LANDTAG NORDRHEIN-WESTFALEN
17. Wahlperiode

Drucksache **17/5634**

02.04.2019

Antrag

der Fraktion der AfD

IT-Infrastruktur der Krankenhäuser in Nordrhein-Westfalen stärken – Patientenschutz sichern

I. Ausgangslage

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat für die zweite Jahreshälfte 2018 eine deutliche Zunahme von Hacker-Angriffen auf Betreiber kritischer Infrastrukturen registriert.

Alleine in diesem Zeitraum gingen insgesamt 157 Meldungen über IT-Sicherheitsvorfälle beim BSI ein. In den Jahren zuvor war die Anzahl der Meldungen wesentlich geringer. (Gesamtjahr 2017/2018: 145 Meldungen, 2016/2017: 34 Meldungen.[1])

Zur kritischen Infrastruktur gehören nach der „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV)“ folgende Sektoren: Energie, Wasser, Ernährung, Information und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr sowie Staat und Verwaltung, Medien und Kultur.

Ab 30.000 stationären Fällen pro Jahr zählt beispielsweise laut Anhang 5 des BSI-KritisV ein Krankenhaus zur sogenannten kritischen Infrastruktur. Laut Verordnung muss dieses Krankenhaus innerhalb von zwei Jahren u.a. seine IT-Sicherheit auf den „aktuellen Stand der Technik“ (§8a IT-Sicherheitsgesetz) bringen sowie Problemfälle an das BSI (§8b IT-Sicherheitsgesetz) weiterleiten.

Hiernach unterliegen in NRW jedoch nur 21 von 344 Krankenhäusern den Kriterien nach BSI KritisV und zählen zu der vom Bund überwachten kritischen Infrastruktur.

Krankenhäuser mit geringeren Fallzahlen zählen nicht zur kritischen Infrastruktur und unterliegen somit auch nicht der Überwachung durch das BSI. Diesen Krankenhäusern wird wie bisher auch freigestellt, wie sie ihre IT-Infrastruktur schützen.

[1] https://www.heise.de/newsticker/meldung/Mehr-Hacker-Angriffe-auf-kritische-Infrastruktur-beim-BSI-gemeldet-4311172.html

Datum des Originals: 02.04.2019/Ausgegeben: 04.04.2019

Das IT-Sicherheitsdebakel des damals noch als „digitaler Leuchtturm“ geltenden Lukas-Krankenhauses in Neuss ist vielen Menschen noch bekannt. Hacker hatten 2016 mit einer „Ransom-Ware-Attacke“ über E-Mail die gesamte IT-Ausstattung und damit den gesamten Medizinbetrieb des Krankenhauses für Wochen lahmgelegt. Der Schaden wurde auf über eine Million Euro geschätzt.[2]

Die Probleme des Lukas-Krankenhauses hatten über Wochen Auswirkungen auf die ganze Region, da diese Klinik in der dortigen Versorgungslandschaft ein zentraler Akteur ist. Krankenhäuser der Umgebung mussten die Versorgung der Patienten übernehmen. Befände das Krankenhaus sich im ländlichen Bereich, hätte der Angriff möglicherweise dramatische Auswirkungen auf die Gesundheit oder gar das Leben der betroffenen Patienten gehabt. Da die Einrichtung jedoch „nur“ 28.942 stationäre Fälle jährlich betreut (Stand 2017), findet die KRITIS-Verordnung hier bisher keine Anwendung und fände sie bei Beibehaltung der Kriterien auch in Zukunft nicht.

Deutschlandweit fallen nur 110 Krankenhäuser unter diese Einordnung. Der Marburger Bund äußerte sich schon 2017 kritisch zu dem Schwellenwert[3]; seitdem hat sich jedoch nichts an den Kriterien der Einstufung geändert.

Die 2016 prognostizierte Konsolidierung der Krankenhäuser in Bezug auf die technische Infrastruktur hat sich nicht eingestellt. Das BSI meldet verstärkte Hackeraktivitäten gegenüber der kritischen Infrastruktur. Die deutsche Cyberabwehr präsentiert sich als Flickenteppich. Bundes- und Landesbehörden betreiben jeweils eigene Cyberabwehrabteilungen.

