BREMISCHE BÜRGERSCHAFT **Drucksache 21/778**
Landtag **(zu Drs. 21/717)**
21. Wahlperiode **1. Oktober 2024**

Mitteilung des Senats

Der Druck wächst – wie ist die aktuelle Cybersicherheitslage in Bremen und welche Aufgaben übernehmen Bremens IT-Dienstleister?

Kleine Anfrage
der Fraktion FDP vom 08. Mai 2024
und Mitteilung des Senats vom 01.10.2024

Vorbemerkung der fragenstellenden Fraktion:

Das fehlerhafte Update einer IT-Security-Lösung des Herstellers Crowdstrike am 19. Juli 2024 hat gezeigt, dass es bei IT-Sicherheitsmaßnahmen zu schwerwiegenden und teuren Problemen kommen kann. Dieser Vorfall führte zu Systemabstürzen bei geschätzt 8,5 Millionen Windows-Geräten weltweit und hat nach ersten Schätzungen zu Versicherungsschäden in Höhe von 1,5 Milliarden Dollar geführt. Vor diesem Hintergrund stellt sich die Frage, ob es hierdurch auch im Land Bremen zu Schäden kam.

Hinzu kommt die regelmäßige Berichterstattung der Presse über Cyberangriffe auf Behörden, Infrastruktur und Unternehmen in Deutschland und Bremen. In jüngster Zeit beispielsweise am 27.07.24 über einen Angriff auf das Handelsunternehmen Melchers am 02.06.24 über gestohlene Patientendaten bei der Geno oder am 11.04.24 über einen Hackerangriff auf die Lürssen-Werft.

Der Senat beantwortet die Fragen wie folgt:

Vorbemerkung:
Die nachfolgenden Antworten betreffen sowohl die Einrichtungen der FHB als auch in Teilen auch Beteiligungsgesellschaften, externe Dienstleister sowie Dataport als zentralen IT Dienstleister des Landes. Für die Stadt Bremerhaven hat diese Rolle der Eigenbetrieb bit.
Die IT-Dienstleister haben – auch unter Verweis auf Betriebsinterna – unterschiedlich detailliert zu den Fragen Stellung genommen, die ihnen vom Senat respektive dem Magistrat gestellt wurden.
Dazu beteiligt haben sich auch Einrichtungen, die gegenüber anderen Verwaltungseinrichtungen IT-Dienstleistungen erbringen.

Insbesondere wurde 2006 das Kompetenzzentrum zur Gestaltung der Informationssysteme (KOGIS) gegründet und das KOGIS-Baukasten-System als Content Management System (CMS) für die Internet- und Intranet-Auftritte der Kernverwaltung verpflichtend vorgeschrieben. Derzeit werden circa 300 Internet- und Intranet Auftritte mit dem KOGIS-Baukasten umgesetzt und auch zentrale Plattformen wie das Serviceportal und das Transparenz- und Gesetzesportal Bremen nutzen das KOGIS-CMS.

1. **In welchen Behörden, öffentlichen Trägern und öffentlichen Unternehmen wird Crowdstrike eingesetzt?**

Die Einrichtungen und Dienststellen der bremischen Verwaltung setzen Produkte der Crowdstrike nicht ein. Auch der Magistrat der Stadt Bremerhaven und sein IT-Dienstleister „bit“ setzen Crowdstrike nicht ein.

2. **Gab es im Zusammenhang mit den durch das Crowdstrike hauseigene Softwareprodukt Falcon Sensor verursachten weltweiten Computerausfällen im Juli 2024 auch Auswirkungen auf Bremen?**
    a. **Wenn ja, welche?**
    b. **Sofern es zu Schäden gekommen ist, wie hoch sind diese?**
    c. **Welche Vorkehrungen werden für solche Fälle getroffen?**
    d. **Wie war die Reaktionskette, wie war der Ablauf?**
    e. **Gab es Fälle von indirekter Betroffenheit, z.B., dass Dienstleister nicht verfügbar waren?**
    f. **Welche Aufgabe hatte Dataport in diesem Zusammenhang?**

In diesem Zusammenhang hatte Dataport die Aufgabe, eine Betroffenheit von Verfahren oder Infrastrukturen, die Dataport im Auftrag der FHB betreibt, zu prüfen. Es lag keine Betroffenheit vor. Auch insgesamt lag keine Betroffenheit von Einrichtungen der FHB vor. Das Gleiche gilt für den Magistrat der Stadt Bremerhaven.

3. **Wie schätzt der Senat die aktuelle Bedrohungslage im Hinblick auf Cyberkriminalität und Cyberspionage in Bremen ein?**

Die Bedrohungslage in Deutschland und im Lande Bremen durch Cyberaktivitäten – sowohl der Cyberspionage als auch der Cybersabotage – ist unverändert hoch. Es ist davon auszugehen, dass Kritische Infrastrukturen, insbesondere Logistik- und Rüstungsunternehmen sowie Hochtechnologieunternehmen besonders gefährdet sind.

Das Eskalationspotenzial im Cyberraum durch russische Akteure befindet sich vor dem Hintergrund des Angriffskriegs gegen die Ukraine auf einem hohen Niveau. Darüber hinaus ist anzumerken, dass neben den russischen Akteuren auch weitere fremde staatliche Akteure Cyberaktivitäten gegen bremische Unternehmen aus den o.g. Sektoren entfalten.

Daneben ergeben sich weitere Bedrohungspotenziale durch z. B. Cyberkriminalität und Hacktivismus (siehe hierzu auch: Bundesamt für Sicherheit in der Informationstechnik „Die Lage der IT-Sicherheit in Deutschland 2023“), welche als Ziele den Staat, die Wirtschaft und die Gesellschaft gleichermaßen adressieren.

