Antwort des Senats
auf die Kleine Anfrage der CDU
vom 27. Juli 2023

Wie sorgt der Senat in seinem Verantwortungsbereich für Datensicherheit?“

Die Fraktion der CDU hat folgende Kleine Anfrage an den Senat gerichtet:

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?

Der Senat beantwortet die Frage wie folgt:

Vorbemerkung

Die Kleine Anfrage der CDU wird aufgrund des Sicherheitsvorfalls bei der GeNo durch Frage 13 inhaltlich um Aspekte zur Sicherheitsorganisation des gesamten Konzerns Bremen erweitert.

Die Pflicht zur Gewährleistung von Informations- und Cybersicherheit (Datensicherheit) in der öffentlichen Verwaltung werden vom Senat umfänglich anerkannt. Gleichzeitig ist die Verantwortung für die Umsetzung eben dieser grundsätzlich in den jeweiligen Ressorts verortet.

Bei der Beantwortung der Kleinen Anfrage wird daher grundsätzlich unterschieden, zwischen

- dem Verantwortungsbereich des Referats 4Y (IT-Querschnitt und Compliance) beim Senator für Finanzen (im folgenden Textbeitrag)
- und allen übrigen Organisationseinheiten der bremischen Verwaltung (in der Anlage, als Excel Dokument). Aufgrund des Betrachtungszeitraum (beginnend mit 2017) erfolgt die Darstellung der Ressorts, zugeordneten Bereiche und Beteiligungen nicht auf den aktuellen Senatszuschnitt.

Beantwortung der Fragen

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?*

   Eine angemessene Sachverhaltsdarstellung der Vorgaben ist hinsichtlich des Umfangs der Anfrage und der zeitlichen Limitierung eine Herausforderung, da die Implikation *Datensicherheit* grundsätzlich sowohl die Belange von Informations- als auch Cybersicherheit (Zuständigkeit SI) als auch Fragen des Datenschutzes berühren. In der Antwort wird der Schwerpunkt auf die Informationssicherheit gelegt.

   Die für die FHB geltenden Mindestvorgaben für die Informationssicherheit ergeben sich zuvorderst aus *der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung* und dem *Umsetzungsplan* des IT-Planungsrates zur Umsetzung des IT-Staatsvertrags. Dieser Beschluss führte in allen Ländern und beim Bund zu einheitlichen Vorgehensweisen, Handlungsfeldern und zur Orientierung an den Standards des BSI.

   Der Senat hat 2013 in Anerkennung des IT-Planungsrats-Beschlusses den Aufbau eines Informationssicherheitsmanagementsystems für Bremen beschlossen. In 2017 wurde die *Informationssicherheitsleitlinie (IS-LL) der Freien Hansestadt Bremen* vom Senat verabschiedet. Grundsätzlich behandeln das Thema Informationssicherheit – neben der Leitlinie – zahlreiche weitere Gesetze sowie Arbeitsanweisungen, Dienstvereinbarungen u.Ä. wegen des Bezugs zu informationstechnischen Systemen und der beinhalteten Datenverarbeitung.

   Der zentrale IT-Sicherheitsbeauftragte (Chief Information Security Officer (CISO)) beim Senator für Finanzen koordiniert insbesondere die Zusammenarbeit mit den dezentralen Informationssicherheitsmanagements in den Ressorts und wesentlichen Behörden

(Arbeitsgruppe), bearbeitet Sicherheitsvorfälle von herausgehobener Bedeutung, vertritt die FHB in Bund-Länder-Gremien und steuert die sicherheitspolitischen Themen beim zentralen IT-Dienstleister (z.B. Computer Emergency Response Team). Das zentrale Informationssicherheitsmanagement beim Senator für Finanzen ist für die Informationssicherheit der von der FHB vertraglich beauftragten zentralen IKT-Infrastrukturen beim IT-Dienstleister Dataport (einschl. etwaiger Unterauftragnehmer) zuständig.