Hatte die vorige Landesregierung 2016 noch auf die gute Finanzausstattung der Krankenhäuser in NRW verwiesen,[4] ergab eine aktuelle Studie von KPMG, dass die Krankenhäuser in NRW für die nächsten fünf Jahre allein ihren IT-Investitionsbedarf auf ca. 344 Mio. Euro pro Jahr einschätzen.[5]

Wer angesichts dieser Finanznöte noch von einer funktionierenden Selbstverantwortung der Krankenhäuser beim Aufbau einer gut gesicherten und essentiellen IT-Infrastruktur spricht, verkennt die Realitäten.

Zwar läuft seit Januar 2019 eine erweiterte Förderung über das Krankenhausfinanzierungsgesetz (KHG); hier greifen die durch das Pflegepersonal-Stärkungs-Gesetz (PpsG) im §12a KHG neu hinterlegten Fördertatbestände auch bei Investitionen zur IT-Sicherheit in Krankenhäusern ab Januar 2019. Die Gesamtfördersumme aus dem Krankenhausstrukturfonds sowie eine mind. 25prozentige Kofinanzierung durch die Länder ergibt Fördermittel von ca. 0,75 bis 1 Mrd. Euro pro Jahr. Den Krankenhäusern in NRW würden nach dem Königsteiner Schlüssel ca. 105 Mio. Euro (Bund) sowie mindestens 26 Mio. Euro (Land) als Förderung zur Verfügung stehen. Das jedoch immer unter der Voraussetzung, dass die Träger der Krankenhäuser ihren Anteil von bis zu 25% für die geförderten Vorhaben eigenständig aufbringen können.

Allerdings gilt hier die Priorität der IT-Sicherheitsförderung bei Krankenhäusern, welche, um die die Voraussetzungen des Anhangs 5 Teil 3 der BSI-Kritisverordnung zu erfüllen, ihr IT-

[2] https://www.heise.de/newsticker/meldung/Trojaner-im-OP-wie-ein-Krankenhaus-mit-den-Folgen-lebt-3617880.html
[3] https://www.marburger-bund.de/bundesverband/pressemitteilung/kritis-einstufung-schwellenwert-fuer-krankenhaeuser-ueberpruefen
[4] Landtag Nordrhein-Westfalen, Plenarprotokoll 16/106
[5] https://hub.kpmg.de/die-geschäftsführung-spricht-klartext-krankenhäuser-in-nrw

Sicherheitsmanagement an die Vorgaben von § 8a des BSI-Gesetzes anpassen müssen. In NRW trifft das auf 21 Krankenhäuser zu. Die übrigen 323 Kliniken und allgemeinen Krankenhäuser würden nicht von diesem Fördertopf für die Ausstattung ihrer IT-Systeme profitieren.

Darüber hinaus hat das Land NRW durch sein 2018 verabschiedetes Entfesselungspaket I, zusätzlich zur bisherigen pauschalen Förderung von Investitionen, in § 21a des Krankenhausgestaltungsgesetzes NRW (KHGG NRW) eine Einzelförderung von Investitionen ermöglicht. Dafür stehen von 2018 bis 2021 insgesamt zusätzliche 600 Millionen Euro zur Verfügung. Allerdings wurde 2018 in den Förderkriterien nicht der Aufbau oder Ausbau von IT-Systemen oder Maßnahmen der Verbesserung von IT-Sicherheit hinterlegt. 2018 waren die Förderschwerpunkte „Qualitätsverbesserung der Versorgung von Menschen mit seltenen Erkrankungen sowie die Versorgung von schwerkranken Kindern und Jugendlichen“.[6] Zu erwarten ist, dass sich die Förderschwerpunkte im Jahre 2019 ebenfalls nicht auf die Verbesserung der IT-Sicherheit in Krankenhäusern beziehen werden.

Da diese Mittel für den Abbau des Investitionsstaus aber nicht ausreichen und, angesichts der Finanznöte mancher Krankenhäuser, nicht einmal die prozentual geringen Eigenmittel für die Finanzierung aufzubringen sind, ist eine zusätzliche niedrigschwellige Förderung zur Steigerung der IT-Sicherheit aller Krankenhäuser in NRW dringend vonnöten.