4. **Wie hoch ist das Budget, das aktuell jährlich insgesamt für die Informations- und IT Sicherheit aufgewendet wird und wie hat sich dieses Budget seit der letzten großen Anfrage zur Lage der Cybersicherheit in der Freien Hansestadt Bremen entwickelt (Bitte insgesamt und nach Ressort aufgeschlüsselt angeben)?**

Im Allgemeinen gibt es keine gesondert ausgewiesenen Sicherheitsbudgets auf Ressortebene. Ein Großteil der IT-Systeme werden von Dataport verwaltet. Dort wird auch die Sicherheit der IT-Infrastrukturen aufrechterhalten.
Zentral existiert für den Chief Information Security Officer (CISO) des Landes ein zentrales Budget auf einem SAP Innenauftrag in Höhe von 180T€ in 2024 und 350T€ in 2023.

Einzelne Ressorts und Einrichtungen weisen Budgets für einzelne Maßnahmen aus:

SBMS plant für das Ressort 5-8T€, für das ASV 8T€ und GEO 30T€ jeweils ein.

SWHT:
Für das Informationssicherheitsmanagement stehen 65T€ zur Verfügung. Das Budget hat sich seit 2022 nicht verändert.

Zugeordnete Einrichtungen bzw. Gesellschaften des Ressorts:

- Flughafen bisher 30T€, ab 2025: 80T€
- BLG > 1 Mio. €
- WFB/BAB – Intensivierung der Anstrengung an die laufende Entwicklung 2022 9% des IT Budgets /2024 16% des IT Budgets
- M3B: IT-Budget für Themen der IT-Sicherheit ca. 88 T€

SJV

Im Bereich Personal sind bei der Senatorin für Justiz und Verfassung derzeit 1,3 VZÄ (Stellenanteile) ausschließlich für den Bereich Informations- und IT-Sicherheit zuständig. Zum einen wurde bei der IT-Stelle Justiz die Stelle einer Informationssicherheitskoordinatorin (EG13) geschaffen, die sich mit 1,0 VZÄ übergreifend um sämtliche Informations- und IT-Sicherheitsthemen kümmert. Zum anderen gibt es bei der Staatsanwaltschaft Bremen zwei Sonderdezernate "Internet-Kriminalität" mit einem Pensum von jeweils 0,15 VZÄ (R1), insgesamt also 0,3 VZÄ (R1) in denen Cybercrimestraftaten im engeren Sinne verfolgt werden.

In der letzten großen Anfrage der Fraktion der FDP 09/2022 („Änderung der Bedrohungslage in der Cybersicherheit: Bremische IT in Großkrisenlagen“) fand zum (Personal-)Budget keine Abfrage statt, so dass zum Vergleich der Zeitpunkt der davor zuletzt erfolgten großen Anfrage der Fraktion der FDP 12/2018 („Cybersicherheit in Bremen“) gewählt wird. Damals waren im Bereich Personal bei der Senatorin für Justiz und Verfassung 0,5 VZÄ ausschließlich für den Bereich Informations- und IT-Sicherheit zuständig. Hierbei handelte es sich um zwei Staatsanwälte mit einem Sonderdezernat "Internet-Kriminalität" mit einem Pensum von jeweils 0,25 VZÄ.

Zudem werden u.a. im Rahmen der SSLAs beim Verfahrensbetrieb bei Dataport, aber auch im Rahmen der Software(weiter)-entwicklung in den Verbünden, auch Kosten für IT-Sicherheit aufgewendet.

Eigenbetrieb Performa Nord: Die Kosten belaufen sich jährlich auf ca. 400T€.

Eigenbetriebe des Senators für Kultur:
Volkshochschule (VHS): Jährliches Gesamtbudget ca. 40T €
Stadtbibliothek (Stabi): Jährliches Gesamtbudget ca. 30T€
Stiftungen ö. R.:
Überseemuseum: Für die Anschaffung von Virenscanner und Backups sind jährlich 6T€ eingeplant.
Das Focke-Museum gibt jährlich 14T€ für IT-Überwachung aus.
Beteiligungen:
Theater Bremen: ca. 13T€
Bremer Philharmoniker: ca. 1,5T€

BHV. Über die Magistratskanzlei steht dem bit in 2-Jahres-Zeiträumen ein Budget in Höhe von ca. 7T€ für Penetrationstest zur Verfügung. Seit der letzten Anfrage hat der bit seine bisherige Vorgehensweise (Einkauf von sog. Pen-Tests) auf ein kontinuierliches Screening mit einer eigens dafür angeschafften Software umgestellt. Mithin sind die Personalausgaben deutlich gestiegen, lassen sich gegenwärtig aber noch nicht konkret quantifizieren.

5. **Wie viele Fälle von Cyberangriffen gab es in der Freien Hansestadt Bremen seit der letzten großen Anfrage zur Lage der Cybersicherheit (Bitte nach Jahren sowie nach Angriffszielen (kritische Infrastruktur, Behörden, Wirtschaft) aufschlüsseln)?**

Das Kriminalitätsphänomen „Cybercrime“ (i.w.S.) beschreibt eine Vielzahl unterschiedlicher Delikte, welche verschiedene Deliktsbereiche tangieren können. Auf Grundlage der Daten der bundeseinheitlichen Polizeilichen Kriminalstatistik (PKS) sind im Erfassungszeitraum von 01.01.2022 bis einschließlich 31.12.2023 2.972 und 3.473 Taten zum Phänomen „Cybercrime“ erfasst worden.

