Landtag von Baden-Württemberg **Drucksache 16 / 5876**

16. Wahlperiode **09. 03. 2019**

Kleine Anfrage

der Abg. Dr. Rainer Podeswa und Carola Wolle AfD

und

Antwort

des Ministeriums für Soziales und Integration

Verbesserte Cybersicherheit in Krankenhäusern Baden-Württembergs nach Virenangriffen in den Jahren 2016 und 2017?

Kleine Anfrage

Wir fragen die Landesregierung:

1. Welche Krankenhäuser in Baden-Württemberg waren wann Opfer eines Cyberangriffs (bitte unter Nennung des Vorfalls)?

2. Welche Kenntnisse hat sie über gezahlte Gelder (Lösegeld) bei Erpressungen von Krankenhäusern?

3. Welche Folgen hatten die finanziellen Schäden der Virenattacken der Schadstoffsoftware „Locky“ (2016) und „WannaCry“ (2017) für den Etat der Krankenhäuser in Baden-Württemberg?

4. Welche direkten (falls betroffen) und indirekten (beispielsweise Umstellung von Prozessen) Auswirkungen hatten die Virenattacken der Schadstoffsoftware „Locky“ (2016) und „WannaCry“ (2017) für die Patientendaten der Krankenhäuser?

5. Welchen Maßnahmen zur Schulung der Mitarbeiter der Krankenhäuser wurden ergriffen, um bei erneuten Vorfällen bzw. der generellen Gefährdungslage durch Cyberangriffe adäquat und vor allem zeitnah reagieren zu können?

6. In welcher Form nimmt sie Warnungen (beispielsweise in der WirtschaftsWoche vom 4. Februar 2019 „Wenn der Klinik-Rechner zum Angriffsziel wird“) ernst, dass es nur eine Frage der Zeit ist, bis erneute Angriffe stattfinden und welche konkreten Maßnahmen hat sie seit dem letzten Cyberangriff zum Schutz der Daten in den Krankenhäusern des Landes ergriffen?

7. Wie setzt sie sich auf Bundesebene für ein staatliches Programm oder gemeinsames Vorgehen gegen Cyberkriminalität, speziell im Gesundheitswesen, ein?

Eingegangen: 09. 03. 2019 / Ausgegeben: 11. 04. 2019

8. Räumt sie der in Baden-Württemberg ansässigen IT-Branche und deren Produkten ein höheres Vertrauen in Bezug auf die Sicherung von Patientendaten und Abwehr vor Cyberangriffen ein bzw. unterstützt sie deren Förderung oder bevorzugt sie diese in (teil)staatlichen Einrichtungen, damit diese insbesondere zur Sicherung vor Cyberangriffen bevorzugt zum Einsatz kommt?

08. 03. 2019

Dr. Podeswa, Wolle AfD

Begründung

Nach Angriffen auf die Krankenhäuser durch die Schadsoftware „Locky“ wie im Februar 2016 und dem Erpresservirus „WannaCry“ im Mai 2017 sind die Möglichkeiten erneuter Angriffe, vor allem mit dem Ziel, sensible Patientendaten auszuspionieren, nach Expertenmeinungen weiterhin gegeben. Auch ist bekannt, dass es Krankenhäuser gab, die Lösegeld gezahlt haben, um wieder schnell an sensible Daten zu gelangen.

Antwort

Mit Schreiben vom 3. April 2019 Nr. 52-0141.5-016/5876 beantwortet das Ministerium für Soziales und Integration im Einvernehmen mit dem Ministerium für Inneres, Digitalisierung und Migration die Kleine Anfrage wie folgt:

1. Welche Krankenhäuser in Baden-Württemberg waren wann Opfer eines Cyberangriffs (bitte unter Nennung des Vorfalls)?

2. Welche Kenntnisse hat sie über gezahlte Gelder (Lösegeld) bei Erpressungen von Krankenhäusern?

3. Welche Folgen hatten die finanziellen Schäden der Virenattacken der Schadstoffsoftware „Locky“ (2016) und „WannaCry“ (2017) für den Etat der Krankenhäuser in Baden-Württemberg?

