BREMISCHE BÜRGERSCHAFT
Landtag
21. Wahlperiode

Drucksache 21/1717
(zu Drs. 21/1600)
24. März 2026

Mitteilung des Senats

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

Große Anfrage
der Fraktion der CDU vom 10. Februar 2026
und Mitteilung des Senats vom 24. März 2026

Vorbemerkung der fragenstellenden Fraktion:

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.

Der Senat beantwortet die Große Anfrage wie folgt:

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?

In der Freien Hansestadt Bremen sind Eigen- und Beteiligungsbetriebe häufig entweder nur in Teilen in die Informations- und Kommunikationstechnik (IKT) der öffentlichen Verwaltung eingebunden oder organisatorisch vollständig außerhalb der unmittelbaren öffentlichen Verwaltung angesiedelt. IKT umfasst hierbei die Informationstechnologie (IT), also die technischen

Mittel zur Verarbeitung und Speicherung von Daten, sowie die Kommunikationsinfrastruktur und -dienste für Vernetzung und Informationsaustausch. Daraus ergeben sich teilweise eigenständige IKT-Strukturen und Sicherheitsverantwortlichkeiten, die nicht oder nur teilweise den zentralen Steuerungs- und Sicherheitsmechanismen der öffentlichen Verwaltung unterliegen. Eine einheitliche Betrachtung der Cyberbedrohungslage erfolgt daher überwiegend auf Grundlage allgemeiner Erkenntnisse zur gesamtwirtschaftlichen Bedrohungssituation.

Die IT-Sicherheitslage in Deutschland befindet sich auf einem angespannten Niveau. Nach dem Kosten-Nutzen-Kalkül cyberkrimineller Angreifer:innen gibt es keine uninteressanten Ziele mehr. Jede aus dem Internet erreichbare Institution oder Person ist prinzipiell bedroht. Auch steigt die Angriffsfläche durch die allgemeine Digitalisierung weiter an. Neben Einzeltäter:innen geht eine gesteigerte Gefahr von organisierten Cyberkriminellen sowie staatlichen und staatlich gelenkten oder beeinflussten Akteuren aus, welche zunehmend unternehmerisch operieren und die einzelnen Schritte eines Cyberangriffs arbeitsteilig vornehmen.

Die größte Gefahr stellen hierbei so bezeichnete Ransomware-Angriffe dar, bei denen Angreifer:innen Daten zuerst stehlen (Exfiltration) und anschließend sowohl die Verschlüsselung der Systeme als auch die Drohung, die gestohlenen Daten zu veröffentlichen, kombinieren, um Lösegeld zu erzwingen (sog. „Double Extortion“). Parallel beschleunigt der Einsatz von Künstlicher Intelligenz die Automatisierung von Angriffen. Automatisierte Schwachstellenscans, die Erstellung glaubhafter Phishing-Inhalte, wie gefälschte E-Mails oder Webseiten, die die Nutzer:innen zur Preisgabe sensibler Daten oder zur Ausführung schädlicher Aktionen verleiten sollen, abgestimmt auf die entsprechenden Unternehmensinhalte, sowie sich schnell adaptierende Schadsoftware beeinflussen die Bedrohungslage über die gesamte Wirtschaft hinweg. Diese Cyberangriffe zielen hierbei in den meisten Fällen auf Unternehmen ab, die vergleichsweise einfach zu kompromittieren sind, etwa durch unzureichend gesicherte Systeme, veraltete Software oder ungeschützte Zugänge, da diese durch den geringen Aufwand und die hohe Erfolgswahrscheinlichkeit lohnende Ziele darstellen. Ebenfalls zeigt sich, dass von einem Cyberangriff betroffene Unternehmen in vielen Fällen nicht gezielt ausgesucht wurden, sondern aufgrund leicht auszunutzender Schwachstellen als „Zufallsopfer” betrachtet werden müssen.

Dem Senat liegen keine Erkenntnisse über eine spezifische Bedrohungslage für die Eigen- und Beteiligungsbetriebe im Land Bremen vor.