Angesichts des weiterhin dramatischen Investitionsstaus bei der IT-Sicherheit sowie der sich weiterhin verschlechternden Finanzausstattung der Krankenhausträger und der am tatsächlichen Investitionsbedarf der IT-Infrastruktur vorbeigehenden bisherigen Förderungen von Bund und Land muss die Landesregierung, die sich die Digitalisierung als Kernthema auf die Fahne geschrieben hat, das Heft in die Hand nehmen und die IT-Sicherheit und den Datenschutz in den Krankenhäusern von NRW signifikant voranbringen. Dazu sollte sie ein zweckgebundenes Sonderinvestitionsprogramm „IT-Sicherheit im Gesundheitssystem“ auflegen.

Möglich wäre hier beispielsweise ein eigenständiges Projekt der NRW.Bank. Darin könnten analog zum Förderprogramm „Gute Schule 2020“ IT-Investitionen der Krankenhäuser gefördert werden.

Alternativ dazu könnte der § 21a des Krankenhausgestaltungsgesetzes NRW (KHGG NRW) dahingehend geändert werden, dass im Förderzeitraum bis 2021, zusätzlich zu den jährlichen Förderschwerpunkten, die Förderung der IT-Sicherheit permanent festgeschrieben wird.

Ziel soll es sein, dass bis 2021 alle Krankenhäuser in NRW dem „Branchenspezifischen Sicherheitsstandard“ (B3S) für die medizinische Versorgung nach BSI-KritisV genügen. Dieser Standard (nach „Umsetzungsplan kritische Infrastrukturen“ (UP KRITIS)) orientiert sich u.a. an den Anforderungen der Norm ISO 27001 und den für das Gesundheitswesen spezifischen Anforderungen nach ISO 27799.

Ergänzend zu den Sachinvestitionen muss weiterhin und möglichst verpflichtend in das IT-Sicherheitsgrundwissen der Mitarbeiter investiert werden.

Weiterhin müssen diejenigen Krankenhäuser, die unmittelbar von den Kriterien der im Juni 2017 in Kraft getretenen Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) für den Sektor Gesundheitsversorgung betroffen waren und damit zur kritischen Infrastruktur zählen, bei Bedarf durch kurzfristige Investitionsförderungen in ihren Bemühungen unterstützt

[6] https://www.mags.nrw/sites/default/files/asset/document/faq_zur_einzelfoerderung.pdf

werden, damit sie nach der Übergangsfrist von zwei Jahren, die Verpflichtungen aus dem IT-Sicherheitsgesetz bis zum Juni 2019 einhalten können.

II. Der Landtag stellt fest:

1. Die Sicherstellung der Gesundheitsvorsorge der Bürger muss für das Land oberste Priorität haben.
2. Die IT-Infrastruktur der Krankenhäuser in Nordrhein-Westfalen ist häufig veraltet und entspricht nicht dem aktuellen Stand.
3. Die IT-Sicherheit der Krankenhäuser in Nordrhein-Westfalen liegt in der Regel weit unter den Mindestanforderungen des IT-Sicherheitsgesetzes.
4. Die nach BSI-KritisV erfolgte Klassifizierung von Krankenhäusern nach stationären Fallzahlen ist kein geeignetes Bewertungskriterium für deren regionale Systemrelevanz.
5. In Zeiten des digitalen Wandels und der zunehmenden Vernetzung ist eine funktionierende und gut abgesicherte IT-Infrastruktur für Krankenhäuser von entscheidender Bedeutung.
6. Die bisherige Förderpraxis ist nicht ausreichend, um die dringend benötigten Investitionslücken der Krankenhäuser zu schließen.

III. Der Landtag fordert die Landesregierung auf,

1. ein Konzept zu entwickeln, das die Finanzierung der Investitionen in die IT-Infrastruktur und die IT-Sicherheit der Krankenhäuser am realen Bedarf orientiert;
2. die Finanzierung dieser Infrastruktur, angesichts der kritischen finanziellen Ausstattung der Krankenhausträger, vollumfänglich aus Landesmitteln zu bestreiten;
3. sicherzustellen, dass bis 2021 sämtliche Krankenhäuser in NRW den „Branchenspezifischen Sicherheitsstandard“ (B3S) für die medizinische Versorgung nach BSI-KritisV erfüllen, auch wenn sie aufgrund einer zu geringen Anzahl stationärer Fälle nicht als kritische Infrastruktur (nach BSI-KritisV) gelten.

Sven W. Tritschler
Dr. Martin Vincentz
Markus Wagner
Andreas Keith

und Fraktion