-Pandemie, dass Datenschutz gerade bei unvorhersehbaren Ereignissen vielfach nicht im geforderten Maße regulärer Bestandteil eines Arbeitsprozesses ist, sondern erst nachträglich mit einer Korrektur im laufenden Verfahren vollumfänglich Berücksichtigung findet.

Vor dem Hintergrund der in stichprobenhaften Kontrollen deutlich werdenden strukturellen Rückstände erscheint es ratsam, eine übergreifende Bestandsaufnahme der Datensicherheit im gesamten Verantwortungsbereich des Senats einzuholen, um auf dieser Grundlage weiteren Handlungsbedarf auszuloten.

Wir fragen den Senat:

1. Welche (ggf. abgestuften) zentralen Mindestvorgaben/-standards im Bereich der Informations-/Datensicherheit gelten jeweils in den Organisationseinheiten im Verantwortungsbereich des Senats (damit ist hier und im Folgenden gemeint: Kernverwaltung – aufgeschlüsselt nach Ressorts, Dienststellen – sowie Ausgliederungen, Eigenbetriebe, Beteiligungen etc. der Freien Hansestadt Bremen (Land und Stadt))? Wie sind zentrale Verantwortlichkeiten des Informationssicherheitsbeauftragten der FHB und dezentrale Verantwortlichkeiten der Informationssicherheitsbeauftragten voneinander abgegrenzt und wie erfolgt die Koordinierung?

2. Zu welchen Zeitpunkten wurde die IS-LL seit Inkrafttreten einer überprüfenden Revision unterzogen? Wie war jeweils das Ergebnis? Welche Änderungen wurden anschließend jeweils vorgeschlagen, welche beschlossen?

3. Wie viele IT-Sicherheitsbeauftragte sind benannt (bitte aufschlüsseln nach einzelnen Organisationseinheiten im Verantwortungsbereich des Senats., intern oder extern, Vollzeit oder neben anderen Aufgaben (mit welchem Anteil))? In welchen Organisationseinheiten gibt es keine IT-Sicherheitsbeauftragten? Bitte jeweils einzeln für jeden Fall erläutern, warum keine Benennung erfolgt ist.

4. Wie wird die Anforderung aus dem BSI-Grundschutzkompendium, eine Organisationsstruktur für den Sicherheitsprozess aufzubauen, jeweils in den Organisationseinheiten im Verantwortungsbereich des Senats umgesetzt?

5. Welche Organisationseinheiten im Verantwortungsbereich des Senats haben schriftliche Regelungen zur Informationssicherheit mit definierten Kompetenzen und Maßnahmen? In welchen Organisationseinheiten gibt es aus jeweils welchen Gründen keine Regelungen zur Informationssicherheit?

6. Wie werden die Regelungen zur Informationssicherheit in den einzelnen Organisationseinheiten im Verantwortungsbereich des Senats umgesetzt und evaluiert? Wann fand dort jeweils die letzte Fortschreibung/Aktualisierung statt?

7. In welchen Organisationseinheiten im Verantwortungsbereich des Senats existieren jeweils IT-Sicherheitskonzepte? Wann wurden diese zuletzt aktualisiert? Wie werden diese umgesetzt und evaluiert? In welchen Organisationseinheiten existieren jeweils aus welchen Gründen keine IT-Sicherheitskonzepte?

8. In welchen Organisationseinheiten im Verantwortungsbereich des Senats existieren jeweils IT-Notfallpläne? Wann wurden diese zuletzt aktualisiert? Wie werden diese umgesetzt und evaluiert? In welchen Organisationseinheiten existieren jeweils aus welchen Gründen keine IT-Notfallpläne?

9. Wie hoch sind die finanziellen Ressourcen für den Bereich IT-Sicherheit im Verantwortungsbereich des Senats (bitte aufschlüsseln nach Ressorts)? Inwiefern stellt der Senat sicher, dass die Fachressorts für alle Organisationseinheiten in ihrem Verantwortungsbereich ausreichende Ressourcen zur Verfügung stellen, wenn neue Aufgaben im Bereich der IT-Sicherheit an diese übertragen werden?

10. Wie viele Personalstellen sind im aktuellen Haushaltsplan für den Bereich IT-Sicherheit im Verantwortungsbereich des Senats vorgesehen (bitte mit Soll-/Ist-Vergleich nach Organisationseinheiten aufschlüsseln)?

11. Wie schützt der Senat Daten von Mitarbeiterinnen und Mitarbeitern, Bürgerinnen und Bürgern sowie Unternehmen, die der öffentlichen Hand vorliegen, vor dem Zugriff von unbefugten Dritten?

12. Welche Fälle von Cyberangriffen sowie Datendiebstählen gegen Stellen der FHB haben sich seit 2017 ereignet (bitte Überblick über die Lage u.a. mit jährlichen Kennzahlen geben und herausragende Ereignisse gesondert erläutern)?

13. Wie viele Datensätze wurden bei dem Vorfall im Klinikum Bremen-Ost entwendet? Wie viele Patienten sind betroffen? Wann wurde der Datendiebstahl bekannt und wie wurde darauf reagiert? (bitte einzelne Ereignisse/Schritte im Verfahren chronologisch darstellen)? Gibt es zu den mutmaßlichen Tätern bereits Erkenntnisse?

Beschlussempfehlung:

Simon Zeimke, Frank Imhoff und Fraktion der CDU