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?

Aufgrund der organisatorischen Eigenständigkeit der Eigen- und Beteiligungsbetriebe im Land Bremen bestehen unterschiedliche Regelungen hinsichtlich der Notfall- und Krisenpläne für IT-Sicherheitsvorfälle. Dem Senat liegen daher keine einheitlichen oder zentral gepflegten Übersichten über Incident-Response-Pläne (gemeint sind hiermit Ablaufpläne, die bei der Erkennung von IT-Sicherheitsvorfällen sowie der anschließenden Eindämmung, Untersuchung und Behebung genutzt werden, um Schäden und Betriebsunterbrechungen zu minimieren), Wiederanlaufpläne oder vergleichbare Notfallkonzepte der Eigen- und Beteiligungsbetriebe vor.

Weitere Aussagen zu Eigen- und Beteiligungsbetrieben basieren auf den von den Ressorts an die Zentralstelle Cybersicherheit zurückgemeldeten Informationen zu Eigen- und Beteiligungsbetrieben im Land Bremen. Die überwiegende Mehrzahl der Eigen- und Beteiligungsbetriebe verfügt über grundlegende Ablaufpläne und Verfahrensanweisungen für IT-Sicherheitsvorfälle. Diese variieren, auch aufgrund der Heterogenität der Eigen- und Beteiligungsbetriebe, in ihrer Ausprägung, ihrer Art und ihrem Umfang. Hierzu zählen u. a. Checklisten, Notfallhandbücher, Kommunikationspläne, Incident-Response-Pläne sowie Disaster-Recovery-Konzepte (hierbei handelt es sich um dokumentierte Pläne mit technischen Maßnahmen und Prozessen, die

sicherstellen sollen, dass IT-Systeme, Daten und Geschäftsprozesse nach einem schwerwiegenden Ausfall schnell wiederhergestellt werden können) und weitere Geschäftsfortführungspläne.

Eine pauschale Bewertung der Notfall- und Krisenpläne ist aufgrund der Heterogenität nicht möglich. Sofern normative, rechtliche oder branchenspezifische Anforderungen, z. B. aufgrund bestehender Zertifizierung nach einem bestimmten Standard, existieren, werden die bestehenden Notfall- und Krisenpläne im Rahmen interner und externer Auditierungen überprüft. Ebenso finden Auditierungen auf freiwilliger Basis statt. Bei den Auditierungen werden die bestehenden Konzepte auf ihre Angemessenheit überprüft und bei Bedarf angepasst.

a. In welchem Turnus werden diese Notfallpläne jeweils überprüft, aktualisiert und praktisch erprobt (z.B. durch Simulationen, Penetrationstests oder Notfallübungen)?

Die Festlegung von Überprüfungs-, Aktualisierungs- und Übungsintervallen obliegt grundsätzlich den jeweiligen Eigen- und Beteiligungsbetrieben im Rahmen ihrer organisatorischen Verantwortung. Aufgrund der unterschiedlichen organisatorischen Einbindung in die IKT der öffentlichen Verwaltung bestehen hierzu keine einheitlichen Vorgaben des Senats.

Die Notfallpläne werden in wiederkehrenden Intervallen, zumeist jährlich bzw. bei Bedarf, überprüft. Zusätzlich werden Back-Up-Tests (geplante Prüfungen, bei denen gesicherte Daten und Wiederherstellungsverfahren regelmäßig wiederhergestellt und geprüft werden, um die Integrität der Backups und die Wiederanlaufbarkeit der Systeme sicherzustellen), Penetrationstests (autorisierte, kontrollierte Sicherheitstests, bei denen Expert:innen Angriffe simulieren, um Schwachstellen in IT-Systemen, Netzwerken oder Anwendungen aufzudecken) und Angriffssimulationen in unterschiedlichen Intervallen sowie anlassbezogen durchgeführt. Hierbei variieren die Intervalle in Abhängigkeit der Dynamik der entsprechenden Risiken, die durch die umgesetzten Konzepte und Maßnahmen gemindert werden sollen.

