Abgeordnetenhaus BERLIN

Drucksache 18 / 17 268
Schriftliche Anfrage

18. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Dirk Stettner (CDU)

vom 10. Dezember 2018 (Eingang beim Abgeordnetenhaus am 12. Dezember 2018)

zum Thema:
IT-Sicherheit an Berliner Krankenhäusern

und **Antwort** vom 28. Dezember 2018 (Eingang beim Abgeordnetenhaus am 02. Jan. 2019)

Die Drucksachen des Abgeordnetenhauses sind bei der Kulturbuch-Verlag GmbH zu beziehen.
Hausanschrift: Sprosserweg 3, 12351 Berlin-Buckow · Postanschrift: Postfach 47 04 49, 12313 Berlin, Telefon: 6 61 84 84; Telefax: 6 61 78 28.

Senatsverwaltung für Gesundheit,
Pflege und Gleichstellung

Herrn Abgeordneten Dirk Stettner (CDU)

über

den Präsidenten des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

A n t w o r t
auf die Schriftliche Anfrage Nr. 18/17268
vom 10. Dezember 2018
über IT-Sicherheit an Berliner Krankenhäusern

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

1. In den Jahren 2011 und 2012 fand im Auftrag des Bundes das Projekt „Risikoanalyse Krankenhaus-IT“ (RiKrIT) statt. Was waren die Ergebnisse dieser Analyse und welche Auswirkungen haben sich dadurch für das Land Berlin und seine Krankenhäuser ergeben?

Zu 1.:

In dem Projekt „Risikoanalyse Krankenhaus-IT“ (RiKrIT) wurde ein Leitfaden und eine Methode entwickelt, mit der kritische IT-Abhängigkeiten in einem Krankenhaus und daraus erwachsende Risiken für die Patientenversorgung und weitere wichtige Prozesse identifiziert und bewertet werden können. Der Leitfaden entstand aus einer Initiative des Senats. Das Vorhaben wurde in den Jahren 2011 und 2012 unter Federführung des Bundesamts für Sicherheit in der Informationstechnik (BSI) und mit Beteiligung des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) sowie dem Unfallkrankenhaus Berlin (ukb) durch Auftragnehmer aus Industrie und Wissenschaft durchgeführt. Dieser Leitfaden steht nunmehr allen Krankenhäuser als Handlungsinstrument zur Verfügung. Damit sind die Grundlagen geschaffen, nach denen die Krankenhäuser in eigener Verantwortung eine Risikoanalyse im IT-Bereich durchführen können.

2. Inwiefern ist der Senat seiner Eigentümerverpflichtung gegenüber den landeseigenen Krankenhäusern in Bezug auf die IT-Sicherheit seit 2012 nachgekommen und welche Maßnahmen wurden getroffen?

Zu 2.:

Zum Krankenhaus des Maßregelvollzugs:
Ebenso wie die anderen Behörden des Landes Berlin unterliegt das Krankenhaus des Maßregelvollzugs - Krankenhausbetrieb des Landes Berlin (KMV) als Vollzugsbehörde - den seitens des IT-Dienstleistungszentrum (ITDZ Berlin) vorgegebenen IT-Sicherheitsstandards unmittelbar. Um höchstmögliche Datensicherheit zu gewährleisten betreibt das kommunale IT-Unternehmen daher zwei eigene, stark gesicherte Rechenzentren sowie das abgeschirmte Berliner Landesnetz. An dieses mehrfach gesicherte Hochgeschwindigkeitsnetz ist die komplette Verwaltung - also auch das Krankenhaus des Maßregelvollzugs - im Land Berlin angeschlossen. Für die gesamte IT-Infrastruktur sowie die Sicherheitsprozesse ist das ITDZ Berlin durch das Bundesamt für Informationstechnik (BSI) nach ISO 27001 zertifiziert.

Zu Vivantes Netzwerk für Gesundheit GmbH:
Die landeseigene Krankenhaus Vivantes Netzwerk für Gesundheit GmbH verantwortet als privatrechtliche Person ihre Gesamtnotfallkonzepte eigenverantwortlich.

Zur Charité:
Für die Charité dient ein erheblicher Teil der Maßnahmen im IT-Bereich auch der IT-Sicherheit.
Investitionen in den IT-Bereich erfolgen aus dem (allgemeinen) investiven Zuschuss sowie für verschiedene Maßnahmen als einzeln veranschlagte bauliche Maßnahmen bzw. Beschaffungen aus dem Landeshaushalt und SIWANA.

Der Senat wirkt gegenüber den landeseigenen Krankenhäusern auf die Qualitätssicherung und Weiterentwicklung des Risikomanagements hin.

