Landtag Brandenburg **Drucksache 6/4310**
6. Wahlperiode

Antwort

der Landesregierung
auf die Kleine Anfrage Nr. 1672
der Abgeordneten Saskia Ludwig und Raik Nowka
CDU-Fraktion
Drucksache 6/4045

Cyberangriffe auf Brandenburger Krankenhäuser und Praxen – IT Sicherheitskonzept der Landesregierung

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

Vorbemerkungen der Fragesteller: Gemäß § 11 des Krankenhausgesetzes des Landes Brandenburg (LKGBbg) liegt die Rechtsaufsicht über die stationären Versorgungseinrichtungen bei dem für Gesundheit zuständigen Ministerium des Landes. Durch die zunehmende Vernetzung im Gesundheitswesen steigt für Krankenhäuser in Brandenburg das Risiko, Opfer von Viren, Trojanern, Würmern, Spyware, Spam und anderen Cyberattacken aus dem Netz zu werden. Immer lauter werden daher Forderungen nach einem IT-Risikomanagement, welches sich an Empfehlungen des Landes ausrichtet. Berichtet wird über medizinische Geräte, die über unzureichend geschützte Schnittstellen von außen erreichbar und in zentralen Funktionen manipulierbar sein könnten, wie etwa Röntgengeräte oder Infusionspumpen, deren Dosierung sich per Fernsteuerung verändern ließe. Auch sei es möglich, das Kühlsystem für Blutkonserven mitsamt Alarmsystem durch Manipulation abzuschalten. Zum Schutz der Patienten und um das Vertrauen in die Brandenburger Kliniken zu stärken ist Transparenz und eine vollumfängliche Darstellung der IT-Sicherheitslage notwendig. Auch eine Benennung, wie oft ein Zugriff auf vertrauliche Daten, etwa in psychiatrischen Kliniken, eine Manipulation oder Löschung von Daten, eine Gefährdung von Patienten (Ausfall, Manipulation von Geräten beziehungsweise Daten), sowie Sabotagen / Störungen der Betriebsabläufe oder Erpressungen von Brandenburger Krankenhäuser vorlagen, ist erforderlich. Die Landesregierung ist in der Pflicht, dass jeder Patient im Brandenburger Krankenhäusern sicher behandelt wird und dass seine Daten maximal geschützt werden.

Frage 1: Welche Kenntnisse liegen der Landesregierung über schwerwiegende Sicherheitslücken in medizinischen Netzwerken vor, die in Brandenburger Krankenhäusern und Praxen bestehen?

zu Frage 1: Der Landesregierung liegen dazu keine Erkenntnisse vor. Seitens der Landeskrankenhausgesellschaft Brandenburg (LKB) wurde auf Nachfrage bisher kein Fall gemeldet.

Datum des Eingangs: 01.06.2016 / Ausgegeben: 06.06.2016

Frage 2: Welche Konsequenzen hat die Landesregierung für Brandenburg gezogen, nachdem Berichte über die Ausbreitung von Computerviren in Krankenhäusern in Nordrhein-Westfalen Anfang Februar 2016 bekannt wurden?

zu Frage 2: Bei den in Rede stehenden Cyberangriffen auf Krankenhäuser wurde das lokale IT-Sicherheitsmanagement angegriffen. Dieses ist nicht Bestandteil der Telematikinfrastruktur und unterliegt damit auch nicht den Sicherheitsanforderungen der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH. Dies zeigt, dass es wichtig ist, dass das lokale Sicherheitsmanagement in Krankenhäusern und anderen Einrichtungen der medizinischen Versorgung kontinuierlich überprüft und auf ein hohes Sicherheitsniveau gebracht wird, um sensible Gesundheitsdaten zu schützen und die Patientensicherheit zu gewährleisten. Die LKB und Kliniken sind gefordert, Sicherungssysteme zu nutzen und zu aktualisieren.