So findet z. B. eine monatliche Evaluation der Wirksamkeit von Systemen zur Angriffserkennung bei einem Eigen- und Beteiligungsbetrieb statt, der ebenfalls jährliche bzw. zwei-jährliche Penetrationstests durchführt, wohingegen in einem anderen Eigen- und Beteiligungsbetrieb halbjährlich bis jährlich Rückspieltests zur Absicherung der Backup-Qualität durchgeführt werden.
Generell variieren die Intervalle auch in Bezug auf die entsprechenden Gefahren; als kürzestes Intervall ist z. B. die vierteljährliche Überprüfung für die Kataster der Risiken und Anforderungen eines Eigen- und Beteiligungsbetriebs zu nennen, wohin gegen das Intervall zur Überprüfung der Risikoanalyse der Naturgefahren am Standort desselben Betriebs fünf Jahre beträgt.

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?

Aufgrund der eigenständigen IKT-Strukturen der Eigen- und Beteiligungsbetriebe erfolgen die Auswahl und der Einsatz technischer Maßnahmen zur IT-Sicherheitsüberwachung grundsätzlich in eigener Verantwortung der jeweiligen Einrichtungen.

Basierend auf den vorliegenden Rückmeldungen gehören Firewall-Systeme und Anti-Virus-Software zur Überprüfung auf Schadsoftware in E-Mails, externen Datenträgern sowie den Endgeräten zu den standardmäßig eingesetzten technischen Sicherheitsmaßnahmen. Zusätzlich werden bei einer Mehrzahl der Eigen- und Beteiligungsbetriebe auch weiterführende Sicherheitsmaßnahmen umgesetzt. Der Umfang der technischen Maßnahmen zur IT-Sicherheitsüberwachung orientiert sich zudem an weiteren rechtlichen, normativen und branchenspezifischen Anforderungen.

Bei den technischen Maßnahmen, die in unterschiedlichem Umfang von den Eigen- und Beteiligungsbetrieben ergänzend umgesetzt werden, handelt es sich um die Folgenden:

- Endpoint Detection and Response (EDR; System zur kontinuierlichen Überwachung von Endgeräten, um verdächtiges Verhalten zu erkennen und automatisierte sowie manuelle Reaktionsmaßnahmen zur Eindämmung und Untersuchung von Bedrohungen einleiten zu können),
- zentrales Update- und Patchmanagement,
- Schwachstellen- und APT-Scanner,
- Datenträgerverschlüsselung,
- Netzwerksegmentierung,
- zentrales Monitoring des Netzwerkverkehrs,
- Protokollierung des Netzwerkverkehrs mit anlass- und verdachtsbezogener Auswertung,
- Multi-Faktor-Authentifizierung (MFA),
- Regelmäßige Datensicherung (Back-Ups),
- Überwachung des Active Directory,
- 24/7-Monitoring der IT-Infrastruktur durch externe Security Operation Center (SOC),
- Einsatz von Security Information and Event Management Systemen (SIEM) zur Auswertung von Log-Dateien,
- Einsatz von Intrusion-Detection-Systeme (IDS),
- Nutzung vordefinierter Images zur einheitlichen Installation von Arbeitsplatzsystemen,
- Systemseitige Durchsetzung der Passwortrichtlinie ergänzt durch den Einsatz eines Passwortmanagers,
- sicheres Löschen von Datenträgern und deren Vernichtung.

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?

Verbindliche, einheitliche organisatorische Mindeststandards zur Informationssicherheit bestehen für Eigen- und Beteiligungsbetriebe nur insoweit, wie diese unmittelbarer Teil der IKT der öffentlichen Verwaltung sind oder entsprechenden Vorgaben durch die Fachaufsicht unterliegen. Die Leitlinie für Informationssicherheit der Freien Hansestadt Bremen (IS-LL) sieht die Einhaltung der Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) vor. Einrichtungen außerhalb der unmittelbaren Verwaltung sind grundsätzlich eigenverantwortlich für die Ausgestaltung ihrer Informationssicherheitsorganisation. Hierbei orientieren sich die Eigen- und Beteiligungsbetriebe an anerkannten generellen Standards der Informationssicherheit. Zusätzlich sind in Einzelfällen weitere branchenspezifische Standards umgesetzt bzw. befinden sich in der Umsetzung. Bei den Standards handelt es sich um die Folgenden:

- ISO/IEC 27001 – Informationssicherheitsmanagement,
- BSI IT-Grundschutz,
- Compliance Informations-Sicherheitsmanagement System in 12 Schritten (CISIS 12),
- LA-SCS (World Lottery Association Security Control Standard),
- Payment Card Industry Data Security Standard (PCI-DSS),
- Business Continuity Management nach BSI Standard 200-4,

- Branchenspezifischer Sicherheitsstandard (B3S) „Medizinische Versorgung“, Branchenspezifischer Sicherheitsstandard (B3S) „Siedlungsabfallentsorgung“.

Die Einhaltung wird durch interne sowie externe Audits, die erforderlichenfalls durch akkreditierte Zertifizierungsunternehmen durchgeführt werden, in festgelegten Intervallen überprüft.
Zudem prüfen einige Eigen- und Beteiligungsbetriebe, die in den durch das Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung geregelten Sektoren tätig sind, ob eine Betroffenheit besteht und ob die Anforderungen des NIS-2-Umsetzungsgesetzes somit umgesetzt werden müssen.

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?

Generell liegt die Zuständigkeit für die unmittelbare Lagebewältigung, die Einbindung der Polizei bei dem Verdacht auf ein strafbares Handeln sowie die Information des verantwortlichen Ressorts bei dem potenziell betroffenen Eigen- oder Beteiligungsbetrieb. Hiernach ist eine Information des Chief Information Security Officers (CISO) bzw. des zentralen Informationssicherheitsmanagements der Freien Hansestadt Bremen (ISM FHB), des Computer Emergency Response Team für die Verwaltungen der Länder Schleswig-Holstein, Hamburg, Bremen und Sachsen-Anhalt (CERT Nord) sowie der Zentralstelle Cybersicherheit vorgesehen. Im Rahmen der Lagebewertung wird durch die involvierten Stellen geprüft, ob eine kurzfristige Information der politischen Ebene, z. B. aufgrund der zu erwartenden Auswirkungen, erforderlich ist.
Die bisherigen Erfahrungen haben gezeigt, dass die Information der entsprechenden Stellen in einem angemessenen Zeitrahmen erfolgt.

Auf Grundlage der bisherigen Erfahrungen hat sich gezeigt, dass Organisationen, die organisatorisch nicht oder nur eingeschränkt in die zentrale IKT-Organisation eingebunden sind, teilweise über weniger etablierte Kommunikations- und Meldewege verfügen. In diesen Fällen besteht die Möglichkeit, dass die strukturierte Weitergabe von Informationen im Vergleich zu Einrichtungen mit enger Anbindung an die öffentlichen IKT-Strukturen verzögert oder weniger standardisiert erfolgt. Vor diesem Hintergrund besteht weiterhin Verbesserungspotenzial, insbesondere bei der Vereinheitlichung von Meldewegen, der Sensibilisierung für Berichtspflichten sowie der frühzeitigen Einbindung der zuständigen Stellen.

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?

In der Polizei Bremen, Direktion Kriminalpolizei/LKA, wurde analog zu allen weiteren Landeskriminalämtern und dem Bundeskriminalamt eine Zentrale Ansprechstelle Cybercrime (ZAC) innerhalb des Ermittlungsbereichs Cybercrime eingerichtet. Die Erreichbarkeit ist auf entsprechenden Internetpräsenzen veröffentlicht. Die Aufgabe dieser Stelle umfasst sowohl präventive wie repressive Tätigkeiten.

