LANDTAG NORDRHEIN-WESTFALEN
16. Wahlperiode

Drucksache **16/14486**

14.03.2017

Antwort

der Landesregierung

auf die Kleine Anfrage 5593 vom 14. Februar 2017
des Abgeordneten Daniel Schwerd FRAKTIONSLOS
Drucksache 16/14238

Wie sicher sind Daten im Gesundheitswesen in NRW?

Vorbemerkung der Kleinen Anfrage

In kaum einem anderen Lebensbereich werden von Bürgern immer mehr persönlich sensible Daten erhoben und auf digitalem Wege gespeichert wie im Bereich des staatlichen Gesundheitssystems. Zur gleichen Zeit erleben wir, dass Informationen aus dem Gesundheitswesen als das „neue Gold der Datenbranche“ betrachtet werden.

Im Silicon Valley werden derzeit umfassende Konzepte für das Data-Mining, Nudging und die Auswertung von Referenzwerten davon auf Patienten und Patientinnen entwickelt.

Die hochsensiblen Daten werden auf vielfältige Weise gewonnen. In zunehmendem Maße geschieht dies auch auf illegalem Wege durch Hackerangriffe auf Krankenhäuser und Versicherungen. So ist bekannt, dass es in der Gesundheitsbranche 340% mehr Hackerangriffe und Zwischenfälle, die Datensicherheit betreffend gibt, als im Durchschnitt in der restlichen Industrie.[1]

Die Ministerin für Gesundheit, Emanzipation, Pflege und Alter hat die Kleine Anfrage 5593 mit Schreiben vom 13. März 2017 namens der Landesregierung im Einvernehmen mit dem Minister für Inneres und Kommunales beantwortet.

1. Welche Informationen liegen der Landesregierung darüber vor, wie sich die Anzahl der Hackerangriffe auf Datensätze im Bereich des Gesundheitswesens in den letzten fünf Jahren in Nordrhein-Westfalen entwickelt hat?

[1] http://www.politico.eu/article/ransomware-in-health-care-draft/

Datum des Originals: 13.03.2017/Ausgegeben: 17.03.2017

4. Welche Erkenntnisse besitzt die Landesregierung über die Urheber dieser Hackerangriffe?

5. Wie hoch beurteilt die Landesregierung den finanziellen Schaden, der durch derartige Angriffe entstanden ist? Geben Sie bitte eine jährliche Einschätzung für den Zeitraum von 2012 bis heute.

Die Fragen 1, 4 und 5 werden gemeinsam beantwortet.

Hackerangriffe auf Daten des Gesundheitswesens werden in der Polizeilichen Kriminalstatistik nicht in aggregierter Form ausgewiesen. Die zur Beantwortung der Frage erforderliche Einzelfallauswertung kann im Rahmen der für die Beantwortung einer Kleinen Anfrage zur Verfügung stehenden Zeit nicht durchgeführt werden.

Im Rahmen der Meldepflicht nach § 42a BDSG und § 83a SGB X werden vereinzelt Sachverhalte zur Kenntnis an die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI.NRW) gegeben, die eine unrechtmäßige Kenntniserlangung von besonders schutzwürdigen (Sozial-)Daten zum Gegenstand haben. Hierbei handelt es sich in der Regel nicht um gezielte Angriffe von außen, sondern um individuelle Versäumnisse oder sonstiges Fehlverhalten einzelner Personen. Meldungen aus den letzten fünf Jahren im Zusammenhang mit gezielten Hackerangriffen auf IT-Infrastrukturen liegen nicht vor. Auch aus Bürgereingaben haben sich bisher keine solchen Erkenntnisse ergeben.

Die in den Medien bekannt gewordenen Ransomware-Attacken auf Krankenhäuser werden durch die Krankenhausaufsicht aufmerksam verfolgt. Dabei handelt es sich jedoch nicht um gezielte Angriffe zur Erlangung von Gesundheitsdaten. Die Schadsoftware verschlüsselt Dateien, um ein Lösegeld für die Entschlüsselung zu erpressen. Die Angriffe erfolgen meist nicht gezielt auf Einrichtungen des Gesundheitswesens, sondern nach dem Gießkannenprinzip, d. h. die Schadsoftware wird breit gestreut, beispielweise per E-Mail. Einrichtungen wie Krankenhäuser oder die gesetzlichen Krankenversicherungen unterliegen im Ereignisfall keiner Meldepflicht an die Aufsichtsbehörden. Der Landesregierung liegen daher nur Informationen zu einzelnen Fällen vor. Eine repräsentative Erhebung dieser Vorfälle aus den letzten fünf Jahren war innerhalb der für die Beantwortung der Kleinen Anfrage zur Verfügung stehenden Frist nicht möglich. Patientendaten oder die Patientenversorgung waren in keinem der bekannten Fälle gefährdet.