4. Welche direkten (falls betroffen) und indirekten (beispielsweise Umstellung von Prozessen) Auswirkungen hatten die Virenattacken der Schadstoffsoftware „Locky“ (2016) und „WannaCry“ (2017) für die Patientendaten der Krankenhäuser?

Die Krankenhäuser in Baden-Württemberg werden von kommunalen, privaten oder gemeinnützigen Trägern eigenverantwortlich betrieben. Sie sind nicht verpflichtet, dem Ministerium für Soziales und Integration Cyber-Sicherheitsvorfälle durch Schadprogramme und Fälle von digitaler Erpressung zu melden. Auch der Baden-Württembergischen Krankenhausgesellschaft e. V. (BWKG) liegen dazu keine Informationen vor.

Ungeachtet dessen weist die BWKG darauf hin, dass durch die laufend ergriffenen Absicherungs- und Abwehrmaßnahmen erhebliche Belastungen der Krankenhaus-IT-Abteilungen entstehen. Eine Übersicht über diese Maßnahmen liegt der BWKG aber ebenfalls nicht vor.

5. Welchen Maßnahmen zur Schulung der Mitarbeiter der Krankenhäuser wurden ergriffen, um bei erneuten Vorfällen bzw. der generellen Gefährdungslage durch Cyberangriffe adäquat und vor allem zeitnah reagieren zu können?

Die Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamtes Baden-Württemberg bietet für IT-Verantwortliche von Krankenhäusern spezielle Awarenessveranstaltungen an. Hierdurch werden die Vorgehensweisen der Cyberkriminellen und das Risikopotenzial anhand von zahlreichen Praxisbeispielen zielgruppengerecht aufgezeigt. Die dabei vermittelten konkreten Handlungsempfehlungen zur Risikominimierung und zum Umgang mit Cyberattacken können von den Verantwortlichen der Krankenhäuser im Bedarfsfall herangezogen werden.

Entsprechende Schulungen der ZAC wurden bereits bei Vertretern des Bundesverbandes der Krankenhaus-IT-Leiterinnen/Leiter e. V. und des Berufsverbandes Medizinischer Informatiker e. V. auf Landesebene durchgeführt. Weitere Veranstaltungen erfolgten bei der Bezirksärztekammer Süd-Württemberg und der Bezirksärztekammer Karlsruhe. Im Jahr 2018 fanden vier Awarenessveranstaltungen der ZAC bei und mit dem Bezug zu Krankenhäusern statt. Auch Veranstaltungen der IHK oder sonstige teilnehmeroffene Veranstaltungen zur Cybersicherheit werden nach Kenntnis der ZAC regelmäßig von Krankenhausvertretern besucht.

Aktuell werden mehrere Cyber-Krisenübungen für Betreiber kritischer Infrastrukturen durch die ZAC vorbereitet, in denen Notfallprozesse anhand von realistischen Angriffsszenarien erprobt werden. Im November 2019 ist die Durchführung einer Krisenübung zur Cyberkriminalität mit Vertretern aus diversen Krankenhäusern vorgesehen.

6. In welcher Form nimmt sie Warnungen (beispielsweise in der WirtschaftsWoche vom 4. Februar 2019 „Wenn der Klinik-Rechner zum Angriffsziel wird“) ernst, dass es nur eine Frage der Zeit ist, bis erneute Angriffe stattfinden und welche konkreten Maßnahmen hat sie seit dem letzten Cyberangriff zum Schutz der Daten in den Krankenhäusern des Landes ergriffen?

7. Wie setzt sie sich auf Bundesebene für ein staatliches Programm oder gemeinsames Vorgehen gegen Cyberkriminalität, speziell im Gesundheitswesen, ein?

Der Landesregierung sind die angesprochenen Probleme in der Datensicherheit bewusst und sie hat bereits entsprechende Schritte eingeleitet.