Die Präventionsaufgabe beinhaltet die Sensibilisierung, die Erhöhung der Awareness und die Stärkung der innerbetrieblichen Eigenverantwortung, welche durch die Teilnahme an unterschiedlichen Veranstaltungen in Form von Vorträgen, Beratungen und intensiver Netzwerkarbeit mit Verbänden öffentlicher und nicht-öffentlicher Institutionen, kritischer Infrastrukturen

und Unternehmen abgebildet wird. Dabei stehen insbesondere die Entscheidungs-/Führungsebene, wie Geschäftsführung oder die Behörden-/Abteilungsleitung, sowie die IT-Leitung und der CISO im Fokus der Zusammenarbeit.

Dem gegenüber agiert die ZAC in repressiven Situationen als erste und direkte Ansprechstelle für Unternehmen, Institutionen und Behörden, stellt die zentrale Erstberatung in Schadensfällen inkl. Anzeigenaufnahme sicher und fungiert als Steuerungselement der unmittelbaren Aufnahme weiterer Ermittlungsmaßnahmen. Durch die Integration der ZAC im Fachbereich Cybercrime-Ermittlungen des LKA Bremen werden ein medienbruchfreier Übergang und eine 24/7-Erreichbarkeit in der ersten zeitkritischen Phase gewährleistet.

Der Fachbereich Cybercrime der Polizei Bremen gewährleistet die unmittelbare Aufnahme von Ermittlungen, Kommunikation und Begleitung von betroffenen Unternehmen mit Sitz im Land Bremen. Bei vorliegender Zuständigkeit der Ortspolizeibehörde (OPB) Bremerhaven erfolgt eine abgestimmte Abgabe des Verfahrens nach Abschluss der ersten polizeilich notwendigen Maßnahmen. Die Integration in diversen landes- und bundesweiten Netzwerken ermöglicht die zeitnahe Informationssteuerung und Erkenntnisgewinnung für die laufenden Verfahren.

Die OPB Bremerhaven ist im Rahmen ihres gesetzlichen Auftrags für die Gefahrenabwehr und die Durchführung strafrechtlicher Ermittlungen im Stadtgebiet Bremerhaven zuständig. Neben der Aufnahme von relevanten Sachverhalten sind die Polizei Bremen sowie die OPB Bremerhaven auch für die Sicherung digitaler Spuren und die Prävention zuständig.

Die Zentralstelle Cybersicherheit kann den Eigen- und Beteiligungsbetrieben beim Vorliegen entsprechender Anfragen ebenfalls allgemeine Präventionshinweise übermitteln bzw. verweist auf die Angebote weiterer Stellen, wie z. B. die Angebote des BSI.

Sollte bei der Bewertung eines etwaigen Cyberangriffs festgestellt werden, dass weitere Stellen innerhalb des Landes Bremen informiert bzw. gewarnt werden müssen, so erfolgt dies in enger Absprache zwischen dem CISO und der Zentralstelle Cybersicherheit. Hierfür kann z. B. auch auf das CERT Nord zurückgegriffen werden. Gleiches gilt für die Information von Stellen außerhalb des Landes Bremen. Eine Information und Erkenntnisabfrage findet bei Bedarf z. B. durch das CERT Nord über den Verwaltungs-CERT-Verbund (VCV) bzw. über die Zentralstelle Cybersicherheit bei gleichgelagerten Stellen außerhalb des Landes Bremen statt.

Bei Bedarf kann darüber hinaus, sofern ein außergewöhnlicher IT-Sicherheitsvorfall vorliegt, auf Grundlage eines Amtshilfeersuchens des Landes auch das Mobile Incident Response Team (MIRT) des BSI hinzugezogen werden. Dieses unterstützt betroffene Einrichtungen insbesondere bei der technischen Analyse, Eindämmung und Bewältigung schwerwiegender IT-Sicherheitsvorfälle.

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?