Es wurden folgende Straftatenschlüssel berücksichtigt:
511120 Betrügerisches Erlangen von Kfz § 263a
511212 Weitere Arten des Warenkreditbetruges § 263a
516300 Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN
516520 Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten
516920 Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel

517220 Leistungskreditbetrug § 263a StGB
517500 Computerbetrug (sonstiger)
517900 Missbräuchliche Nutzung von Telekommunikationsdiensten
518112 Abrechnungsbetrug im Gesundheitswesen § 263a StGB
518302 Überweisungsbetrug § 263a StGB
543000 Fälschung beweiserheblicher Daten, Täusch. im Rechtsverkehr bei Datenverarbeitung
543010 Fälschung beweiserheblicher Daten
543020 Täuschung im Rechtsverkehr bei Datenverarbeitung
674200 Datenveränderung, Computersabotage
674210 Datenveränderung
674220 Computersabotage
678000 Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei
678010 Ausspähen von Daten gemäß § 202a StGB
678020 Abfangen von Daten gemäß § 202b StGB
678030 Vorbereiten des Ausspähens und Abfangens von Daten
678040 Datenhehlerei
897000 Cybercrime
897100 Computerbetrug § 263a StGB

Im polizeilichen Kontext ist der Terminus „Cyberangriff“ nicht definiert. In Anlehnung an das BKA-Lagebild Cybercrime und weitere mediale Veröffentlichungen werden unter „Cyberangriff“ jene ausgewählten Straftaten verstanden:

Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung (Straftatenschlüssel 543000) (208 Fälle), Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen und Datenhehlerei (Straftatenschlüssel 678000) (194 Fälle) und Datenveränderung, Computersabotage (Straftatenschlüssel 674200) (22 Fälle).
In Anbetracht der dargestellten Operationalisierung wurden im betrachteten Zeitraum von August 2022 bis einschließlich 31.12.2023 insgesamt 424 Cyberangriffe identifiziert. Die Datenlage bezieht sich auf alle erfassten Strafanzeigen und unterscheidet nicht zwischen Privatpersonen und Unternehmen. Anzumerken ist, dass Unternehmen oder Institutionen häufig durch Verschlüsselung / Erpressung (Ransomware) betroffen sind, welche als Grunddeliktsform nicht unter der PKS-Auflistung Cybercrime subsumiert wird. Für 2023 wurden sieben Ransomware-Fälle identifiziert, aus den Vorjahren liegen insoweit keine nachvollziehbaren Daten vor. Die Erfassung des Phänomens Ransomware ist in der PKS erst seit dem 01.01.2024 verpflichtend, was zukünftig zu einer besseren Datenlage führen wird.

Eine Unterscheidung von betroffenen Unternehmen oder Institutionen nach Bedeutung findet in den polizeilichen Verarbeitungssystemen nicht statt, wodurch eine entsprechende Detailzuordnung nicht möglich ist.

a) Soweit bekannt, welche Beeinträchtigungen und welche Schäden wurden durch diese Angriffe verursacht?

Die Beeinträchtigungen müssen abhängig vom betroffenen Unternehmen betrachtet werden, da es vereinzelt zu langwierigen Produktions-/Nutzungsunterbrechungen durch Verschlüsselung der IT-Infrastrukturen (kein Zugriff möglich) oder eigene Abschaltung von externen Zugängen (wie Internetverbindung) zum Schutz und Bereinigung der IT-Infrastruktur kommen kann. Weiterhin kann es zwischenzeitlich als Standard angesehen werden, dass einer täterseitigen Verschlüsselung ein Datenabfluss von internen Informationen vorausgeht.
Im Betrachtungszeitraum wurde für den Summenschlüssel Cybercrime eine Schadenssumme von insgesamt 3.446.887 Euro festgestellt. Hierbei gilt zu beachten, dass für Cybercrime-Delikte in der PKS nur Schäden aus dem Bereich Computerbetrug § 263a StGB erfasst werden. Finanzielle Schäden, die etwa durch cyberspezifische Erpressungsdelikte oder durch damit einhergehenden Produktionsausfälle bei Unternehmen entstehen, fließen nicht in die Cybercrime-Schadenssumme ein.
Gemäß dem BKA-Lagebild Cybercrime werden 205,9 Milliarden Euro als bundesweiter Gesamtschaden für 2023 angegeben.

Im Geschäftsbereich von SGFV ist im Zusammenhang mit dem Abfluss von Daten aus dem GeNo-Netzwerk ein Schaden i.H.v. 185T€ entstanden.

Bei den KOGIS Systemen fanden seit 2019 acht DDOS Attacken sowie vier Versuche statt, KOGIS für SPAM zu missbrauchen. Es fand eine Verlangsamung der Systeme statt.

b) Wie viele Täter konnten im Zusammenhang mit diesen Angriffen ermittelt werden?

Da, wie bereits unter Frage 5 dargestellt, der Begriff „Cyberangriff“ im polizeilichen Kontext nicht definiert ist, wurde sich bei der Erhebung der Anzahl der Tatverdächtigen auf die in der PKS erfassten Straftaten des Phänomens Cybercrime (i.w.S.) berufen.
Danach wurden im Land Bremen im Zeitraum 01.08.2022 bis einschließlich 31.12.2023 insgesamt 4.283 Straftaten mit insgesamt 317 Tatverdächtigen erfasst.

BHV: Seit der letzten großen Anfrage im Jahr 2022 wurden keine Fälle nach § 303a StGB sowie § 303 b StGB bei der Ortspolizeibehörde Bremerhaven angezeigt.

~~c)~~ Wie viele Täter wurden im Zusammenhang mit diesen Angriffen bereits verurteilt?

Dem Senat sind in diesem Zusammenhang keine Verurteilungen bekannt.

6. Wie viele Fachkräfte, die sich hauptsächlich mit der Abwehr von Cyberangriffen beschäftigen stehen der Bremer Polizei zur Verfügung, wie hat sich diese Zahl entwickelt und wie hoch ist das jährliche finanzielle Budget (Bitte die Entwicklung über die letzten 5 Jahre aufgeschlüsselt angeben)?

Aus der Abteilung Informations- und Kommunikationstechnik (Z 4) der Polizei Bremen sind einschließlich Führungskräften derzeit 42 Mitarbeiter:innen dem IT-Betrieb zuzurechnen. Hinzu kommen weitere 14 Funktionsstellen in diesem Bereich, die aktuell vakant sind. Von diesen 42 Mitarbeiter:innen sind drei Mitarbeiter:innen für das Informationssicherheitsmanagement und ein Mitarbeiter im engeren Sinne im Bereich Cybersicherheit tätig. Die Polizei

Bremen verfügt über kein separates Budget für Cyber- und Informationsmanagement.

BHV: Die IT-Infrastrukturen der Ortspolizeibehörde Bremerhaven sind vernetzter Bestanteil der Infrastrukturen der Stadt Bremerhaven, der Polizei Bremen in Kombination mit Dataport und den Verbünden auf Landes- und Bundesebene.