Frage 3: Wie wird in Brandenburg sichergestellt, dass die hochsensiblen Patientendaten sowohl im ambulanten, als auch im stationären Bereich gegenüber Angriffen aus dem Netz vollständig geschützt sind?

zu Frage 3: Das IT-Sicherheitsgesetz, das am 25. Juli 2015 in Kraft getreten ist, bietet einen Ansatzpunkt zur Verbesserung der IT-Sicherheit in Krankenhäusern. Das Gesetz sieht für die Betreiber kritischer Infrastrukturen die Einhaltung von Mindeststandards hinsichtlich der IT-Sicherheit und Meldepflichten an das Bundesamt für Sicherheit in der Informationstechnik bei erheblichen IT-Sicherheitsvorfällen vor. Welches die kritischen Infrastrukturen sind, wird durch eine nicht zustimmungsbedürftige Rechtsverordnung des Bundesministeriums des Innern im Einvernehmen mit den jeweils betroffenen Ressorts bestimmt. Die LKB informiert zudem, dass die landes- und bundesrechtlichen Vorgaben zum Datenschutz in den Kliniken Anwendung finden, z. B. die Orientierungshilfe „Krankenhaus-Informationssysteme“ der Datenschutzbeauftragen des Bundes und der Länder bzw. das Krankenhausgesetz des Landes (LKGBbg) in Brandenburg.

Frage 4: Wie hoch ist der finanzielle Schaden in Brandenburg, der im ambulanten und stationären Bereich durch Angriffe aus dem Netz in den Jahren 2013 - 2015 entstanden ist?

zu Frage 4: Dazu liegen der Landesregierung keine Informationen sowie der LKB keine Meldungen aus den Mitgliedseinrichtungen vor.

Frage 5: Wie wird sichergestellt, dass in Brandenburger Kliniken regelmäßig Penetrationstests durchgeführt werden, um Schwachstellen in der IT-Infrastruktur herauszufinden?

zu Frage 5: Im Rahmen der Absicherung von IT-Netzwerken können IT-Sicherheits-Penetrationstests (IS-Penetrationstests) geeignet sein, um Schwachstellen aufzudecken. Verbindliche Vorgaben zur konkreten Ausgestaltung von IT-Sicherheitstests bestehen jedoch nicht. Unter Federführung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wurde ein Leitfaden zur Risikoanalyse von Krankenhaus-IT entwickelt. Dieser kann den Krankenhäusern als Orientierungshilfe dienen, wenn es darum geht, ihre IT-Systeme auf ein hohes Sicherheitsniveau zu bringen. In jedem Fall besteht die Möglichkeit einer fachlichen Kopplung mit dem BSI, um Sicherheitsanforderungen zu prüfen und zu gewährleisten.

Frage 6: Wie bewertet die Landesregierung den Netzwerksicherheitsstandard in Brandenburger Krankenhäusern?

zu Frage 6: Dazu liegen der Landesregierung keine Informationen vor, die eine Bewertung zulassen.

Frage 7: Wie groß fallen die durchschnittlichen finanziellen Ressourcen aus, die in Brandenburger Krankenhäusern für IT-Security zur Verfügung stehen?

zu Frage 7: Dazu liegen der Landesregierung keine Informationen vor.

Frage 8: Wie wird sichergestellt, dass z.B. bei der Fernwartung, die von den Krankenhäusern zu erfüllenden Datenschutzbestimmungen und gesetzlichen Auflagen eingehalten werden?

zu Frage 8: Die Orientierungshilfe „Krankenhaus-Informationssysteme“ der Datenschutzbeauftragten des Bundes und der Länder beschreibt datenschutzrechtliche Anforderungen an Hersteller und Betreiber von Krankenhaus-Informations-Systemen, die in eigener Verantwortung umgesetzt werden. Danach muss nachvollziehbar sein, welche Arbeiten im Rahmen der Fernwartung durchgeführt wurden, insbesondere welche Zugriffe auf personenbezogene Daten hierbei erfolgt sind. Hierzu müssen die Aktivitäten im Rahmen der Fernwartung (Zeitpunkt, Dauer, Art des Zugriffs) in entsprechenden Protokolldateien festgehalten werden. Das Krankenhaus muss seinerseits sicherstellen, dass eine Fernwartung nur im Einzelfall und mit Einverständnis des Krankenhauses erfolgen kann. Fernwartungsarbeiten müssen über verschlüsselte Verbindungen und unter separaten, über Identifikations- und Authentisierungsmechanismen geschützten Benutzerkennungen durchgeführt werden. Deren Zugriffsmöglichkeiten müssen auf das für die Durchführung der Wartungsarbeiten erforderliche Maß beschränkt sein; erforderlichenfalls sind mehrere Wartungskennungen einzurichten.

