

Antwort

der Landesregierung

auf die Kleine Anfrage Nr. 3956

des Abgeordneten Dr. Rainer van Raemdonck (AfD-Fraktion)

Drucksache 6/9741

IT-Sicherheit in Krankenhäusern

Namens der Landesregierung beantwortet die Ministerin für Arbeit, Soziales, Gesundheit, Frauen und Familie die Kleine Anfrage wie folgt:

1. Wie viele Krankenhäuser im Land Brandenburg wurden seit den letzten fünf Jahren bereits attackiert bzw. waren Opfer einer sog. Cyberattacke?

Zu Frage 1: Der Landesregierung liegen dazu keine Angaben vor.

2. In wie vielen Fällen wurde der Betrieb eines Krankenhauses, in denen sog. Cyberangriffe stattgefunden haben, derart beeinträchtigt, dass eine medizinische Versorgung erschwert oder unmöglich gemacht worden ist? (Bitte aufschlüsseln nach Art der Beeinträchtigung und des Angriffes)

Zu Frage 2: Der Landesregierung liegen dazu keine Angaben vor.

3. Sind Fälle bekannt, in denen durch Cyberangriffe Daten von Patienten oder Mitarbeitern gefährdet waren bzw. erbeutet wurden? Wenn ja, in welcher Größenordnung ist der (potenzielle) Schaden jeweils zu beschreiben?

Zu Frage 3: Der Landesregierung liegen dazu keine Angaben vor.

4. Sind Fälle bekannt, in denen durch Cyberangriffe sensible Daten zur Sicherheit von Geräten und Objekten gefährdet waren bzw. erbeutet wurden? Wenn ja, in welcher Größenordnung ist der (potenzielle) Schaden jeweils zu beschreiben?

Zu Frage 4: Der Landesregierung liegen dazu keine Angaben vor.

5. Welche einzelnen Krankenhäuser im Land Brandenburg fallen unter die gesetzliche Meldepflicht als Betreiber kritischer Infrastruktur (KRITIS-Betreiber)?

Zu Frage 5: Entsprechend der Definition „Kritische Infrastrukturen“ sind dazu alle Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden, zu zählen. Das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) in Verbindung mit der BSIKritis-Verordnung gibt Kriterien und

Eingegangen: 14.11.2018 / Ausgegeben: 19.11.2018

Schwellwerte vor, anhand derer die unter das Gesetz fallenden Betreiber Kritischer Infrastrukturen eindeutig identifiziert werden. Damit fallen die beiden Krankenhäuser im Land Brandenburg (Potsdam und Cottbus), die die Schwellenwerte überschreiten, unter die Meldepflicht.

6. Wie schätzt die Landesregierung die IT-Sicherheitslage in den Krankenhäusern im Land Brandenburg ein? (Bitte Bedrohungsarten und Gegenmaßnahmen beschreiben)

Zu Frage 6: Aus polizeilicher Sicht dürften sich insbesondere Bedrohungsszenarien durch Hackerangriffe bzw. Angriffe mittels Schadstoffsoftware ergeben - ggf. mit der Zielrichtung der Erlangung von Patienten-/Gesundheitsdaten. Das Landesweite IT-Sicherheitsmanagement - zuständig für die IT-Sicherheit der Landesverwaltung (Kritis-Sektor „Staat und Verwaltungen“) - hat keine konkreten Informationen zur IT-Sicherheitslage der brandenburgischen Krankenhäuser. Gleichwohl schließt sich die IT-Leitstelle den allgemeinen Einschätzungen des BSI an. Grundsätzlich sind alle Bedrohungsarten gegen die IT-Sicherheitsziele Integrität, Vertraulichkeit und Verfügbarkeit auch für den Kritis-Sektor „Gesundheit“ aufzuzählen. Dazu gehört der Ausfall der Stromversorgung genauso wie der Befall von Schadsoftware der in den Krankenhäusern eingesetzten IT-Systeme. Insbesondere der Befall mit Ransomware (Verschlüsselungstrojaner) stellt eine enorme Bedrohung dar, da mit derartiger Schadsoftware eine Verschlüsselung - und damit Unbrauchbarmachung - von medizinischen Daten mit dem Ziel der Erpressung erfolgen kann. Ein weiteres Bedrohungsfeld für die o.g. Schutzziele eröffnet sich mit der Verbreitung des „Internet of Things“ (IoT). IoT bedeutet, dass in zunehmendem Maße Geräte zum Einsatz gelangen, die eine Betriebssteuerungsschnittstelle - insbesondere über das Internet anbieten. Folgende grundsätzliche Maßnahmen sollten zur Härtung der IT-Sicherheit ergriffen werden:

- Einführung und Betrieb eines Informationssicherheitsmanagementsystems (BSI-Grundsatz 200-2)
- Einführung und Betrieb eines Risikomanagementsystems (BSI-Grundsatz 200-3)
- Einführung und Betrieb eines Notfallmanagementsystems (BSI-Grundsatz 100-4)

Nach dem IT-Sicherheitsgesetz sind Betreiber Kritischer Infrastrukturen - sofern nicht andere Spezialregelungen bestehen - verpflichtet, die für die Erbringung ihrer wichtigen Dienste erforderliche IT nach dem Stand der Technik angemessen abzusichern und diese Sicherheit mindestens alle zwei Jahre überprüfen zu lassen. Sofern Sicherheitsmängel aufgedeckt werden, darf das BSI im Einvernehmen mit den Aufsichtsbehörden deren Beseitigung anordnen.