Für den IT-Betrieb im weiteren Sinne sollen bei der OPB Bremerhaven planmäßig 15 VZÄ zum Einsatz kommen. Derzeit sind davon 9,5 Stellen besetzt.

Für die Abwehr von Cyberangriffen steht der OPB kein explizites Budget zur Verfügung. Daher kann dazu keine Aufschlüsselung erfolgen. Zur Umsetzung der notwendigen Maßnahmen werden dem IT-Betrieb finanzielle Mittel im Zuge der jährlichen Investitionen nach Priorisierung zur Verfügung gestellt."

7. **Wie entwickelte sich die Anzahl der IT-Mitarbeiterinnen und Mitarbeiter bei den zentralen IT-Dienstleistern des Landes Bremen seit der letzten großen Anfrage zur Lage der Cybersicherheit in der Freien Hansestadt Bremen (Bitte aufgeschlüsselt nach Dienstleister und Positionen inkl. Funktion)?**

Für die FHB ist nur Dataport als zentraler IT-Dienstleister des Landes zu kategorisieren. Dazu liegen folgende Angaben vor:

Mitarbeitende gesamt (in Köpfen, interne aktive MA ohne Azubis):
- 2022: 4.615; davon haben 64% in IT-Positionen gearbeitet
- 2023: 5.256; davon haben 63% in IT-Positionen gearbeitet

Zu den IT-Positionen zählen IT-Administratoren, IT-Berater, IT-Sicherheit, Software-Architekten, Software-Entwickler sowie Tester.

BHV:
Seit der Anfrage in Q3 2022 wurde eine Stelle für IT-Sicherheit beim Betrieb für Informationstechnologie (bit) geschaffen.
Ferner stehen mit Genehmigung des Haushaltes (inkl. Stellenplan) 2024 weitere 14,5 neue Stellen im IT-Bereich zur Verfügung.

8. **Wie viele Stellen sind bei den Dienstleistern derzeit vakant (Bitte insgesamt sowie aufgeschlüsselt nach den Personalbedarfen der Dienstleister angeben)?**

Über die Zahl der vakanten Stellen kann nach Aussage des Personalbereiches von Dataport keine Auskunft erteilt werden.

BHV/bit:
Aktuell sind 3,5 Stellen vakant und befinden sich in der Ausschreibung.

Mit Genehmigung des Haushalts 2024 kommen weitere Stellen dazu (Beschluss im Personal- und Organisationsausschuss vom 30.01.2024). Somit ergibt sich eine Vakanz von insgesamt 18 Stellen (14,5 neu).

Angaben zu weiteren Dienstleistern liegen dem Senat nicht vor.

9. **Wie viel Budget wird von den Dienstleistern für die Informationssicherheit und IT-Sicherheit eingeplant (Bitte um Angaben über das Budget für das IT-Personal insgesamt insbesondere mit Angaben zum Budget für das IT-und Informationssicherheitspersonal und ebenfalls zum Budget für die technische IT-**

Sicherheitsausstattung der Dienstleister sowie nach Dienstleister aufgeschlüsselt)?

Dataport investiert rund 10% des Umsatzes in IT-Sicherheit.

Ansonsten liegen keine Angaben der Dienstleister vor.

bit:

- Personal 2024: ~ 400T€ / jährlich für 1x Informationssicherheitsbeauftragte (ISB) und 3x IT-Sicherheitsteam
- Personal 2025: ~ 570T€ / jährlich für 3x ISB und 3x IT-Sicherheitsteam

Informationssicherheitsmanagementsystem (ISMS) Aufwände 20T€ jährlich
Jährliche Aufwände für IT-Sicherheitssysteme 250T€, dazu gehören u. a.:
für Schwachstellenscanner, E-Mail-Scanner, Virenschutz, DDoS-Schutz und Firewall.

10. **Wie genau und wie regelmäßig erfolgt die Überwachung und Reaktion auf Sicherheitsvorfälle bei den unterschiedlichen IT-Dienstleistern und welche Reportinglines wurden von der Freien Hansestadt Bremen durch welche in der Verantwortung stehende Person organisiert? (Bitte bei der Beantwortung der Fragen sowohl die Anzahl der Mitarbeiterinnen und Mitarbeiter im IT-Sicherheitsteam und deren berufliche Qualifikation ein als auch die Tools/Werkzeuge und Prozesse angeben, die zur Überwachung bei den Dienstleistern eingesetzt werden.**

Dataport hat einen Prozess zu Sicherheitsvorfallbearbeitung mit definierten Meldewegen zu den Kunden. Dieser Prozess wird bei Dataport durch die Software BMC Remedy unterstützt.

FHB: Alle Ressorts und der Magistrat erhalten vom Warn- und Informationsdienst CERT-Nord bei bekannten Sicherheitslücken eine entsprechende Information. Bei Bekanntwerden von Sicherheitslücken werden diese umgehend geschlossen. Routinemäßig werden auf Server und Clients die monatlichen Patches eingespielt, bei erhöhtem Sicherheitsrisiko geschieht dieses unverzüglich.

Im Bereich von SWHT gibt es hierzu folgende Maßnahmen:
BAB und WFB und M3B:
Regelmäßigkeit : 24/7 Betriebs- und SIEM Monitoring Reportinglines: Abhängig von Vorfallsart Geschäftsführung, Stabs- und Abteilungsleitungen, Datenschutz, Risikomanagement Cyberversicherung, Cybercrime LKA Polizei, Unternehmenskommunikation, hinzu kommen ggf. BSI und BaFIn IT-Sicherheitsteam: 5 VZÄ (WFB/BAB/M3B)
Kundenportal BAB ergänzend über vordefinierte UseCases im DL SIEM/SOC

IT-Sicherheitsteam: 5 VZÄ (WFB/BAB/M3B)
Dienstleister werden über Kennzahlen / Reporting-Ansätze überwacht.