Frage 9: Wie wird sichergestellt, dass in Brandenburg verwendete Medizingeräte die gleichen Sicherheitskriterien (z.B. Malware-Schutzfunktion) erfüllen, die an IT-Komponenten im Hinblick auf den Betrieb in Netzwerken gestellt werden?

zu Frage 9: Für Medizinprodukte gelten spezialgesetzliche Regelungen (Medizinproduktegesetz), insbesondere hinsichtlich des Betriebs. Dies umfasst auch die Zulässigkeit von Änderungen am System, bspw. die Installation und Aktualisierung von Virenschutzmaßnahmen. Darüber hinaus existieren Normen auf dem Gebiet der Netzwerksicherheit im medizinischen Bereich, insbesondere die DIN EN 80001:2011, welche ein Risikomanagement in medizinischen IT-Netzwerken beschreibt.

Frage 10: Wie muss sich ein Brandenburger Krankenhaus verhalten, wenn z.B. ein Virus auf einem Beatmungsgerät festgestellt wurde, dies aber nicht „einfach ausgeschaltet“ werden kann?

zu Frage 10: Es ist immer davon auszugehen, dass das Krankenhaus ordnungsgemäß funktionierende, nicht virenverseuchte Medizingeräte einsetzt. Im Schadenfall ist ein Wechsel des Geräts, sofern vorhanden und nicht ebenfalls kompromittiert, bzw. die Beschaffung eines Ersatzgeräts mit dem Rettungswagen bzw. die Verlegung in ein anderes Krankenhaus bzw. einen Notdienst eine adäquate Alternative.

Frage 11: Wie ist die durchschnittliche personelle Ausstattung von Brandenburger Klinken mit spezialisiertem Netzwerk beziehungsweise Sicherheitspersonal?

zu Frage 11: Die Ausstattung des Krankenhauses ist maßgeblich von der Größe der Einrichtung abhängig und reicht von einzelnen Mitarbeitern bis zu einer ganzen Abteilung.

Frage 12: Wie wird sichergestellt, dass in Brandenburger Kliniken eingesetzten Gateways zwischen den Subnetzen und dem herkömmlichen Kliniknetzwerk kein Sicherheitsrisiko darstellen?

zu Frage 12: Dazu liegen der Landesregierung keine Informationen vor.

Frage 13: Über welche Gesamtstrategie bzgl. technischer und organisatorischer Sicherheitsmaßnahmen verfügt die Landesregierung, um Brandenburger Krankenhäuser effektiv vor Cyberangriffen zu schützen?

zu Frage 13: Mit dem Ende 2015 in Kraft getretenen E-Health-Gesetz wurden bereits wichtige Rahmenbedingungen zum Schutz des elektronischen Datenaustauschs im Gesundheitswesen festgeschrieben. Das bereits erwähnte IT-Sicherheitsgesetz bietet einen Ansatzpunkt zur Verbesserung der IT-Sicherheit in Krankenhäusern. Die Beratungen zur Bestimmung von Kritischen Infrastrukturen im Bereich Gesundheit werden unter Einbeziehung der Krankenhäuser auf Bundesebene geführt. Länderübergreifend wird festgelegt, welche Mindeststandards und Meldepflichten für Kritische Infrastrukturen bestehen. Ziel des Bundesministeriums für Gesundheit ist es, für maßgebliche Einrichtungen im Gesundheitswesen eine Erhöhung der IT-Sicherheit zu erreichen und diese deshalb in die Verordnung aufzunehmen. Diese Bemühungen werden durch die Landesregierung Brandenburg mitgetragen und unterstützt.

Frage 14: Welche aktuellen Forschungsprojekte und –vorhaben gibt es in Brandenburg, um ein höheres Sicherheitslevel in den Krankenhäusern (Netzwerksicherheit und Medizinprodukte) zu gewährleisten?

zu Frage 14: Dazu liegen der Landesregierung keine Informationen vor.

Frage 15: Wie viele Advanced Persistent Threats (komplexe, zielgerichtete Angriffe auf kritische IT-Infrastrukturen von medizinischen Netzwerken) wurden in den Jahren 2013 - 2015 verübt?

zu Frage 15: Dazu liegen der Landesregierung keine Informationen vor.

Frage 16: Wie viele Botnets wurden in den Jahren 2013 - 2015 in Brandenburger Kliniken verübt?

zu Frage 16: Dazu liegen der Landesregierung keine Informationen vor.