BREMISCHE BÜRGERSCHAFT Drs. 19/2148
Landtag
19. Wahlperiode 23.04.19

Antwort des Senats
auf die Kleine Anfrage der Fraktion Bündnis 90/Die Grünen
vom 26. Februar 2019

„IT-Sicherheit in bremischen Krankenhäusern“

Die Fraktion Bündnis 90/Die Grünen hat folgende Kleine Anfrage an den Senat gerichtet:

„Die Digitalisierung und Vernetzung hat auch im Gesundheitswesen in den letzten Jahren stark zugenommen. Die intensive Nutzung von technischen Systemen bietet dabei nicht nur Vorteile, sondern auch mehr Angriffsmöglichkeiten für Cyberkriminelle. Diese können insbesondere bei Kritischen Infrastrukturen, zu denen unter Umständen auch Krankenhäuser zu zählen sind, verheerende Auswirkungen haben. So musste Mitte November das Klinikum Fürstenfeldbruck aufgrund einer Infizierung mit Schadsoftware tagelang schwere Störungen im Betriebsablauf hinnehmen. Die Ameos-Kliniken in Bremerhaven waren im September Opfer eines Hackerangriffs und mussten zeitweise die Notaufnahme schließen.

Wir fragen den Senat:

1. In wie vielen Fällen seit der Antwort des Senats auf Drucksache 19/647 ist in Krankenhäusern im Land Bremen durch Schadsoftware oder Hackerangriffe der Betrieb beeinträchtigt oder der Schutz personenbezogener Daten verletzt worden? Bitte die jeweilige Beeinträchtigung oder Datenschutzverletzung detailliert beschreiben. Welche Maßnahmen wurden in den betroffenen Krankenhäusern getroffen, um derartige Vorfälle künftig zu vermeiden?
2. Welche einzelnen Krankenhäuser in Bremen und Bremerhaven gelten als kritische Infrastruktur im Sinne der BSI-KRITIS-Verordnung?
3. Wie schätzt der Senat die aktuelle IT-Sicherheitslage in den bremischen Krankenhäusern ein? Welche Maßnahmen wurden in den vergangenen zwei Jahren zur Verbesserung der IT-Sicherheitslage getroffen oder eingeleitet?
4. Welche weiteren Maßnahmen plant der Senat, um die IT-Sicherheit in den bremischen Krankenhäusern weiter zu stärken?
5. Wie hoch ist nach Einschätzung des Senats der aktuelle IT-Investitionsbedarf in den Krankenhäusern im Land Bremen?
6. Welche Krankenhäuser in Bremen und Bremerhaven haben bisher für welche ihrer Verfahren eine Datenschutz-Folgenabschätzung gemäß Artikel 35 der Datenschutz-Grundverordnung durchgeführt?
7. Welche Vorkehrungen werden in den Krankenhäusern getroffen, um die Infizierung durch Schadsoftware über eingehende E-Mails, USB-Speicher oder Webmail- und Cloud-Dienste zu verhindern?
8. In welchen Krankenhäusern in Bremen und Bremerhaven besteht ein Hinweisgebersystem, um die vertrauliche Meldung potentieller IT-Sicherheitsmängel zu ermöglichen?“

Der Senat beantwortet die Kleine Anfrage wie folgt:

1. In wie vielen Fällen seit der Antwort des Senats auf Drucksache 19/647 ist in Krankenhäusern im Land Bremen durch Schadsoftware oder Hackerangriffe der Betrieb beeinträchtigt oder der Schutz personenbezogener Daten verletzt worden? Bitte die jeweilige Beeinträchtigung oder Datenschutzverletzung detailliert beschreiben. Welche Maßnahmen wurden in den betroffenen Krankenhäusern getroffen, um derartige Vorfälle künftig zu vermeiden?

Seit der Antwort auf die Drucksache 19/647 (*IT-Sicherheit und Datenschutz in Krankenhäusern*) ist es lediglich in den AMEOS-Kliniken in Bremerhaven (AMEOS Klinikum Am Bürgerpark, AMEOS Klinikum Mitte Bremerhaven) zu einer Beeinträchtigung der IT-Systeme infolge eines Angriffes mit Schadsoftware gekommen. Die Schädigung der IT-Systeme in den AMEOS-Kliniken in Bremerhaven wurde durch Crypto-Ransomware verursacht; hierbei handelt es sich um Schadsoftware, die Computer sperrt oder Dateien verschlüsselt. Infolge des Virusbefalls wurden circa 100 Office-Dokumente auf Gruppenlaufwerken verschlüsselt und die Neuanmeldung an den Terminalservern unterbunden. Nach Angaben von AMEOS kam es durch den Vorfall zu keinem Datenverlust und es wurden keine Daten unbefugten Dritten zugänglich. In Reaktion auf den Vorfall wurden von der AMEOS Klinikum Bremerhaven GmbH alle Systeme mit möglichen Sicherheitslücken dauerhaft außer Betrieb genommen. Eine neue Antivirus-Lösung wurde in Ende 2018 auf allen Computern und Servern ausgerollt. Aktuell laufen alle IT-Systeme in den AMEOS Kliniken in Bremerhaven sicher und stabil.