Eigenbetriebe im Ressortbereich des Senators für Kultur:

- Volkshochschule: Geplant ist eine Dienstleistersteuerung bei der in regelmäßigen Abständen die Umsetzung der Anforderungen an die IT-Sicherheit der Bremer VHS geprüft wird. Derzeit haben unsere Dienstleister eine Kontaktmöglichkeit zur Meldung von Sicherheitsvorfällen in Form von Telefon und E-Mail. In Verantwortung ist unser externer IT-Sicherheitsbeauftragter von Datenschutz Nord. Qualifikationen des ISB sind ISO 27001 Auditor, IT-Grundschutz, IT-GS-Praktika sowie mehrjährige Erfahrung in der Beratung von zertifizierten ISMS. ISMS-Team in der VHS vorhanden. Risikoanalyse mit Betrachtung der IT-Dienstleister.

- Stadtbibliothek: Sicherheitsvorfälle werden in den regelmäßigen Arbeitssitzungen des ISM-Gremiums der Stadtbibliothek erörtert und im Risikobehandlungsplan dokumentiert. Zusammen mit einem externen IT-Sicherheitsbeauftragten von Datenschutz Nord wird an einem ISM nach ISO 27001 gearbeitet.

bit:
Drei Mitarbeitende im Team Sicherheit und Infrastruktur, Schwerpunkt Sicherheit. Die Beschäftigten verfügen über mehr als fünf Jahre an Erfahrung im Bereich IT-Sicherheit und haben entweder eine Ausbildung oder ein Studium im IT-Bereich.

IT-Sicherheitsvorfälle werden im Ticketsystem dokumentiert und bearbeitet. Eine Information an die Verwaltungsspitze erfolgt umgehend bei kritischen Vorfällen. Die Anzahl der dokumentierten Fälle wird im Betriebsausschuss bit vorgestellt. Ferner erfolgt ein regelmäßiger Austausch zwischen Verwaltungsspitze und bit-Leitung, bei dem auch IT-Sicherheitsvorfälle angesprochen werden. In der AG IT-Strategie des Magistrats Bremerhaven berichtet der IT-SiBe zwei Mal jährlich über Sicherheitsvorfälle.
Bei der Ortspolizeibehörde Bremerhaven wird ein tägliches Monitoring der aktuellen Sicherheitslage durchgeführt. Dabei werden auch Hinweise des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verarbeitet. Zusätzlich steht der Fachbereich der OPB in einem engen Austausch mit Dienstleistern und der Polizei Bremen sowie dem bit.

11. Mit welchen präventiven Maßnahmen und Vorgaben erhöht der Senat die Informations- und IT-Sicherheit in den unterschiedlichen Ressorts?

a. Wer ist für die Umsetzung in Personalunion verantwortlich?

Für die Umsetzung sind in einigen Ressorts die Dienststellenleitungen verantwortlich, in anderen ist diese Aufgaben den Sicherheitsbeauftragten zugewiesen.

Zusätzlich können folgende Angaben zu den Einrichtungen im Ressortbereich SWHT gemacht werden.
BAB/WFB/M3B:
- Steuerung und Überwachung durch SWHT
- Überwachung Aufsichtsrat (IT-Prüfungen im Rahmen des Jahresabschlusses)
- Revisionsprüfungen BAB und WFB

b. Mit welchen Maßnahmen technisch und organisatorisch und Sicherheitsvorgaben erhöhen die Dienstleister die Resilienz ihrer IT-Systeme und ihrer Prozesse (Bitte aufgeschlüsselt nach Dienstleister angeben)?

In der IT-Sicherheitsleitlinie hat Dataport sich dazu verpflichtet, grundsätzlich BSI Grundschutz mit einem normalen Sicherheitsniveau anzuwenden. Dataport weist dies für einige Infrastrukturen durch Zertifizierungen und umfassende Sicherheitstests nach. Darüber hinaus können Kund*innen Grundschutz für ihre Verfahren bei Dataport beauftragen.

Wesentliche Eckpfeiler der Informationssicherheit bei Dataport sind:
- Nach BSI-Grundschutz zertifiziertes Rechenzentrum
- 10-Schichtenmodell für IT-Sicherheit
- Nach BSI-Anforderungen ausgelegte Zugangsnetze
- Warn- und Informationsdienst (CERT-Nord)
- Security Operations Center (SOC)

Konkret ergreift Dataport u.a. folgende Maßnahmen:
Prävention:
Maßnahmen zur Verhinderung von Sicherheitsverletzungen und Bedrohungen.

z. B. Implementierung von Sicherheitsrichtlinien, Firewalls, Verschlüsselung, gemanagte Endgeräte.
Detektion:
Identifizierung von Sicherheitsvorfällen und Angriffen, sobald sie auftreten.
Überwachung von Systemen und Netzwerken, um verdächtige Aktivitäten und Anomalien zu erkennen.
Reaktion:
Maßnahmen, die bei Sicherheitsvorfällen ergriffen werden.
Ziele sind Schadensbegrenzung, Isolation der Angreifer und Wiederherstellung der Systeme.

Beim zentralen KOGIS-CMS der FHB wurde 2022 von dem beim Institut für Technologiequalität (ITQ) zertifizierten Dienstleister ein umfassendes Sicherheitsmanagementsystem etabliert, das sämtliche Produktivsysteme überwacht. Verträge zur Wartung und Pflege sowie regelmäßig durchgeführte Sicherheitsüberprüfungen (sogenannte Penetrationstests beziehungsweise Webchecks) sollen mögliche Schwachstellen aufdecken, schließen und neue Angriffe bestmöglich vorbeugen. Nach Abschluss der Pentests werden die aussagekräftigen Prüfberichte inklusive Handlungsempfehlungen zur Behebung von Schwachstellen ausgewertet und zugehörige Maßnahmen in die Wege geleitet.