Die Ressorts und zugeordneten Bereiche können die geltenden Mindestanforderungen aus der FHB IS-LL weiter konkretisieren und im eigenen Verantwortungsbereich spezifische und weitergehende Leitlinien erlassen. Die Ressorts können in ihrem Geschäftsbereich das Informationssicherheitsmanagement übergreifend organisieren oder durch weitere Delegation und Mandatierung in den zugeordneten Bereichen erweitern. Grundsätzlich liegt die Verantwortung für die Informationssicherheit beim jeweiligen Ressort, insbesondere für ihre Fachverfahren und für Verträge mit IKT-Dienstleistern außerhalb der zentralen IKT-Infrastrukturverantwortung.

Um eine sichere und effiziente IKT-Infrastruktur unter den Bedingungen des Fachkräftemangels und angespannter Haushalte zu betreiben, bedient sich der Senat umfänglich seines IT-Dienstleisters Dataport als spezialisierten Infrastrukturbetreiber mehrerer Bundesländer.
Durch die Bündelung von Ressourcen beim Dienstleister Dataport können Kosteneinsparungen und Skaleneffekte realisiert werden. Die zentralisierte IKT-Infrastruktur fördert eine einheitliche IT-Sicherheit und sorgt für schnellen und spezialisierten Support. Der sichere Betrieb von resilienten IKT-Infrastrukturen und Diensten stehen unter der anhaltenden Cybersicherheitsbedrohungslage im Vordergrund dieser strategischen Ausrichtung.
Die bremische Verwaltung standardisiert seit 2012 die IT-Servicemanagementprozesse (ITSM) und erweitert seitdem fortlaufend den Umfang der von Dataport gemanagten Clients, Dienste und Infrastrukturen. Der operative IT-Betrieb wurde und wird dabei aus den dezentralen Einheiten herausgelöst und fortan von Dataport realisiert. Intendierter Teil des ITSM ist auch das operative Informationssicherheitsmanagement, das nunmehr ebenfalls von Dataport – für die von Dataport verantworteten Infrastrukturen und Diensten – wahrgenommen wird.
Dataport Clients und weitere Infrastrukturen in Bremen werden nach den Maßstäben des BSI als „Grundschutzkonform“ betrieben. Die Aufgabenübertragung zielt dabei grundsätzlich auch auf den Betrieb von Fachverfahren ab. Fachverfahren sollen in den BSI zertifizierten Rechenzentren (RZ²) Dataports betrieben werden. Die Verantwortung für die Planung und Steuerung verbleiben hingegen in den Facheinheiten als strategische Aufgabe erhalten.

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?*

Die IS-LL wird anlassbezogen und jährlich einer Revision durch den CISO unterzogen. Für die seit 2017 verabschiedete Leitlinie ergaben sich derzeit noch keine gravierenden Änderungsbedarfe, die berücksichtigt wurden. Die Notwendigkeit dürfte sich im kommenden Jahr abzeichnen, da die europäischen, nationalen und föderalen Rechtsänderungen dies erfordern. Insbesondere handelt es sich dabei um die Umsetzung der NIS-2-Richtlinie (vgl. Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)).

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.*

   Der zentrale IT-Sicherheitsbeauftragte (Chief Information Security Officer (CISO)) der FHB sowie Ansprechpersonen für Informationssicherheit in den Ressorts wurden vom Senat 2013 mit der Vorlage „Informationssicherheitsmanagementsystem“ beschlossen.
   Die aktuelle Anzahl der IT-Sicherheitsbeauftragen neben dem CISO kann für die Ressorts, Dienststellen sowie Ausgliederungen, Eigenbetriebe und Beteiligungen der Anlage entnommen werden.