Auf Grund der Struktur des Internets, den individuell genutzten Hard- und Softwaresystemen, IT-Sicherheitspersonal und den unterschiedlichsten Angriffsmöglichkeiten auf individuell aufgesetzten IKT-Infrastrukturen, ist eine vorherige Erkennung eines Cyberangriffs sehr schwierig. Die Eigenverantwortung hinsichtlich der Hygiene der eigenen IKT-Infrastruktur, kontinuierlicher Updates der Systeme, Awareness der eigenen Mitarbeiter:innen oder separater IT-Sicherheitsprodukte der Netzwerküberwachung stellen die Grundlage jeglicher Aktivität dar. Die Erkennung von Cyberangriffen erfolgt in den meisten Fällen direkt durch den betroffenen Betrieb, wenn Bestandteile der IKT-Infrastruktur gestört oder nicht mehr funktionsfähig

sind. In Einzelfällen nimmt das Landeskriminalamt beim Vorliegen entsprechender Erkenntnisse im Vorfeld aktiv Kontakt zu einem potenziell geschädigten Betrieb auf und weist auf ein bestehendes Sicherheitsrisiko mit dem Ziel der Verhinderung des Schadenseintrittes hin. Die Zusammenarbeit der betroffenen Bereiche mit der zuständigen polizeilichen Ermittlungsdienststelle erfolgt i. d. R. über die ZAC sofort nach Kenntnis des Vorfalls und abhängig von der Angriffsvariante direkt durch die verantwortliche IT-Abteilung und/oder einen eingesetzten IT-Dienstleister.

Sofern die Zentralstelle Cybersicherheit eigene Erkenntnisse zu ggf. bevorstehenden oder angeblich erfolgreichen Cyberangriffen gewinnen kann, erfolgt die Information der vermeintlich betroffenen Einrichtungen unabhängig davon, ob es sich um Eigen- und Beteiligungsbetriebe oder sonstige privatwirtschaftliche Unternehmen handelt. Die Information erfolgt nach vorheriger Abstimmung zwischen den Stellen, bei denen die Erkenntnisse ebenfalls vorliegen könnten (z. B. der Zentralstelle Cybersicherheit und der Zentralen Ansprechstelle Cybercrime), um eine einheitliche Kommunikation zu gewährleisten. Je nach Verortung der vermeintlich betroffenen Einrichtung (Eigen- und Beteiligungsbetrieb, öffentliche Verwaltung, privatwirtschaftliche Stelle), erfolgt eine Information durch die Zentralstelle Cybersicherheit, das CERT Nord oder die Polizeivollzugsbehörden im Land Bremen. Dies gilt ebenfalls für Hinweise, die den o. g. Stellen im Land Bremen durch Dritte übermittelt werden.

Eigen- und Beteiligungsbetriebe, die organisatorisch unabhängig von den zentralen IKT-Strukturen der öffentlichen Verwaltung betrieben werden, können bei Bedarf in bestehende Informationsverbünde zur Cyber-Sicherheitslage eingebunden werden. Dadurch soll auch für Einrichtungen außerhalb der unmittelbaren IKT-Organisation ein strukturierter Austausch sicherheitsrelevanter Informationen ermöglicht werden.

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?

Grundsätzlich sind die Eigen- und Beteiligungsbetriebe für die Sicherung ihrer IT sowie die hiermit verbundenen präventiven Maßnahmen selbst verantwortlich.

