BREMISCHE BÜRGERSCHAFT **Drucksache 19/647**
Landtag
19. Wahlperiode 14.06.16

Antwort des Senats auf die Kleine Anfrage der Fraktion der SPD

IT-Sicherheit und Datenschutz in Krankenhäusern

Antwort des Senats

auf die Kleine Anfrage der Fraktion der SPD
vom 10. Mai 2016

„IT-Sicherheit und Datenschutz in Krankenhäusern“

Die Fraktion der SPD hat folgende Kleine Anfrage an den Senat gerichtet.

In Krankenhäusern bündelt sich eine Vielzahl sensibler personenbezogener Daten. Seien es Informationen zum Gesundheitszustand von Patienten, deren Versicherungsdaten oder auch die Personaldaten der Belegschaft. Außerdem werden zahlreiche medizinische Geräte, zum Beispiel Narkoseautomaten oder Arzneimittelpumpen, mit Software betrieben.
In den letzten Wochen kam es besonders in Nordrhein-Westfalen vermehrt zu Berichten über attackierte IT-Systeme in Krankenhäusern, die zur sogenannten "kritischen Infrastruktur" gehören. Sogenannte Malware – Schadprogramme wie Viren und Trojaner – infizierten dabei die Netzwerke von Hospitälern und führten dazu, dass Systeme teilweise komplett heruntergefahren werden mussten. Die von Kriminellen entwickelten Programme, die teilweise Datenträger verschlüsseln und so größere Geldsummen zu erpressen versuchen, machten in Nordrhein-Westfalen Einsätze des dortigen Landeskriminalamtes nötig, bevor die Systeme Schritt für Schritt wieder hochgefahren werden konnten.

Vor diesem Hintergrund fragen wir den Senat:

1. Sind in allen bremischen Krankenhäusern Datenschutzbeauftragte angestellt?

2. Sind dem Senat Fälle bekannt, in denen die IT-Struktur von bremischen Krankenhäusern mit Schadsoftware angegriffen bzw. infiziert wurde?

3. Mit welchen Folgen ist bei einem Angriff mit Schadsoftware auf die IT-Systeme von Krankenhäusern zu rechnen? Würden Einschränkungen für die Behandlung von Patientinnen und Patienten entstehen und könnten daraus gesundheitliche Risiken – beispielsweise für Notfallpatientinnen und -patienten – resultieren?

4. Wie agieren bremische Krankenhäuser im Fall entsprechender Attacken? Gibt es Notfallpläne?

5. Wie wird die medizinische und pflegerische Behandlung von Patientinnen und Patienten auch im Falle eines Ausfalls von IT-Systemen sichergestellt?

6. Wie bewertet der Senat die Möglichkeit, dass kommunale Unternehmen wie die GeNo in regelmäßigen Abständen Berichte über ihre IT-Sicherheit vorlegen?

Der Senat beantwortet die Kleine Anfrage wie folgt:

Zu Frage 1

Sind in allen bremischen Krankenhäusern Datenschutzbeauftragte angestellt?

Eine Umfrage durch die Krankenhausgesellschaft der Freien Hansestadt Bremen e.V. hat ergeben, dass es in allen Krankenhäusern im Land Bremen gemäß § 9 BremKHDSG (Bremisches Krankenhausdatenschutzgesetz) entsprechend bestellte Datenschutzbeauftragte gibt. In einer Reihe von Krankenhäusern gibt es zusätzlich IT-Sicherheitsbeauftragte.

Zu Frage 2

Sind dem Senat Fälle bekannt, in denen die IT-Struktur von bremischen Krankenhäusern mit Schadsoftware angegriffen bzw. infiziert wurde?