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

   Das Sicherheitsvorfallmanagement und die entsprechende Organisationsstruktur sind beim zentralen IT-Dienstleister im Zusammenwirken mit den Ressorts und dem CISO etabliert worden. Sicherheitsvorfälle in den bremischen Organisationsbereichen müssen dem CERT-Nord gemeldet werden. Das CERT-Nord untersteht der inhaltlichen und vertraglichen Kontrolle der Kernträgerländer (HB, HH, SH, ST) Dataports. Auf Seiten des IT-Dienstleisters werden die gemeldeten Sicherheitsvorfälle Bremens und die des Dienstleisters im Sicherheitsmanagement bearbeitet und monatlich an den CISO gemeldet, sofern die Dienstleistungen vertraglich bei Dataport bezogen werden. Das CERT ist Teil des Cyber Defense Center (CDC) Dataports und erfüllt zusammen mit dem Security Operation Center (SOC) die Anforderungen des BSI Grundschutzkompendium im Abschnitt Detektion und Reaktion (DER).

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?*

   Der CISO der FHB sowie das zentrale Informationssicherheitsmanagement beim SF haben in Bezug auf die Sicherheit der zentralen informationstechnischen Systeme besondere Befugnisse in Abstimmung mit den Trägerländern Dataports erhalten. Dies betrifft insbesondere Regelaufgaben in der Freischaltungspolitik des Verwaltungsnetzes sowie Notfallmaßnahmen. Besondere Regelungen beruhen auf Beschlusslage des Verwaltungsrates und sind protokolliert. Neben der Benennung als CISO sind keine weiteren schriftlichen Mandate fixiert worden.

   Für die Ressorts wird auf die Antworten in der Anlage verwiesen.

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?*

   Die Regelungen zur Informationssicherheit werden anhaltend fortentwickelt, da das Themenfeld einer dynamischen Entwicklung unterliegt. In Anerkennung der europäi-

schen Richtlinien und deren Umsetzungen in den Mitgliedsstaaten und auf Länderebene wurden zuletzt die Zuständigkeitsbereiche für die Informationssicherheit und die Cybersicherheit durch Senatsbefassung neu definiert.
Grundsätzlich erfolgen Evaluierungen der Umsetzung der Informationssicherheit in Bremen. Erste Umfragen hierzu fanden 2015 (Umfrage mit Excel-Listen), 2017 (Beantwortung mit Hilfe von definierten Antwortbögen) und 2019 (Anforderung von Ressortjahresberichten) statt, die in einem Jahresbericht an den Senat in 2020 mündeten.
Seit 2021 wird der Stand der Informationssicherheit mit Hilfe einer empirischen Studie durch die der Universität Bremen/Ifib jährlich erhoben und dem Senat berichtet.

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?*

   Für die mit dem zentralen IT-Dienstleister Dataport vertraglich geregelten IKT-Infrastrukturen existieren regelmäßig Sicherheitskonzepte und Service Level Agreements auf Basis des BSI Grundschutzes. Sie werden anlassbezogen fortgeschrieben und mit dem Auftraggeber evaluiert, insbesondere bei technischen Änderungen in den Infrastrukturen. Dataport deckt dadurch einen Großteil der Anforderungen ab. Es bleiben naturgemäß Aufgaben (z.B. Schutzbedarfsfeststellungen, Risikoanalysen, Gebäudeinfrastruktur, Zutrittsregelungen) in den Bereichen, die von den beauftragenden Organisationen zu leisten sind.
   Auch für Verträge mit weiteren Dienstleistern ist dies durch die jeweilige beauftragende Organisation sicherzustellen. Hierzu wird auf die Anlage verwiesen.

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?*

   Für die im Verantwortungsbereich des im zentralen Managements befindlichen IKT-Infrastrukturen liegen beim IT-Dienstleister Notfallkonzepte im Rahmen des Grundschutzes vor. Insbesondere in Bezug auf weitergehende Anforderungen eines Business Continuity Managements (Gem. BSI 200-4) sind entsprechende Umsetzungsschritte noch einzuleiten. Weitere Stellungnahmen sind in der Anlage zu finden.