2. Welche einzelnen Krankenhäuser in Bremen und Bremerhaven gelten als kritische Infrastruktur im Sinne der BSI-KRITIS-Verordnung?

Gemäß Anhang 5 zu § 6 Abs. 6 Nr. 2 der *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz* (BSI-Kritisverordnung – BSI-KritisV) gelten Krankenhäuser als kritische Infrastrukturen, wenn sie 30.000 oder mehr vollstationäre Behandlungsfälle im Jahr versorgen. Im Land Bremen erfüllt lediglich das Klinikum Bremen-Mitte (KBM) dieses Formalkriterium. Kritische Infrastrukturen im Sinne des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) sind Einrichtungen, Anlagen oder Teile davon, die (1.) den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, *Gesundheit*, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und (2.) von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Unabhängig vom oben genannten Formalkriterium ist anzunehmen, dass bereits der Ausfall von Krankenhäusern mit einer niedrigeren Zahl an vollstationären Behandlungsfällen pro Jahr, einen bedeutenden Einfluss auf das Funktionieren des Gemeinwesens ausüben würde, da unter Umständen eine Vielzahl von Patientinnen und Patienten durch andere Krankenhausstandorte mitversorgt werden müssten. Aus diesem Grund ist die Senatorin für Wissenschaft, Gesundheit und Verbraucherschutz der Auffassung, dass Krankenhäuser auch unabhängig vom Formalkriterium (Schwellenwert gemäß BSI-Kritisverordnung: jährliche Zahl an vollstationären Behandlungsfällen > 30.0000) als kritische Infrastrukturen angesehen werden sollten.

3. Wie schätzt der Senat die aktuelle IT-Sicherheitslage in den bremischen Krankenhäusern ein? Welche Maßnahmen wurden in den vergangenen zwei Jahren zur Verbesserung der IT-Sicherheitslage getroffen oder eingeleitet?

Es ist zu differenzieren zwischen gezielten Angriffen auf die IT-Infrastruktur von Krankenhäusern und eher indirekten Angriffen durch so genannte Drive-By-Attacken (beispielsweise durch das Aufrufen infizierter Internetseiten). Nach Einschätzung des Bundesamtes für Sicherheit und Informationstechnik richten sich Angriffe auf IT-Strukturen in der Regel nicht gezielt gegen Krankenhäuser. Die Krankenhäuser im Land Bremen aktualisieren vor diesem Hintergrund permanent ihre IT-Sicherheitsinfrastruktur, um sich an die dynamische Gefährdungslage anzupassen; in einer Reihe von Krankenhäusern gibt es neben Datenschutz- auch IT- und Informationssicherheitsbeauftragte, die in ihrer Gesamtheit die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von Informationen und informationstechnischen Systemen sicherstellen. Die Krankenhäuser betonen dabei, dass einer ausreichenden Sensibilisierung der Mitarbeiterinnen und Mitarbeiter in Fragen der IT- und Informationssicherheit eine ebenso hohe Bedeutung zukommt wie umfassenden und auf dem aktuellen Stand der Technik befindlichen Sicherheitssystemen. Darüber hinaus ist die Mehrzahl der Krankenhäuser auf dem Stadtgebiet Bremen trägerübergreifend im so genannten Arbeitskreis „*IT-Sicherheit der bremischen Krankenhäuser*“ organisiert. Der Arbeitskreis definiert unter anderem jährlich neue Prüfszenarien, die durch externe Dienstleister getestet werden. Zusätzlich berichtet das Landeskriminalamt seit 2017 dem Arbeitskreis zweimal pro Jahr über die übergeordnete IT-Sicherheitslage. Die Aktivitäten innerhalb des Arbeitskreises stellen eine wichtige Grundlage dar, um die IT- und Informationssicherheit an die dynamische Gefährdungslage anzupassen.