Weiterhin können folgende Angaben zu den Einrichtungen im Ressortbereich SWHT gemacht werden:

BAB bzw. WFB

- Austausch zu Regularien wie gesetzlichen Vorgaben und Compliance Themen (Org)
- Abstimmung von Richtlinien und Organisationsformen (Org)
- Ausrichtung nach BSI Kompendium (Org)
- Granulares Zugriffs- und Berechtigungsmanagement (Tech/Org)
- Risikoorientierte Integration von Redundanzen (Tech)
- Agiles Schwachstellen- und Patchmanagement (Tech)
- Eigen- wie Fremdüberprüfungen der Maßnahmen (Tech)
- Ausweitung von Verschlüsselungsmaßnahmen sowie Multi-Faktor-Authentifizierung (Tech)
- Optimierung und Qualitätssicherung der Backup-Strategien und Methoden (Tech)
- Einsatz von internem SIEM sowie SOC beim Kundenportal BAB (Tech)
- Verpflichtung auf vereinbarte TOMs im Rahmen der abgeschlossenen AVVs
- Einsatz von internem SIEM sowie SOC beim Kundenportal BAB (Tech)

BHV/bit:
Folgende Systeme werden eingesetzt, um die Resilienz zu erhöhen:
- Redundante Kernsysteme und Anbindungen
- Zwei Firewall Cluster

Proxyserver
- Automatisches Patchmanagement
- Einsatz einer Software zur Schwachstellenerkennung
- Einsatz von Antivirus Software sowohl auf Clients als auch auf Hypervisor-Systemen
- E-Mail-Scanner
- DDoS-Schutz
- Mehrschichtiges Backup

Geplant oder in Umsetzung sind zudem:
- Einführung von Network Access Control
- Einführung eines Security Incident and Event Monitoring (SIEM)
- Einführung von Multifaktorauthentifizierung

Der bit ergreift zudem folgende organisatorische Maßnahmen:

- Betrieb eines Informationssicherheitsmanagementsystems nach CISIS12
- Fortlaufende Weiterbildung der Mitarbeitenden sowohl im Bereich Informationssicherheit als auch im technischen Bereich
- Revisionierung von IT-Richtlinien in Abstimmung mit dem Magistrat
- Berechtigungsvergabe nach dem Need-to-know-Prinzip

Die OPB betreibt die IT-Infrastruktur nach den Vorgaben des BSI und nutzt grundsätzlich BSI-zertifizierte Lösungen.

12. In welchen Abständen werden die IT-Sicherheitsrichtlinien der Dienstleister überprüft (Bitte angeben durch wen die Überprüfung erfolgt und wer auf Seiten des Senats bzw. der Resorts/Behörden über die Ergebnisse bzw. Anpassungsbedarfe (Gaps) informiert wird)?

Sicherheitsrichtlinien bei Dataport werden i.d.R. jährlich in Zertifizierungs- und Rezertifizierungsprozessen für den BSI-Grundschutz auditiert.

BHV. Die neue Rahmenrichtlinie zur Informationssicherheit
beim Magistrat der Stadt Bremerhaven sowie alle untergeordneten Sicherheitsrichtlinien werden ab sofort bei Bedarf oder mind. alle drei Jahre evaluiert.

Bei Neuverträgen und Vertragsverlängerungen werden die Sicherheitsrichtlinien durch den IT-Sicherheitsbeauftragten sowie die Zentralstelle Datenschutz geprüft. Die Umsetzung der Rahmenrichtlinie des Magistrats wird bei der OPB bewertet.

13. Wie werden die Mitarbeiterinnen und Mitarbeiter der Dienstleister für den sicheren Umgang mit IT-Ressourcen und Daten sensibilisiert (Bitte die Maßnahmen nach den jeweiligen Dienstleistern aufschlüsseln)?

Dataport verfolgt ein umfangreiches Schulungs- und Sensibilisierungsprogramm für seine Beschäftigten, u.a. ein Schulungskonzept Informationssicherheit mit verbindlichen, flächendeckenden Pflichtschulungen sowie anwender- und zielgruppenspezifischen Schulungsangebote; zusätzlich gibt es Merkblätter, verbindliche Intranet-Meldungen sowie Wikis und Confluence-Angebote.

Performa Nord betreibt ein umfangreiches Schulungsprogramm über Vorgesetzte, Webschulung mittels Dienstanbieter und Sensibilisierung im Haus.

Zusätzlich können folgende Angaben zu den Einrichtungen in der Verantwortung verschiedener Ressortbereiche und Bremerhaven gemacht werden.

WFB und BAB:

- Schulungen und Unterweisungen durch eigene Sicherheits- und Datenschutzverantwortliche
  E-Learning Bewusstseinsschärfung für Risiken wie Phishing, Social Engineering, …
- Besuch von Veranstaltungen zu Sicherheitsthemen (wie z.B. IFIT, BSI, Cyberallianz, …)
  Durchführung von Sicherheitsbewusstseinskampagnen z.B. Phishing-Simulation

  Regelmäßige Durchführung von Notfallübungen sowie deren Nachbereitung zur KVP
  Best-Practice-Analysen mit externen Spezialisten

Senator für Kultur Eigenbetriebe:

- Volkshochschule: Mitarbeitende werden mit E-Learning geschult in den Bereichen Datenschutz, Compliance, Arbeitssicherheit und Informationssicherheit. Eine Endbenutzerrichtlinie liegt vor, welche den Umgang mit Ressourcen des Arbeitgebers mit

Passwörtern, mit Informationssicherheitsvorfällen und mit Berechtigungsvergaben mit verschiedenen Rollen vorgibt.

- Stadtbibliothek: In der Stadtbibliothek verpflichtende Kurse zum Thema Informationssicherheit, Datenschutz, Cyber-Attacken finden regelmäßig über eine eLearning-Plattform statt. Des Weiteren gibt es jährlich stattfindende Informationsveranstaltungen zur Sensibilisierung. Der verantwortungsbewusste alltägliche Umgang mit dem PC-Arbeitsplatz ist per Dienstanweisung verbindlich geregelt.