Erkenntnisse über die Urheber der Hackerangriffe sowie gegebenenfalls entstandene finanzielle Schäden durch die Angriffe liegen der Landesregierung nicht vor.

2. Welche Maßnahmen hat die Landesregierung ergriffen, um Daten aus dem Gesundheitsbereich besser vor Hackern zu schützen? Nennen Sie bitte auch den genauen Zeitpunkt der beschlossenen Maßnahmen.

Ransomware-Attacken und sonstige Angriffe auf IT-Systeme mit Viren sind kein neues Phänomen und verpflichten die Krankenhäuser schon aus Eigeninteresse zunächst selbst, entsprechende Sicherheits- und Sicherungsmaßnahmen zu ergreifen. Die Krankenhausgesellschaft Nordrhein-Westfalen hat die Problematik ebenfalls aufgegriffen und alle Mitgliedskrankenhäuser sensibilisiert. Krankenhäuser erhalten zudem Unterstützung bei der Prävention und Aufklärung solcher Vorfälle durch die Polizei Nordrhein-Westfalen. Das Landeskriminalamt Nordrhein-Westfalen (LKA) führt zur Cybercrime auch Präventionsveranstaltungen für Wirtschaftsunternehmen durch. Dies schließt Unternehmen

aus dem Gesundheitsbereich ein. Eine statistische Erfassung der beratenen Unternehmen erfolgt hingegen nicht.

Krankenhäuser können die Ausgaben für IT-Sicherheit aus den Mitteln für die „Wiederbeschaffung kurzfristiger Anlagegüter“ finanzieren, die die Krankenhäuser in Nordrhein-Westfalen seit zehn Jahren als pauschale Zuwendung vom Land erhalten. Für das Jahr 2017 wurde die jährliche Zuwendung von 317 Millionen Euro auf 323 Millionen Euro angehoben. Wie diese Mittel im Einzelnen verwendet werden, obliegt den jeweiligen Einrichtungen.

Ergänzend wird auf die NIS-Richtlinie (Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union) hingewiesen, die den EU-weiten Aufbau nationaler Kapazitäten für die Cyber-Sicherheit, eine stärkere Zusammenarbeit der Mitgliedstaaten der Europäischen Union sowie Mindestsicherheitsanforderungen und Meldepflichten für bestimmte Dienste vorsieht. Die Richtlinie ist am 8. August 2016 in Kraft getreten und muss bis zum 9. Mai 2018 in nationales Recht umgesetzt werden. Die europarechtlichen Vorgaben wurden weitestgehend bereits durch das am 18. Juli 2015 in Kraft getretene IT-Sicherheitsgesetz in deutsches Recht umgesetzt. Es sind weitere Änderungen, unter anderem im BSI-Gesetz (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik), sowie die Ergänzung des § 291b SGB V vorgesehen. Im Gesundheitswesen ergibt sich aus den Regelungen ein begrenzter Erfüllungsaufwand für bestimmte Telekommunikationsanbieter, für die gematik sowie für weitere Betreiber sogenannter „Kritischer Infrastrukturen“. Ebenso entsteht für die Anbieter digitaler Dienste durch die Verpflichtung zur Einhaltung der Mindestsicherheitsanforderungen und die Einführung von Meldepflichten für bestimmte IT-Vorfälle ein Erfüllungsaufwand, der sich derzeit jedoch nicht quantifizieren lässt. Auch der Kreis der betroffenen Anbieter kann derzeit nicht konkret benannt werden.

3. Wie haben sich die ergriffen Maßnahmen auf die Datensicherheit in NRW im Gesundheitsbereich ausgewirkt?

Welche konkreten Maßnahmen die jeweiligen Einrichtungen aus den Informationen durch das LKA oder die KGNW (Krankenhausgesellschaft Nordrhein-Westfalen) abgeleitet haben oder in welchem Umfang die zur Verfügung stehenden Mittel für IT-Sicherheit eingesetzt werden, wird weder durch die Polizei Nordrhein-Westfalen noch die Aufsichtsbehörden recherchefähig erhoben. Der Landesregierung liegen hierzu keine verwertbaren Daten vor.