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?*

   Dem zentralen Informationssicherheitsmanagement beim Senator für Finanzen stehen im Rahmen des Haushaltsvollzugs des Produktplans 96 jährlich geplante Haushaltsmittel in Höhe von 350T€ (in 2023) zur Verfügung. Insbesondere werden hiermit die zentralen Aus- und Fortbildungsmaßnahmen, das CERT-Nord bei Dataport, Sicherheitsmaßnahmen des gemanagten Clientbetriebs sowie Beratungsleistungen finanziert. Die für Informationssicherheit bei Dataport notwendigen finanziellen Ressourcen für IKT-Infrastrukturen und Dienste sind in den Betriebskosten inkludiert. Insoweit finanzielle Mittel in den Ressorts explizit den Ausgaben für Informationssicherheit zuzurechnen sind, enthält die Anlage zu Frage 9 diese Angaben.

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)?*

    Für das zentrale Informationssicherheitsmanagement ist neben der Personalstelle für den CISO eine weitere Stelle vorgesehen (insgesamt 2 VZÄ). Dies entspricht den Planungen. Insoweit Personalstellenanteile in den Ressorts explizit der Informationssicherheit zuzurechnen sind, enthält die Anlage zu Frage 10 diese Angaben.

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?*

    Für zentrale IKT-Infrastrukturen werden angemessene Maßnahmen zum Schutz der Beschäftigten-, Bevölkerungs- und Unternehmensdaten getroffen. Insbesondere werden Maßnahmen auf dem „Stand der Technik“ mit dem Dienstleister geplant, mit den zuständigen Gremien vereinbart und umgesetzt. Weiterhin stellt das zentrale IT- Servicemanagement mit dem zentralen IT-Dienstleister und zusammen mit dem Informationssicherheitsmanagement eine strukturierte Vorgehensweise zur Erhöhung der Resilienz dar. Aktuelle und flächendeckende Investitionen in die Infrastrukturen der Bremischen Verwaltung werden entlang von Anforderungen des BSI-Grundschutzes geplant und umgesetzt.

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)?*

    Die Anzahl von Cyberangriffen auf die Öffentliche Verwaltung und ihre Abwehr ist Teil der Berichterstattung gegenüber dem zentralen Informationssicherheitsmanagement. Erfolgreiche Angriffe gegen die Infrastrukturen Bremen sind bislang beherrschbar geblieben und konnten gemeinsam mit dem IT-Dienstleister abgearbeitet werden. Folgende Auflistung ist seitens des IT-Dienstleisters mit Stand vom 31. Juli 2023 zur Verfügung gestellt worden:

    2017
    - Vorfälle Schadcode auf Clients/Spam-Mails/Link in Phishing/Spam-Mail geklickt: 15
    - Infizierter Rechner: 1
    - Dieser Rechner wurde eingezogen und ersetzt. Keine Erkenntnis über Datenabfluss.

    2018
    Seit Ende 2018 ist der Schadcode „Emotet“ aktiv:
    - Vorfälle Schadcode auf Clients: 39
    - Von Virenscanner entfernt/Abwehr durch weitere Mechanismen: 38
    - Datenfluss nach Emotet-Infektion: 1
    - Das betroffene Gerät musste neu aufgesetzt werden, höchstwahrscheinlich Postfachdaten abgeflossen.

    In 2018 gab es mehrere Scareware-Ereignisse.
    Meist ist nach Aufruf einer verseuchten Webseite der Bildschirm blockiert und der Nutzer soll eine kostenpflichtige Telefonnummer zu Abhilfe anrufen. Der UHD konnte die Blockade aufheben, danach wird das System per FullScan mit dem Virenschutz geprüft.
    - Vorfälle mit Scareware: 6

2019
Emotet:

- Vorfälle Schadcode auf Clients: 23
- Von Virenscanner entfernt/Abwehr durch weitere Mechanismen: 10
- Datenfluss nach Emotet-Infektion: 13
- Die betroffenen Geräte mussten neu aufgesetzt werden, höchstwahrscheinlich Postfachdaten abgeflossen.

