**Kleine Anfrage zur kurzfristigen schriftlichen Beantwortung
gemäß § 46 Abs. 2 GO LT
mit Antwort der Landesregierung**

Anfrage der Abgeordneten Björn Försterling, Susanne Victoria Schütz und Lars Alt (FDP)

Antwort des Niedersächsischen Ministeriums für Soziales, Gesundheit und Gleichstellung namens der Landesregierung

Hackerangriffe auf Kliniken

Anfrage der Abgeordneten Björn Försterling, Susanne Victoria Schütz und Lars Alt (FDP), eingegangen am 31.08.2021 - Drs. 18/9852
an die Staatskanzlei übersandt am 02.09.2021

Antwort des Niedersächsischen Ministeriums für Soziales, Gesundheit und Gleichstellung namens der Landesregierung vom 16.09.2021

Vorbemerkung der Abgeordneten

Am 14. Juli 2021 hat die Stadt Wolfenbüttel mitgeteilt, dass nach einer Hacker-Attacke auf das IT-System des Klinikums die Computersysteme vorsorglich heruntergefahren worden seien. Nach bisherigen Erkenntnissen wollten die Hacker Geld vom Klinikum erpressen. Nach Angaben der Niedersächsischen Krankenhausgesellschaft sind vergleichbare Vorfälle in Niedersachsen nicht bekannt, bundesweit habe es aber in den vergangenen Jahren vereinzelt Fälle gegeben (vgl. *HAZ* vom 16. Juli 2021 S.8 „Hacker-Attacke auf Klinikum: Spezialisten ermitteln“).

Innenminister Boris Pistorius (SPD) äußerte sich in diesem Zusammenhang mit der Aussage: „Cyberangriffe dieser Art sind aktuell eine der größten Bedrohungen, der wir als Gesellschaft gegenüberstehen“ (vgl. *HAZ* vom 16. Juli 2021 S.8 „Hacker-Attacke auf Klinikum: Spezialisten ermitteln“).

Vorbemerkung der Landesregierung

Die Gefährdungslage durch Cyberbedrohungen ist weiterhin auf einem hohen Niveau und gestaltet sich zunehmend komplex. Unterschiedliche Gruppen von Angreifenden agieren mit Angriffswerkzeugen, die in früheren Zeiten hochprofessionellen Organisationen zugeschrieben wurden. Selbst technischen Laien ist es mittlerweile durch allgemein zugängliche Informationen und komplette Quellcodes von Schadsoftware für Lösegelderpressung (Ransomware) möglich, sich an den Lösegelderpressungen über das Geschäftsmodell „Ransomware as a Service (RaaS)“ zu beteiligen. Hierbei werden gegen entsprechende finanzielle Beteiligungen Infrastruktur, Werkzeuge und Anleitungen für potenzielle Angreifende zur Verfügung gestellt. Daher stellt insbesondere Ransomware derzeit eine der bedeutendsten Cyberbedrohungen dar.

Mit dem Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit (NDIG) hat der Landtag die Initiative der Landesregierung aufgegriffen, für die Behörden und Gerichte des Landes, deren IT-Systeme mit dem Landesdatennetz verbunden sind, einen Sicherheitsverbund zu definieren. Jedes Mitglied des Sicherheitsverbundes hat auf der Basis von Risikoanalysen eine dem Schutzbedarf der verarbeiteten Daten und der Bedrohungslage angemessene Informationssicherheit, auch im Hinblick auf andere Mitglieder des Sicherheitsverbundes, zu gewährleisten. Für weite Bereiche der Verwaltung sind durch die niedersächsische Leitlinie zur Gewährleistung der Informationssicherheit (ISLL) und das darauf basierende Informationssicherheitsmanagementsystem (ISMS) der niedersächsischen Landesverwaltung untergesetzliche Regelungen getroffen worden, die der Gewährleistung der Informationssicherheit für die unmittelbare Landesverwaltung dienen. Der Bundesgesetzgeber hat mit dem Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) u. a. eine Ausweitung der Pflichten für Betreiber Kritischer Infra-

strukturen und Regelungen für Unternehmen im besonderen öffentlichen Interesse getroffen. In diesem Zusammenhang ist auch die Datenschutzgrundverordnung zu nennen, die für die Verarbeitung personenbezogener Daten festlegt, dass geeignete technische und organisatorische Maßnahmen getroffen werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

1. Was hat die Landesregierung bisher unternommen, dieser Bedrohung für Kliniken entgegenzuwirken bzw. Maßnahmen gegen solche Bedrohungen zu unterstützen?

In ihrer eigenen Verantwortung für den Betrieb sind die Krankenhäuser ebenfalls für den sicheren Betrieb ihrer Datenverarbeitung verpflichtet.

Darüber hinaus hat der Gesetzgeber mit dem neu geschaffenen § 75 c SGB V die Krankenhäuser ab dem 01.01.2022 verpflichtet, „nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind."

Hierfür wird auf Bundesebene derzeit unter Federführung der DKG ein Konzept zur Definition des Stands der Technik entwickelt, das - auch in Abstimmung mit dem BSI - die Krankenhäuser bei der Einhaltung der gesetzlichen Vorgaben unterstützen soll. Hieran ist die NKG über die Beteiligung an den verantwortlichen Gremien beteiligt.