Die von den betroffenen Unternehmen betriebene IKT-Infrastruktur mit Netzwerk, genutzten Hard- /Softwareprodukten oder Serverlandschaft ist stets einzigartig und individuell auf die Bedürfnisse bzw. Tätigkeit der Nutzer:innen ausgerichtet. Bei Vorliegen eines erfolgreichen Cyberangriffs und der Einbindung der Zentralen Ansprechstelle Cybercrime der Polizei Bremen erfolgt grundsätzlich eine enge Zusammenarbeit mit der Geschäftsführung auch in Bezug auf rechtliche Konsequenzen oder weitere Meldeverpflichtungen. Mit der internen IT-Abteilung der betroffenen Unternehmen bzw. mit den beauftragten IT-Dienstleistungsunternehmen erfolgt eine enge Kooperation, um eine Identifizierung des Angriffsvektors und den damit verbundenen Aktivitäten der Angreifer:innen im internen Netzwerk zu ermöglichen. Bei vorliegenden Informationen zu Angreifer:innen kann die Polizei dabei unterstützen, Abläufe im Netzwerk nachzuvollziehen und ggf. täterseitige Kommunikationsprotokolle zu sichern. Ferner können die vorliegenden polizeilichen Erkenntnisse helfen, um offene Schwachstellen im System zu identifizieren, diese zu schließen und mit der Systemwiederherstellung zu beginnen. Diese Standardmaßnahme wird von allen betroffenen Bereichen angenommen. Von polizeilicher Seite aus erfolgt eine forensische Analyse bei gesicherten Schadsoftware-Dateien oder von Protokolldateien ausschließlich für Ermittlungszwecke. Die Wiederherstellung kompromittierter Systeme fällt hingegen nicht in den Aufgabenbereich der Polizei und könnte zudem auch mangels Fachkenntnis in der betriebsspezifischen IT-Administration und Infrastruktur, der individuellen Bedürfnisse des Unternehmens und möglichen rechtlichen Folgewirkungen (u. a. Haftungsfragen) nicht erfolgen.

Es bestehen weiterhin Kontakte unterschiedlicher Art zu spezialisierten IT-Dienstleistern, wie z. B. IT-Forensiker:innen und Cyber-Versicherungen, welche bei Bedarf zur Unterstützung herangezogen werden würden.

Ebenso kann bei Bedarf durch die Stellen des für den betroffenen Eigen- und Beteiligungsbetrieb verantwortlichen Ressorts im Rahmen eines Abrufvertrags mit Dataport eine forensische Analyse beauftragt werden.

Die Zentralstelle Cybersicherheit kann bei einem unmittelbaren Angriff durch koordinierende Maßnahmen, wie die Steuerung des Informationsflusses in die Ressorts und die zentrale Steuerung etwaiger Fragen aus den Ressorts an die betroffene Stelle, unterstützen. Sie fungiert hierbei als Informationsknotenpunkt und unterstützt bei der Koordinierung erforderlicher Absprachen und Maßnahmen als zentrale Anlaufstelle.

Für Eigen- und Beteiligungsbetriebe im Zuständigkeitsbereich der OPB Bremerhaven stehen während und unmittelbar nach einem Cyberangriff verschiedene Unterstützungsangebote zur Verfügung. Hierzu zählen insbesondere die polizeiliche Gefahrenabwehr, die Entgegennahme von Strafanzeigen, die IT-forensische Sicherung und Auswertung digitaler Beweismittel sowie die Einleitung und Durchführung strafrechtlicher Ermittlungen. Die Kriminalpolizei wird hier durch die Technische Einsatz- und Ermittlungsunterstützung innerhalb der Ortspolizeibehörde unterstützt, wenn es um die Umsetzung technischer Bedarfe zwecks Sicherung und Ermittlungen geht.

Die OPB Bremerhaven versteht sich gegenüber betroffenen Betrieben und Einrichtungen als Ansprechstelle, die niedrigschwellig über Sofortmaßnahmen, den Umgang mit möglichen Erpressungsversuchen und den weiteren Ablauf des Ermittlungsverfahrens informiert.

Sofern ein außergewöhnlicher IT-Sicherheitsvorfall vorliegt, kann darüber hinaus auf Grundlage eines Amtshilfeersuchens des Landes das Mobile Incident Response Team (MIRT) des BSI hinzugezogen werden. Die Inanspruchnahme der genannten Unterstützungsangebote erfolgt abhängig vom jeweiligen Einzelfall.

Nach Kenntnis des Senats werden die entsprechenden Angebote der Dienstleister:innen sowie der öffentlichen Stellen präventiv beratend und bei vermuteten Sicherheitsvorfällen nachgefragt und in Anspruch genommen. Weiterhin wurden im Rahmen des bekannt gewordenen Cyberangriffs (es wird auf Frage 8 verwiesen) sowohl die Dienstleistungen einer bestehenden Cyberversicherung sowie die Unterstützung durch die Zentrale Ansprechstelle Cybercrime sowie der Zentralstelle Cybersicherheit 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?