3. In der Sitzung des Ausschusses für Gesundheit, Pflege und Gleichstellung am 3. Dezember 2018 hat die Senatorin angekündigt, sich des Themas IT-Sicherheit in 2019 in Berlin annehmen zu wollen. Was ist hier konkret zu wann geplant?

Zu 3.:

Im ersten Halbjahr des Jahres 2019 werden in zwei Berliner Krankenhäusern Übungen durchgeführt, in denen die Zusammenarbeit der IT-Sicherheit mit dem Krisenmanagement geübt wird. Die Erkenntnisse aus den Übungen sollen genutzt werden, den anderen Berliner Krankenhäusern Hinweise zu geben, wie Sie die Vorsorge weiter ausbauen können. Ferner wird nach Vorlage der Ergebnisse entschieden, ob neben dem unter Nr. 1 genannten Leitfaden und den Übungen weitere Unterstützungsmaßnahmen für die Krankenhäuser sinnvoll sind.

4. Wie viele Cyberangriffe hat es auf die Berliner Krankenhäuser seit 2012 gegeben und welche Auswirkungen hatte dies jeweils? Bitte jährlich nach Krankenhaus getrennt auflisten?

Zu 4.:

Wie unter Ziffer 5 ausgeführt, besteht keine Meldepflicht der Krankenhäuser gegenüber dem Senat. Deshalb liegen keine Informationen über Cyberangriffe vor.

5. Gilt eine behördliche Meldepflicht für Krankenhäuser zu Cyberangriffen? Falls ja, für wen gilt diese und wie viele Krankenhäuser betrifft dies in Berlin im Falle eines Cyberangriffs? Falls nein, warum nicht?

Zu 5.:

Die Meldepflichten bestehen ausschließlich gegenüber dem Bundesamt für Sicherheit in der Informationstechnik. Bestimmte Krankenhäuser müssen seit der Änderung der BSI-Kritisverordnung zum 1.7.2017 einer Meldepflicht gem. § 8b Absatz 4 BSI-Gesetz nachkommen, sofern die anhand der in der BSI-Kritisverordnung festgesetzten Schwellenwerte überschritten werden. In der BSI-Verordnung werden 30.000 vollstationäre Fallzahlen/Jahr als Richtgröße für Krankenhäuser festgelegt.

6. Wie gut sind die einzelnen Berliner Krankenhäuser nach Einschätzung des Senats in der IT-Sicherheit aktuell aufgestellt?

Zu 6.:

Hierzu bestehen ebenfalls keine Meldepflichten. Dem Senat liegen keine negativen Erkenntnisse vor.

7. Wie hoch ist nach Einschätzung des Senats der tatsächliche Investitionsbedarf an den einzelnen Krankenhäusern für die IT-Sicherheit?

Zu 7.:

Krankenhäuser sind in grundsätzlich allen Bereichen verpflichtet, notwendige Sicherheitsstandards einzuhalten und dazu alle erforderlichen Maßnahmen zu ergreifen, um sicherzustellen, dass die betriebenen Anlagen und genutzten materiellen Ressourcen den jeweils aktuellen technischen und gesetzlichen Anforderungen entsprechen. Seit der Änderung des Landeskrankenhausgesetzes (LKG) im Jahr 2015 und der Einführung der Investitionspauschale liegt die Verantwortung sowohl für die Betriebs- als auch für die Investitionskosten nunmehr in einer Hand bei den Krankenhäusern selbst. Sie agieren damit eigenverantwortlich und können flexibel entsprechend ihrer selbstgesetzten Prioritäten zeitnah notwendige Investitionen realisieren - auch für Maßnahmen der IT-Sicherheit.

Aussagen der Krankenhäuser zum Investitionsbedarf bzw. zur Höhe der Aufwendungen speziell im Bereich der IT-Sicherheit liegen dem Senat nicht vor.

8. Wie hoch war der Anteil der Krankenhausinvestitionen, den die Krankenhäuser seit 2012 im Schnitt für die IT-Sicherheit ausgegeben haben? Bitte jährlich angeben?

Zu 8.:

Die Plankrankenhäuser finanzieren ihre Investitionen aus Eigen- und Fördermitteln. Informationen zu aus Eigenmitteln finanzierten Investitionen liegen hier nicht vor. Die Fördermittel des Landes (Investitionspauschalen) werden von den Krankenhäusern eigenverantwortlich verwendet.

In den nach § 17 Absatz 1 Krankenhausförderungs-Verordnung einzureichenden Verwendungsnachweisen wird die Verwendung der Fördermittel dargestellt. Die Beschaffungen für IT-Technik wird nicht differenziert nach Anwendungsbereichen ausgewiesen. Der Anteil der Krankenhausinvestitionen für IT-Technik kann daher nicht beziffert werden.

Berlin, den 28. Dezember 2018

In Vertretung
Martin Matz
Senatsverwaltung für Gesundheit,
Pflege und Gleichstellung