4. Welche weiteren Maßnahmen plant der Senat, um die IT-Sicherheit in den bremischen Krankenhäusern weiter zu stärken?

Mit dem *Gesetz zur Stärkung des Pflegepersonals* (Pflegepersonal-Stärkungsgesetz – PpSG) vom 11. Dezember 2018 wurden die Rahmenbedingungen und die Fördertatbestände zur Fortführung des Krankenhausstrukturfonds in den Jahren 2019-2022 in § 12a Krankenhausfinanzierungsgesetz (KHG) rechtlich geregelt. Das PpSG ist seit dem 01. Januar 2019 in Kraft. Gemäß § 12a Abs. 1 Nr. 3 KHG können auf Basis der erweiterten Förderkriterien unter anderem auch Vorhaben zur Verbesserung der informationstechnischen Sicherheit von Krankenhäusern finanziell gefördert werden. Hierzu zählen nach § 4 Abs. 1 Nr. 4 Krankenhausstrukturfonds-Verordnung (KHSFV) die Beschaffung, Errichtung, Erweiterung oder Entwicklung informationstechnischer oder kommunikationstechnischer Anlagen, Systeme oder Verfahren oder bauliche Maßnahmen, um die Informationstechnik der Krankenhäuser an die Voraussetzungen der BSI-Kritisverordnung und die Vorgaben des BSI-Gesetzes anzupassen. Sofern das Land Bremen die notwendige hälftige Ko-Finanzierung sicherstellt und die zu fördernden Vorhaben am 01. Januar 2019 noch nicht begonnen haben (§ 12a Abs. 3 Nr. 1 und 2 KHG), können im Zeitraum 2019-2022 bis zu 40 Mio. Euro für die Weiterentwicklung der Krankenhausversorgung genutzt werden. Die Senatorin für Wissenschaft, Gesundheit und Verbraucherschutz als zuständige Behörde wird sich in enger Abstimmung mit den Verbänden der Krankenkassen und den Krankenhäusern im Lande Bremen dafür einsetzen, auch Vorhaben zur Verbesserung der informationstechnischen Sicherheit von Krankenhäusern als wichtiges Handlungsfeld zu besetzen und durch entsprechende Investitionen zukunftssicher aufzustellen.

5. Wie hoch ist nach Einschätzung des Senats der aktuelle IT-Investitionsbedarf in den Krankenhäusern im Land Bremen?

Die Krankenhausgesellschaft der Freien Hansestadt Bremen weist in ihrer Stellungnahme zum Krankenhausinvestitionsprogramm 2018 darauf hin, dass Investitionen in eine zukunftssichere IT-Infrastruktur notwendig sind. Die Senatorin für Wissenschaft, Gesundheit und Verbraucherschutz teilt diese Auffassung. Die Krankenhäuser im Land Bremen weisen auf Anfrage einen unterschiedlichen IT-spezifischen Investitionsbedarf aus: Pauschal wird der Aufwand, der notwendig ist, um die Anforderungen der BSI-Kritisverordnung und der DS-GVO zu erfüllen, auf 300.000 bis 400.000 Euro je Krankenhausträger beziffert. Hierbei handelt es sich primär um Aufwendungen, die entstehen würden, wenn ein umfassendes Managementsystem für Informationssicherheit (engl. *information security management system*, ISMS) aufgebaut sowie eine entsprechende Auditierung vorbereitet und durchgeführt werden würde.

6. Welche Krankenhäuser in Bremen und Bremerhaven haben bisher für welche ihrer Verfahren eine Datenschutz-Folgenabschätzung gemäß Artikel 35 der Datenschutz-Grundverordnung durchgeführt?