Weitere:

- SCAM: 1 Fall (SCAM: Erpressungsversuch ohne reale Hintergründe)
- Verschlüsselung eines Clients und von Daten auf einem Gruppenlaufwerk (auf dem der Auslösende gültige Schreibberechtigungen hatte) durch GranCrab
  Schaden: betroffener Client musste neu aufgesetzt werden, Daten im Gruppenlaufwerk und im Home-Laufwerk des Auslösenden wurden aus der Sicherung wiederhergestellt. Geringer Datenverlust zwischen Zeitpunkt Sicherung und Verschlüsselung
- DDoS-Angriff auf öffentliche IP-Adresse: Zeitweise Probleme mit Erreichbarkeit

2020
In 2020 gab es größere Zahlen von „Erfolgreicher Installation von Schadcode“, vor allem bedingt durch die Schadsoftware Emotet. In der Regel bedeutet eine erfolgreiche Installation, dass der Anwender in einer Mail den Link geklickt hat und dann den Download von Schadsoftware gestartet hat. Der Aufruf von entsprechenden verdächtigen Seiten (über IoCs = Indicator of Compromise) wurde durch Auswertung von Proxy-Logs ermittelt, anschließend wurden die Clients überprüft. In der Regel haben weitere Absicherungsmechanismen (App-Locker) auf den von Dataport verwalteten Clients die weitere Installation von Schadcode verhindert. Betroffene Clients wurden geprüft und bereinigt oder ggf. neu aufgesetzt. In einem Fall wurde ein Datenabfluss bekannt.
Emotet:

- Vorfälle Schadcode auf Clients: 34
- Datenabfluß nach Emotet-Infektion: 1
  Das betroffene Gerät mussten neu aufgesetzt werden, höchstwahrscheinlich Postfachdaten abgeflossen.
- Drohanruf an einer Schule in Bremen.

2021
In 2021 gab es einen Fall von Datenabfluss (Emotet Angriff), nach den Recherchen dürfte der Abfluss aber nicht im von Dataport verwalteten Bereich der FHB erfolgt sein, sondern ist wahrscheinlich in einer Anwaltskanzlei erfolgt).
Weiterhin gab es wieder eine einstellige Zahl von Phishing-Mails, die aber keine Auswirkungen zeigten.

- Mail-Adresse im Rahmen von Mailspoofing missbraucht, Datenabfluss wahrscheinlich bei Anwaltskanzlei.
- Betrugsversuch mit Faxnummer des Amtsgerichts Bremerhaven, Call-ID Spoofing durch Dritte
- SCAM/Erpressermail an Mitarbeiterin der FHB
- Phishing Mail
- Phishing Mail
- Verdächtige Webseite (Vorspiegelung Schadcode)

2022
In 2022 gab es keine Fälle von Datenabfluss im von Dataport verwalteten Bereichen der FHB. Nach Auswertung der Meldungen in der ITSM Suite gab es 11 Fälle von potentiellen Schadcodeereignissen, das waren vor allem SPAM/Phishingmails. Die Schutzmechanismen haben gegriffen (Nutzer hat Bedrohung erkannt, Ausführung

durch Applocker verhindert, Links nicht mehr aktuell). In allen gemeldeten Vorgängen gab es keinen Datenabfluss oder Schaden am Endgerät.

- 3 Mails, die Links zu Schadcode enthielten, sind in der Landeshauptkasse Bremen eingegangen. Es erfolgte keine Infektion, die Rechner wurden geprüft. Die E-Mails wurden wahrscheinlich bei Geschäftspartnern (nicht in der FHB!) durch eine Emotet Infektion abgezogen.
- SCAM/Erpressermail
- Nutzer erhält SMS mit Link zu Schadcode, Infektion wahrscheinlich durch schlechte Anbindung verhindert.
- 2 x Spam/Phishing Mail
- Trellix meldet Bedrohungsereignisse, Prüfung durch SOC
- Spam/Phishing Mail
- 2 x Spam/Phishing Mail
- Spam/Phishing Mail

2023

In 2023 sind mehrere Spamkampagnen zu verzeichnen.