BHV
Der Magistrat bietet allen Mitarbeitenden auch weiterhin Sensibilisierungsmaßnahmen (Fortbildungen) an. Dazu zählen u.a. regelmäßige Angebote wie "Informationssicherheit am Arbeitsplatz" und "Die Hacker kommen". Darüber hinaus steht allen Mitarbeitenden orts- und zeitunabhängig das E-Learning-Tool "Behörden-IT-Sicherheitstraining (BITS)" zur Verfügung.
Außerdem werden alle Mitarbeitenden anlassbezogen über das Intranet über gegenwärtige Bedrohungslagen informiert und sensibilisiert.

Bei der OPB werden projektbezogen die Mitarbeitenden der Dienstleister durch OPB-Mitarbeitende persönlich sensibilisiert. Detaillierte Regelungen finden sich in den Vereinbarungen über die Auftragsverarbeitung zwischen der OPB und den jeweiligen Dienstleistern.

14. Wie viele Sicherheitsvorfälle wurden an welchen Funktionsträger der Freien Hansestadt Bremen durch die jeweiligen Dienstleister zwischen 2020-2024 gemeldet (Bitte die Sicherheitsvorfälle nach Anzahl und Schwere je Dienstleister aufschlüsseln)?

Sicherheitsvorfälle sind an das CERT-Nord zu melden. Dem CERT-Nord liegen hierzu folgende Zahlen vor (vgl. hierzu Anlage Land und Stadtgemeinde Bremen):

BHV
2021: 4
2020: 2
2022: 2
2023: 10
2024: 9 (Stand 2.9.24)
Eine Kategorisierung erfolgte bisher nicht.

15. Welche gemeinsamen Gremien gibt es, um mit den jeweiligen IT-Dienstleistern IT- und Informationssicherheitsinhalte regelmäßig auszutauschen und zu verbessern?

Es gibt eine monatliche CERT-CISO Runde mit CERT-Nord, CISO, Dataport

BHV: Jour Fixe (MK-bit) sowie Arbeitsgruppe "IT-Strategie"

a) In welchen Abständen finden diese statt?

Monatlich bzw. halbjährlich (IT-Strategie in BHV)

b) Wer nimmt an diesen Gremien teil?

Die CISOs sowie die zentralen Sicherheitsmanagements der Trägerländer sowie Dataports eigene CISO und Sicherheitsmanager. In der AG ISM (AG Informationssicherheitsmanagement) der FHB sind außerdem die Dienstleister Dataport, bit (BHV) und BREKOM vertreten.

BHV: Jour Fixe (MK-bit): Verwaltungsspitze, Leitung des bit sowie Leitung IuK (Informations- und Kommunikationstechnik).

AG IT-Strategie: Verwaltungsspitze, Leitung und Abteilungsleitungen des bit, Leitung und Teamleitungen IuK; Sicherheitsbeauftragte/r, Leitung Medienzentrum (Schulbereich), Stadtkämmerei; Mitbestimmung.

c) Welche wesentlichen Anpassungsbedarfe haben sich in den letzten drei Jahren technisch und organisatorisch auf Dienstleisterseite ergeben?

bit:
Durch die interne Reorganisation wurden die Tätigkeitsbereiche von einer stark generalistischen Ausrichtung hin zu einer Spezialisierung auf kleine Fachgebiete eingeführt. Dies ging einher mit der Einführung einer Teamleitungsebene und der Zusammenführung von zwei Technikbereichen zu einem. Es wurde zudem ein Team gegründet, das sich ausschließlich mit Themen der IT-Sicherheit auseinandersetzt.

16. Wer führt Audits bei den Dienstleistern durch und überwacht die Maßnahmen und das IT-Risikomanagement?

Dataport:
Für das Rechenzentrum (TDC), die Verfahrensdienste, das Zugangsnetz (ZWAN) und die NdB-Anschlusszone werden BSI-Grundschutzzertifizierungen in Verantwortung von Dataport mit entsprechend durch Ausschreibung beauftragten Dienstleister durchgeführt.
Weitere Pen-Tests, Webchecks und Audits werden entweder durch Kunden selbst oder durch Dritte im Auftrag von Kunden durchgeführt.

Performa Nord: jährlich von unabhängigen externen Auditoren überprüft (nach CISIS12)

Volkshochschule: Ist derzeit in Planung und wird gemeinsam mit dem ISB durchgeführt werden.

Stadtbibliothek: Die Auditierung erfolgt in der Regel durch die Dienstleister selbst. Im Rahmen des ISM der Stadtbibliothek sind regelmäßige Besuche bei den Dienstleistern in Planung.

WFB und BAB
- IT Prüfer im Rahmen des Jahresabschlusses
- Stabsstelle Revision WFB
- operative Compliance durch Vorgesetzte und Verantwortliche der WFB (corpGov)
- Informationssicherheitsbeauftragter (ISB) der WFB / BAB
- Revision der BAB mit externer Unterstützung (Wirtschaftsprüfer für Finanzdienstleister)
  eigenbeauftragte Spezialisten/Auditoren (möglichst TeleTrusT Deutschland e.V. / BSI zertifiziert)

BHV für bit:
Audits erfolgen im Rahmen von CISIS12 und werden durch den TÜV Nord abgenommen. Interne Audits erfolgen in Abstimmung mit einem externen Berater.

Aufgrund der regelmäßig durchzuführenden länderübergreifenden Auditierungen der IT-Dienstleistungen innerhalb des Polizeiverbundes besteht für die OPB auch kein zusätzlicher Bedarf an einer Auditierung der Polizei Bremen. Zur Störungsbeseitigung beteiligte Dienstleister werden grundsätzlich im Rahmen der Auftragsvergabe intern bewertet.