Der Senat betrachtet Resilienz als ein multidisziplinäres Themengebiet, in welchem der Bereich der Cybersicherheit als ein wichtiger Teilaspekt zu sehen ist. Die digitale Resilienz der Eigen- und Beteiligungsbetriebe ist, so wie die der gesamten Wirtschaft, ein fortwährender Lern- und Weiterentwicklungsprozess, der kontinuierliche Anpassungen und eine stetige Verbesserung der Wiederherstellungsfähigkeit erfordert.

Auf Ebene des Bundes kürzlich erlassene Gesetze, wie das NIS2UmsG sowie das Gesetz zur Stärkung und Regelung der Sicherheit Kritischer Infrastrukturen (KRITIS-DachG), stellen hierbei einschlägige Vorschriften dar, aus welchen sich grundsätzlich weitere Anforderungen an die Cyber- und Informationssicherheit ergeben können. Es ist davon auszugehen, dass eine geringe Anzahl der Eigen- und Beteiligungsbetriebe, die sich aus dem NIS2UmsG abzuleitenden Anforderungen umsetzen müssen. In Abhängigkeit der verfügbaren personellen und materiellen Ressourcen ist zu prüfen, ob durch die verpflichtende Umsetzung zusätzliche

Maßnahmen erforderlich werden oder ob die bestehenden Maßnahmen ausreichend sind. Sofern zusätzliche Maßnahmen umzusetzen sind, kann bei der Umsetzung dieser ebenfalls geprüft werden, ob hierbei Synergieeffekte geschaffen werden können, von denen weitere, nicht unter den Anwendungsbereich des NIS2UmsG fallende, Eigen- und Beteiligungsbetriebe profitieren können.

Darüber hinaus wird im Rahmen der gesetzlichen Umsetzung auf Landesebene geprüft, inwieweit durch entsprechende bremische Regelungen zusätzliche Impulse zur Stärkung der Informationssicherheit bei Eigen- und Beteiligungsbetrieben gesetzt werden können. Ziel ist es insbesondere, ein angemessenes Sicherheitsniveau unter Berücksichtigung der jeweiligen organisatorischen Einbindung und Eigenständigkeit der Einrichtungen zu fördern sowie die Zusammenarbeit mit den zentralen Stellen der Informationssicherheit weiter zu stärken.

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?

Alle mit dem Internet verbundenen Systeme werden tagtäglich mehrfach gescannt. Zudem stellen Spam- und Phishing-E-Mails eine allgemeine Bedrohung dar. Durch die eingesetzten Schutzsysteme wie Firewalls und Mail-Filter kann die überwiegende Mehrzahl dieser Gefahren abgewehrt werden.

In den vergangenen zwei Jahren ist es zu einem erfolgreichen Ransomware-Angriff auf einen Eigenbetrieb im Land Bremen gekommen. Hierbei handelte es sich um den Ransomware-Angriff vom 03.02.2026 auf die Werkstatt Bremen. Im vorliegenden Fall wurde ein Großteil der IT-Systeme der Werkstatt Bremen verschlüsselt. Dies hatte Auswirkungen auf die Erbringung der angebotenen Dienstleistungen, u. a. auf die von der Werkstatt Bremen betriebene Beweisstückstelle auf der Liegenschaft des Polizeipräsidiums. Unmittelbar nach Bekanntwerden des Vorfalls wurden die betroffenen Systeme und Netzwerke vom Internet getrennt, ein Incident-Response-Dienstleister zur Unterstützung hinzugezogen sowie die Polizei Bremen informiert. Weiterführende Angaben zum entsprechenden Vorfall können aufgrund der aktuell noch laufenden Ermittlungen nicht gemacht werden.

Dem Senat sind keine weiteren erfolgreichen Ransomware- oder vergleichbaren Cyberangriffe auf Eigen- oder Beteiligungsbetreibe in den vergangenen zwei Jahren bekannt geworden.

Beschlussempfehlung:

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