Gemäß Artikel 35 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) ist eine Datenschutz-Folgenabschätzung (DSFA) insbesondere erforderlich, wenn spezifische Verarbeitungsvorgänge voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben. Die zuständige Aufsichtsbehörde (*Die Landesbeauftragte für Datenschutz*) erstellt und veröffentlicht nach Artikel 35 Abs. 4 DS-GVO eine Liste mit Verarbeitungsvorgängen, für die eine Datenschutz-Folgenabschätzung durchzuführen ist. Spezifische Verfahren speziell in Krankenhäusern sind bislang kein Bestandteil dieser Liste. Zu beachten ist dabei, dass das Fehlen von Verarbeitungstätigkeiten in der Liste nicht bedeutet, dass keine Datenschutz-Folgenabschätzung erforderlich ist. Es ist stattdessen Aufgabe des Verantwortlichen, mittels einer Vorabprüfung einzuschätzen, ob die Verarbeitung aufgrund ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke voraussichtlich ein hohes Risiko für die Rechte und Pflichten natürlicher Personen aufweist. Die Landesbeauftragte für den Datenschutz geht davon aus, dass bereits durch die umfangreiche Verarbeitung von Gesundheitsdaten nach Artikel 9 Abs. 1 DS-GVO eine Datenschutz-Folgenabschätzung nach Artikel 35 Abs. 3 Buchstabe b DS-GVO erforderlich ist. In der Leitlinie zur Datenschutzfolgeabschätzung wird eine solche Tätigkeit unter anderem bei der Verarbeitung von genetischen und medizinischen Daten in Krankenhausinformationssystemen angenommen und die Notwendigkeit einer Datenschutz-Folgeabschätzung als wahrscheinlich eingestuft. Die Krankenhäuser im Land Bremen haben zu folgenden Verfahren eine spezifische Datenschutz-Folgenabschätzung vorgenommen: Prozess der Patientinnen- und Patientendokumentation, IT-gestützte Kontrolle des Zugangs zu bestimmten Krankenhausbereichen, Videoüberwachung im Krankenhaus, Meldung von Menschen mit schweren Behinderungen nach § 163 SGB IX (Zusammenwirken der Arbeitgeber mit der Bundesagentur für Arbeit und den Integrationsämtern), Verarbeitung, Speicherung und Weiterleitung von Elektrokardiogrammen durch Anwendung von EKG-Daten-Management-Systemen.

7. Welche Vorkehrungen werden in den Krankenhäusern getroffen, um die Infizierung durch Schadsoftware über eingehende E-Mails, USB-Speicher oder Webmail- und Cloud-Dienste zu verhindern?

Die Risiken für die IT-Infrastruktur werden in allen Krankenhäusern des Landes Bremen grundsätzlich durch geeignete mehrstufige Sicherheitssysteme minimiert; in allen Krankenhäusern existieren dabei Notfallpläne, um adäquat auf die notwendige Abschaltung der IT-Systeme bei gezielten und massiven Angriffen reagieren zu können. In den Krankenhäusern kommen unter anderem die folgenden Maßnahmen zum Einsatz, um eine Infizierung durch Schadsoftware zu vermeiden: Einsatz von Virenscannern, Einsatz von Software zur Gerätesteuerung (so genannte Device-Control-Software) zur Überwachung und Kontrolle von USB-Anschlüssen und daran angeschlossenen Speichermedien, Schaffung isolierter Umgebungen (so genannte Sandboxverfahren) zur Testung neuer Software und Verfahren, Filtern von Inhalten durch den Einsatz von https- und URL-Filtern. Zusätzlich zu den genannten technischen Maßnahmen, werden die Mitarbeiterinnen und Mitarbeiter der Krankenhäuser regelmäßig über die aktuelle Gefahrenlage informiert (beispielsweise über interne Mailverteiler) und in Schulungen oder Fortbildungen für IT-spezifische Risiken sensibilisiert.

8. In welchen Krankenhäusern in Bremen und Bremerhaven besteht ein Hinweisgebersystem, um die vertrauliche Meldung potentieller IT-Sicherheitsmängel zu ermöglichen?

In circa der Hälfte der Krankenhäuser im Land Bremen werden aktuell anonyme Hinweisgebersysteme und Critical-Incident-Reporting-Systeme (CIRS) eingesetzt oder zeitnah eingeführt. Hierdurch besteht für die Mitarbeiterinnen und Mitarbeiter die Möglichkeit, vertraulich potenzielle IT-Sicherheitsmängel zu melden. Die genannten Systeme sind dabei in der Regel nicht IT-spezifisch ausgerichtet, sondern erfassen Beinahe-Zwischenfälle aus allen Krankenhausbereichen; die Meldungen werden themenspezifisch aufbereitet und an die jeweils zuständigen Abteilungen weitergeleitet. Die Krankenhäuser im Land Bremen verfolgen damit das Ziel, Risiken und Gefahren für Patientinnen und Patienten sowie Mitarbeiterinnen und Mitarbeiter sicht- und damit vermeidbar zu machen. Die verstärkte innerbetriebliche Transparenzherstellung wird von den Krankenhäusern als wichtige Voraussetzung dafür angesehen, um aus Beinahe-Zwischenfällen zu lernen und sich auf Ebene der Gesamtorganisation weiterzuentwickeln. Die Krankenhäuser betonen dabei, dass die genannten Systeme den persönlichen Kontakt zu Kolleginnen und Kollegen, Vorgesetzten, Betriebsräten, Datenschutz-, IT- und Informationssicherheitsbeauftragten nicht ersetzen, sondern sinnvoll ergänzen sollen.