Beschlussempfehlung:

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

Anlage(n):
1. ANLAGE_CERT Nord Jahresstatistik 2022-24 HB

Jahresstatistik 2022

Hansestadt Bremen

Ereignistyp	Januar	Februar	März	April	Mai	Juni	Juli	August	September	Oktober	November	Dezember	Summe
Anzahl der durch Dataport Virenschutz betreuten Endgeräte	11.556	11.348	11.566	11.536	11.624	11.692	11.738	11.201	11.339	11.470	11.406	11.372	
2. Erfolgreiche Installation eines Schadprogramms													**0**
3. Systemeinbruch													**0**
4. Unautorisierte Systemnutzung													**0**
5. Datenabfluss durch Schadprogramme oder Hacker													**0**
6. Manipulation von Hard- oder Software													**0**
7. DDoS													**0**
8. Diebstahl oder sonstiger Verlust IT-System			7	5	3	5	3	4	2	4	3		**36**
9. Diebstahl oder sonstiger Verlust Datenträger													**0**
10. Unsachgemäße Entsorgung													**0**
11. Offenlegung durch unautorisiertes Personal													**0**
12. Sicherheitslücke		1					1					2	**4**
13. Schwerwiegender Ausfall von Betriebsmitteln													**0**
14. Schwerwiegende fehlerhafte Funktion	1												**1**
15. Schwerwiegende Überlastsituationen													**0**
16. Widerrechtliche Aktion, Verstoß IT-Sicherheitsrichtlinie				2				2	2	1	3	2	**12**
17. Interne Ursachen									1				**1**
18. Naturgewalten													**0**
19. Beschädigung													**0**
20. Besondere Erkenntnisse							1						**1**
21. Use Case										2			**2**
	1	**1**	**7**	**7**	**3**	**5**	**5**	**6**	**5**	**7**	**5**	**4**	**56**

Jahresstatistik 2023

Hansestadt Bremen

Ereignistyp	Januar	Februar	März	April	Mai	Juni	Juli	August	September	Oktober	November	Dezember	Summe
Anzahl der durch Dataport Virenschutz betreuten Endgeräte	11.428	11.340	11.457	11.586	11.256	11.347	11.477	11.311	11.263	11.392		11.638	
2. Erfolgreiche Installation eines Schadprogramms	1												1
3. Systemeinbruch									1				1
4. Unautorisierte Systemnutzung													0
5. Datenabfluss durch Schadprogramme oder Hacker													0
6. Manipulation von Hard- oder Software													0
7. DDoS								1			1		2
8. Diebstahl oder sonstiger Verlust IT-System	7	2	1		2	2	1	4	1	12	5	11	48
9. Diebstahl oder sonstiger Verlust Datenträger		1											1
10. Unsachgemäße Entsorgung													0
11. Offenlegung durch unautorisiertes Personal											1		1
12. Sicherheitslücke	1				1		4			2			8
13. Schwerwiegender Ausfall von Betriebsmitteln								1					1
14. Schwerwiegende fehlerhafte Funktion							1		1				2
15. Schwerwiegende Überlastsituationen													0
16. Widerrechtliche Aktion, Verstoß IT-Sicherheitsrichtlinie	3	1				2	1	1	1		1		10
17. Interne Ursachen				1	1				1	1			4
18. Naturgewalten													0
19. Beschädigung													0
20. Besondere Erkenntnisse			1							1			2
21. UseCase	3	2	1	7	1		2	12	11	14		1	54
22. Fehlkonfiguration			2		1		1	3	1	4	1	1	14
23. Fremdaccountnutzung		1											1
24. Phishing		2	1						2				5
25. Wirtschaftsunternehmen											3		3
	15	9	6	8	6	4	10	22	19	34	12	13	158

Meldungen im CERT Nord Kundenportal 2023

-1 im Kundenportal zur Verfügung gestellte Sicherheitsinformationen ->Startseite Kundenportal -> Sicherheitsinformationen

-2 im Kundenportal zur Verfügung gestellte Warnungen unter ->Startseite Kundenportal ->Meldungen -> Sicherheitswarnungen

2023 Jan	2023 Feb	2023 Mrz	2023 Apr	2023 Mai	2023 Jun	2023 Jul	2023 Aug	2023 Sep	2023 Okt	2023 Nov	2023 Dez	Jahres gesamt

im Kundenportal zur Verfügung gestellte Sicherheitsinformationen (Startseite Kundenportal -> Sicherheitsinformationen)	153	129	117	112	147	177	210	200	102	170	168	116	1801
im Kundenportal zur Verfügung gestellte Warnungen (Startseite Kundenportal -> Meldungen -> Sicherheitswarnungen)	2	3	3	4	1	4	7	8	1	10	4	1	48
monatliche Anzahl	155	132	120	116	148	181	217	208	103	180	172	117	

2024

Auflistung der Sicherheitsvorfälle August 2024

Ereignistyp	Hamburg	Schleswig-Holstein	Sachsen-Anhalt	Bremen	Summe
Anzahl der durch Dataport Virenschutz betreuten Endgeräte	54.863	43.817	12.816	11.407	122.903
Verhältniss des abgelehnten zum gesamten Mailaufkommens in %	Nutzung gemeinsame Infrastruktur				20,12 %
1. Abgewehrtes Schadprogramm	Nutzung gemeinsamer Infrastrukturen				2175465
2. Erfolgreiche Installation eines Schadprogramms					0
3. Systemeinbruch				1	1
4. Unautorisierte Systemnutzung					0
5. Datenabfluss durch Schadprogramme oder Hacker					0
6. Manipulation von Hard- oder Software					0
7. DDoS	1		1		2
8. Diebstahl oder sonstiger Verlust IT-System	12	2			14
9. Diebstahl oder sonstiger Verlust Datenträger					0
10. Unsachgemäße Entsorgung					0
11. Offenlegung durch unautorisiertes Personal					0
12. Sicherheitslücke	2	1	1	1	5
13. Schwerwiegender Ausfall von Betriebsmitteln			1		1
14. Schwerwiegende fehlerhafte Funktion					0
15. Schwerwiegende Überlastsituationen					0
16. Widerrechtliche Aktion, Verstoß IT-Sicherheitsrichtlinie	16	3	3	4	26
17. Interne Ursachen	1				1
18. Naturgewalten					0
19. Beschädigung					0
20. Besondere Erkenntnisse	1	1			2

21. UseCase		2	1		3
22. Fehlkonfiguration	7	4	3	8	22
23. Fremdaccountnutzung					0
24. Phishing	14			1	15
25. Wirtschaftsunternehmen		2	1		3
Summe:	54	15	11	15	95