Mit folgenden zwei Maßnahmen stellen der Bund und die Landesregierung zusätzliche Mittel speziell für den Ausbau der IT-Sicherheit in Krankenhäusern zur Verfügung:

Krankenhauszukunftsfonds

Mit dem Krankenhauszukunftsfonds nach § 14 a KHG werden Fördermittel von bundesweit insgesamt ca. 4,3 Milliarden Euro für die Digitalisierung bereitgestellt, die nach dem Königsteiner Schlüssel den einzelnen Bundesländern zugewiesen werden, sodass auf Niedersachsen ca. 406 Millionen Euro entfallen. Der Gesetzgeber hat hierbei eine Aufteilung der Förderbeträge dahin gehend vorgesehen, dass die Bundesebene einen Anteil von 70 % trägt, während die restlichen 30 % entweder durch das jeweilige Bundesland oder den Krankenhausträger aufgewendet werden.

Diesen Anteil hat das Land Niedersachsen in Höhe von insgesamt knapp 129 Millionen Euro komplett übernommen.

Für die insgesamt elf Fördertatbestände des Krankenhauszukunftsfonds ist jeweils ein Mindestanteil von 15 % für Investitionen in IT-Sicherheit vorgesehen, was bei Berücksichtigung des Landesanteils einem rechnerischen Betrag von ca. 19 Millionen Euro entspricht.

Der Fördertatbestand 10 „Informationssicherheit" sieht dezidiert Maßnahmen zur Verbesserung der IT- bzw. Cybersicherheit in Krankenhäusern vor.

Für diesen Fördertatbestand haben aktuell 62 Krankenhäuser in Niedersachsen Anträge in Höhe einer Fördersumme von 19 756 579 Euro gestellt, die vom Ministerium für Soziales, Gesundheit und Gleichstellung (MS) zur Antragsstellung an das Bundesamt für Soziale Sicherung bearbeitet werden. Bei Bewilligung trägt das Land Niedersachsen hiervon eine Summe von 5 926 974 Euro.

Krankenhausstrukturfonds und Förderung kritischer Infrastrukturen

Zur Fortführung der Förderung von Vorhaben der Länder zur Verbesserung der Strukturen in der Krankenhausversorgung werden dem beim Bundesamt für Soziale Sicherung errichteten Strukturfonds in den Jahren 2019 bis 2024 weitere Mittel in Höhe von insgesamt bis zu 2 Milliarden Euro aus der Liquiditätsreserve des Gesundheitsfonds zugeführt. Im Rahmen des Strukturfonds können Krankenhäuser, die nach § 8 a BSIG als kritische Infrastrukturen identifiziert wurden, Anträge auf Unterstützung bei der Erfüllung der im Rahmen der BSI-KritisV gestellten, branchenspezifischen Sicherheitsstandards (B3S) zur Förderung der IT-Sicherheit stellen. Das MS hat sich hierbei intensiv für die Unterstützung der Antragstellerinnen und Antragsteller eingesetzt.

2. Plant die Landesregierung vor dem Hintergrund des konkreten Falls in Wolfenbüttel, zusätzliche Maßnahmen bzw. die Unterstützung von Maßnahmen gegen diese Art von Bedrohung?

Über die unter 1. genannten Maßnahmen sind keine Maßnahmen vor dem Hintergrund des konkreten Falls in Wolfenbüttel vorgesehen.

3. Welche Bereiche/Strukturen sind nach Ansicht der Landesregierung abgesehen von Kliniken in Niedersachsen gefährdet, und wie plant sie, diese zu unterstützen?

Cyberkriminelle greifen sowohl öffentliche Institutionen, Unternehmen oder auch Privatpersonen an. Sofern es sich nicht um nachrichtendienstlich gesteuerte Cyberangriffe handelt, steht nach bisheriger Erkenntnislage regelmäßig ein finanzielles Interesse im Vordergrund. Cyberkriminelle mit dem Hintergrund Ransomware unterscheiden bei der Auswahl ihrer Opfer nicht nach den Kategorien Verwaltung, Wirtschaft oder kritischen Infrastrukturen (KRITIS), sondern nach leicht anzugreifenden sowie kurz- bis mittelfristig finanziell lohnenden Zielen. Daher sind grundsätzlich auch alle Bereiche der öffentlichen Verwaltung und der Privatwirtschaft durch Cyberangriffe gefährdet.

Im Bereich der Strafverfolgung werden angesichts der zunehmenden Professionalisierung der Cyberkriminellen in Niedersachsen im Rahmen organisatorischer Anpassungen neue Fachkommissariate Cybercrime in den Zentralen Kriminalinspektionen der Polizeidirektionen eingerichtet, um noch spezialisierter gegen Cyber-Kriminelle ermitteln zu können. Im Landeskriminalamt Niedersachsen wird zur Unterstützung der neuen Kommissariate im Rahmen der dortigen Organisationsanpassung zusätzlich eine QuickReactionForce-Einheit eingerichtet, um die Reaktionsfähigkeit bei Angriffen auf kritische Cyberinfrastrukturen sowie auf Unternehmen und Behörden zu verbessern.

Im Bereich Prävention für die Wirtschafts- und KRITIS-Unternehmen in Niedersachen bieten die Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamtes sowie der Wirtschaftsschutz für geheimschutzbetreute Unternehmen zahlreiche Beratungsleistungen an. Die ZAC bietet zudem über ihre Webseite umfangreiche Informationen über die unterschiedlichen Varianten von Cyberangriffen an und stellt dort u. a. einen Newsletter zu aktuellen Cybercrime-Phänomenen zur Verfügung.

Das Niedersächsische Computer Emergency Response Team (N-CERT) nimmt die gesetzlichen Aufgaben des § 14 NDIG sowie untergesetzliche Aufgaben der ISLL wahr. Es steht mit seinen Beratungs- und Unterstützungsleistungen sowohl der niedersächsischen Landesverwaltung als auch den Kommunalverwaltungen zur Verfügung.

(Verteilt am 17.09.2021)