Eine Reihe von Förderprogrammen sind derzeit in der Bearbeitung, die die vielfältigen Themenschwerpunkte zum Thema Digitalisierung abbilden. Als erstes ist in dieser Reihung der Krankenhausstrukturfonds zu nennen, über den ab 2019 vier Jahre lang verschiedenste Fördertatbestände finanziert werden können. Explizit werden hier die Datennetzwerksicherheit und die telemedizinische Vernetzung als wichtige Eckpfeiler der Digitalisierung zur Förderung vom Bundesgesundheitsministerium vorgeschlagen. Diese Fördertatbestände sollen auch im Land Baden-Württemberg zur Umsetzung kommen.

Ein weiterer großer Baustein ist ein Digitalisierungsprogramm speziell für Krankenhäuser, das in diesem Jahr mit einem Volumen von 10 Mio. Euro zusätzlich zu den laufenden Programmen den Krankenhäusern zur Verfügung gestellt wird. Auch mit diesem Programm haben die Krankenhäuser die Möglichkeit entsprechende Kosten für Sicherheitsvorkehrungen im Datennetzwerk zu finanzieren.

Darüber hinaus steht für Ermittlungen im Bereich Cyberangriffe in der Fachabteilung Cybercrime und Digitale Spuren des Landeskriminalamtes Baden-Württemberg und den Fachinspektionen der regionalen Polizeipräsidien spezialisiertes Personal zur Verfügung.

Hinsichtlich der Sensibilisierung von Verantwortlichen in Krankenhäusern wird auf die Antwort zu Frage 5. verwiesen.

Die potenzielle Gefahr von Cyberattacken auf Krankenhäuser wurde ebenfalls im Rahmen der Bund-Länder-Projektgruppe (BLPG) Kritische Infrastrukturen (KRITIS) berücksichtigt. Diese auf Bundesebene hoch priorisierte BLPG wurde

in den Jahren 2017 und 2018 durch das Landeskriminalamt Baden-Württemberg mit dem Ziel geleitet, die polizeiliche Aufgabenbewältigung bei Cyberangriffen auf kritische Infrastrukturen in Deutschland zu optimieren. Die daraus resultierenden Handlungsempfehlungen befinden sich derzeit bei der Landespolizei Baden-Württemberg in der Umsetzung. Verantwortliche von Krankenhäusern waren in diese Projektgruppe ebenfalls eingebunden.

Angesichts des zunehmenden Risikos von Cyberangriffen wird auch die Notwendigkeit gesehen, eine ganzheitliche Cybersicherheitsstrategie zu erarbeiten und die landesweite Cybersicherheitsarchitektur auf den Prüfstand zu stellen. Die Vorbereitungen dafür hat das Ministerium für Inneres, Digitalisierung und Migration Anfang des Jahres 2019 aufgenommen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht in seinen stets aktuellen Lageberichten die Gefährdungslage der IT-Sicherheit in Deutschland. Aktuelle Informationen und Handlungsempfehlungen zum Schutz vor Schadprogrammen können auf der BSI-Webseite *www.bsi.bund.de* heruntergeladen werden.

8. Räumt sie der in Baden-Württemberg ansässigen IT-Branche und deren Produkten ein höheres Vertrauen in Bezug auf die Sicherung von Patientendaten und Abwehr vor Cyberangriffen ein bzw. unterstützt sie deren Förderung oder bevorzugt sie diese in (teil)staatlichen Einrichtungen, damit diese insbesondere zur Sicherung vor Cyberangriffen bevorzugt zum Einsatz kommt?

Das Ministerium für Inneres, Digitalisierung und Migration fördert aktuell Start-Ups im Bereich IT-Sicherheit im IT-Security-Lab am Cyberforum e. V. in Karlsruhe. Diese Förderung hat das Ziel, mit innovativen jungen IT-Sicherheitsunternehmen und deren Entwicklungen die digitale Souveränität der IT-Sicherheit in Baden-Württemberg zu stärken.

Lucha

Minister für Soziales
und Integration