7. Was sind nach Einschätzung der Landesregierung die größten Bedrohungen für die IT-Sicherheit in den Krankenhäusern im Land Brandenburg?

Zu Frage 7: Aus polizeilicher Sicht geht die größte Bedrohung für die IT-Sicherheit in Krankenhäusern derzeit von Schadsoftware - insbesondere von sog. Ransomware - aus, da dadurch die gesamten digitalen Prozesse und Geschäftsabläufe des Krankenhausbetriebs beeinflusst werden könnten. Im Gegensatz zum Datenschutz - welcher vorrangig auf den Schutz von Persönlichkeitsrechten abstellt - stellt aus allgemeiner Sicht die IT-Sicherheit zunächst grundsätzlich einen Schutz von Werten dar. Davon abgeleitet ist der Schutz des physischen Lebens das am höchsten zu bewertende Schutzziel. In Ableitung aus diesem Kontext heraus sind daher die IT-Sicherheitsziele Verfügbarkeit und Integrität dem Schutzziel der Vertraulichkeit zunächst voranzustellen. In Abwägung demnach sind

die größten Bedrohungsszenarien die, die zunächst auf die Verfügbarkeit der Kritischen Infrastruktur „Krankenhaus“ abstellen. Diese betrifft jegliche Schadsoftware oder DDOS-Angriffe, die den Betrieb eines Krankenhauses gefährden. Dabei ist es unerheblich, ob Eingriffe in den regulären Krankenhausbetrieb direkt auf die medizinische Infrastruktur erfolgen oder indirekt auf Strukturen erfolgen, auf die die eigentlichen medizinischen Prozesse aufsetzen.

8. Wie hoch waren die Summen bzw. die Anteile am Gesamtbudget der einzelnen Krankenhäuser im Land Brandenburg, die jeweils in den einzelnen Krankenhäusern für die IT-Sicherheit aufgewendet wurden? (Bitte nach den letzten fünf Jahren und den einzelnen Krankenhäusern aufschlüsseln)

Zu Frage 8: Der Landesregierung liegen dazu keine Angaben vor.

9. Sind die vorgehaltenen Budgets zur Aufrechterhaltung der IT-Systeme ausreichend?

Zu Frage 9: Der Landesregierung liegen dazu keine Angaben vor.

10. Welche Maßnahmen sind von den Krankenhäusern zur Herstellung und Aufrechterhaltung der IT-Sicherheit zu ergreifen?

Zu Frage 10: Der Landesregierung liegen dazu keine auf jedes einzelne Krankenhaus bezogene Angaben vor. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe hat einen Leitfaden zum „Schutz Kritischer Infrastruktur - Risikomanagement im Krankenhaus“ als Handreichung erarbeitet, bei der die Anmerkungen und Kommentare einer interdisziplinär besetzten Arbeitsgruppe aus Unternehmen, Verbänden und Behörden berücksichtigt wurden. Diese Umsetzungshinweise wurden durch die Landeskrankenhausgesellschaft Brandenburg allen Mitgliedern im Dezember 2017 übergeben.

11. Welche Kosten kommen auf die einzelnen Krankenhäuser zu, damit die IT-Sicherheit in den Krankenhäusern in den nächsten Jahren gewährleistet werden kann?

Zu Frage 11: Der Landesregierung liegen dazu keine Angaben vor.

12. Welche Maßnahmen wurden in dieser Legislaturperiode bisher ergriffen, um die IT-Sicherheit der Krankenhäuser zu gewährleisten? (Bitte aufschlüsseln nach beratender und finanzieller Unterstützung sowie jeweils nach Jahren)

Zu Frage 12: In dieser Legislaturperiode werden die Krankenhäuser durch ein flexibles und planbares neues Instrument der Investitionspauschale gefördert. Die Verwendung der Investitionspauschale hat grundsätzlich im Rahmen des Krankenhausfinanzierungsgesetzes (KHG) zu erfolgen. Ansonsten haben die Krankenhäuser die freie Entscheidung, welche Prioritäten sie beim Einsatz der Mittel setzen. Damit ist die Investitionspauschale in der gesamten Legislaturperiode für IT-Maßnahmen einsetzbar. Darüber hinaus wurde für das laufende Haushaltsjahr das „Sonderprogramm Infrastrukturfonds Zukunft Brandenburg 2018“ für dringend notwendige Modernisierungsmaßnahmen der technischen Ausstattung aufgelegt. Mit dem Programm wurde die Investitionspauschale um 20 Mio. Euro auf 100 Mio. Euro im Haushaltsjahr 2018 erhöht. Die zusätzlichen Mittel fließen insbesondere für Digitalisierung den Krankenhäusern zu.