Angriffe durch Schadsoftware in Emails oder durch infizierte Websites erfolgen täglich. Diese richten sich in der Regel allerdings – wie auch vom BSI (Bundesamt für Sicherheit und Informationstechnik) bestätigt – nicht gezielt gegen Krankenhäuser. Die Angriffe werden grundsätzlich in allen Krankenhäusern durch geeignete mehrstufige Sicherheitssysteme detektiert und abgewehrt. Vor dem Hintergrund der gezielten Attacke auf das St. Lukas Krankenhaus in Neuss in 2016 wurden die Sicherheitseinstellungen in einigen Krankenhäusern zeitweise verschärft. Teilweise wurden insbesondere die Mailsysteme weitaus höheren Sicherheitsstandards unterworfen, indem z.B. selbst Anhänge im Office-Dateiformat (Word, Excel, Power-Point – Dateien) zur Nichtweitergabe von Mails führten. Auch wurden die Mitarbeiterinnen und Mitarbeiter nochmals entsprechend sensibilisiert.

Es wurde bisher kein Krankenhaus im Land Bremen gezielt attackiert. Für die alltäglich vorkommende Schadsoftware waren die vorgehaltenen Sicherheitssysteme bisher erfolgreich.

Zu Frage 3

Mit welchen Folgen ist bei einem Angriff mit Schadsoftware auf die IT-Systeme von Krankenhäusern zu rechnen? Würden Einschränkungen für die Behandlung von Patientinnen und Patienten entstehen und könnten daraus gesundheitliche Risiken – beispielsweise für Notfallpatientinnen und -patienten – resultieren?

In den Krankenhäusern ist das mit dem Internet verbundene IT-Netzwerk von den medizintechnischen Netzwerken getrennt oder mit einer zusätzlichen separaten Firewall abgeschirmt.

Bei einem massiven Schadsoftware-Befall zentraler IT-Systeme würde die Patientenversorgung mit einem zusätzlichen Aufwand für den Informations- und Datenaustausch zwischen allen beteiligten Berufsgruppen sichergestellt werden müssen. Bei einer Umstellung der Dokumentation auf Papierform würde es zu Verzögerungen im Vergleich zum gewohnten Betriebsablauf kommen.

Gesundheitliche Risiken insbesondere für Notfallpatientinnen und –patienten werden als extrem unwahrscheinlich angesehen. Auch sind in der Regel Medizingeräte, die in der

Notfallversorgung eingesetzt werden, wie Defibrillatoren, Beatmungsgeräte und Infusionspumpen, nicht in das IT-Netzwerk eingebunden.

Zu Frage 4

Wie agieren bremische Krankenhäuser im Fall entsprechender Attacken? Gibt es Notfallpläne?

In allen bremischen Krankenhäusern existieren Notfallpläne in Bezug auf die notwendige Abschaltung der IT-Systeme bei gezielten massiven Attacken.

In den Krankenhäusern ist eine mehrstufige IT-Sicherheitsinfrastruktur vorhanden, die bis hin zu besonderen Datensicherungen reicht. Insofern wird ein IT-Ausfall analog zu anderen Bedrohungsszenarien (Katastrophen, Brand) behandelt und die Notfallpläne sind mit entsprechenden Maßnahmen hinterlegt.

Zu Frage 5

Wie wird die medizinische und pflegerische Behandlung von Patientinnen und Patienten auch im Falle eines Ausfalls von IT-Systemen sichergestellt?

Die zentralen medizinischen Geräte sind auch bei einem Ausfall von IT-Systemen weiterhin nutzbar. In einigen Bereichen gibt es Notfallsysteme (z.B. Notfalldrucker in der Radiologie). In anderen Bereichen würde der Umstieg auf Papier und die persönliche Weitergabe von Informationen die Weiterversorgung der Patientinnen und Patienten sicherstellen.

Zu Frage 6

Wie bewertet der Senat die Möglichkeit, dass kommunale Unternehmen wie die GeNo in regelmäßigen Abständen Berichte über ihre IT-Sicherheit vorlegen?

Es findet ein regelmäßiger Austausch mit der Gesundheit Nord über diverse Themen, die auch die IT-Systeme umfassen, statt. Eine darüberhinausgehende gesonderte Berichtspflicht über die IT-Sicherheit hält der Senat für nicht angezeigt. In der (Risiko)-berichterstattung an den GeNo-Aufsichtsrat wird regelmäßig das Thema IT-Sicherheit behandelt.