- Spam Bremerhaven, kein Datenabfluss
- Spam Behörden, kein Datenabfluss
- Möglicher DDOS auf www.bremenports.de (weitere Informationen liegen bei CERT Nord nicht vor)
- Spam Behörden, kein Datenabfluss
- DDOS auf Webseite www.polizei.bremen.de.
  Beginn 04.04., 08:06 Uhr, Ende 05.04., gegen 12:40 Uhr.
  Gegenmaßnahme ab 09:21 Uhr (04.04.) mit Filterregel
  Einschränkung der Verfügbarkeit der Webseite. Kein Datenabfluss.

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?*

Zur Beantwortung verweisen wir auf die folgende Stellungnahme der Senatorin für Gesundheit, Frauen und Verbraucherschutz in Abstimmung mit der Landesbeauftragten für den Datenschutz und Informationsfreiheit:

„Am 10.05.2023 hat die Gesundheit Nord (GeNo) einen externen Hinweis erhalten, dass Daten abgeflossen sind. Insgesamt wurden bei dem Cyberangriff Daten im Umfang von 285 GB / 218 GB kopiert (die GB-Werte beziehen sich auf zwei unterschiedliche Messpunkte; die Differenz ergibt sich aus Metadaten, wiederholten Kopierversuchen und doppelten Kopien). Wie viele Datensätze davon patientenbezogen sind, lässt sich nicht genau quantifizieren. Unmittelbar nach Bekanntwerden des Vorfalls hat die GeNo Gegenmaßnahmen eingeleitet. Gegen 14:00 Uhr wurden die für den Angriff genutzten Server abgeschaltet. Um 19:15 Uhr wurde die GeNo komplett vom Internet getrennt und um 21:00 Uhr wurde die Firma Mandiant mit Incident Response Maßnahmen beauftragt, mit denen die GeNo sich mindestens einmal täglich abgestimmt hat. Folgend wurde die Aufsichtsratsvorsitzende, die Landesbeauftragte für Datenschutz und Informationsfreiheit und das Bundesamt für Sicherheit und Informationstechnik informiert. In den darauffolgenden Tagen erfolgte eine enge Zusammenarbeit mit der CyberCrime-Abteilung der Bremer Polizei. Ab dem 14.05.2023 wurde ein strukturierter „Back to new normal“-Prozess eingeleitet, der die Sicherstellung des Krankenhaus-Betriebes und die Stärkung der Resilienz umfasste. Die GeNo erstellte eine Liste mit Diensten, die für die Patientenversorgung und den Unternehmensbetrieb erforderlich waren. Die Liste wurde täglich neu priorisiert. Mit den betroffenen Fachbereichen

wurde regelhaft kommuniziert und es wurde über den GeNo-Newsletter informiert. Am 28.06.2023 wurde das „new normal“ erreicht und es erfolgte die Re-Aktivierung der Internet-Kommunikation für die Beschäftigten. Begleitend dazu wurde eine „Managed Defense“-Lösung eingerichtet, sodass die IT-Infrastruktur der GeNo rund um die Uhr von Experten überwacht und bei Auffälligkeiten umgehend reagiert wird. Insgesamt wird die IT-Infrastruktur mit verschiedenen Maßnahmen schrittweise weiter gehärtet (Vereinheitlichung der Antivirus-Umgebung, Anpassung des Regelwerks von SIEM, IPS und DLP, Konzernweiter Passwort-Reset etc.). Zu den mutmaßlichen Tätern liegen der GeNo keine genauen Erkenntnisse vor.“

Anlage:
FHB-Konzernübersicht-Datensicherheit – nicht öffentlich.

Beschlussempfehlung:

Die Bürgerschaft (Landtag) nimmt von der Antwort des Senats auf die Kleine Anfrage Kenntnis.