Bayerischer Landtag

19. Wahlperiode 05.04.2024 Drucksache 19/637

Schriftliche Anfrage

der Abgeordneten **Andreas Krahl, Benjamin Adjei BÜNDNIS 90/DIE GRÜNEN**
vom 30.01.2024

Cyberattacken auf bayerische Krankenhäuser

Krankenhäuser und Pflegeeinrichtungen werden immer häufiger zum Ziel von Cyberattacken. Erst kürzlich wurden die Bezirkskliniken Mittelfranken Opfer eines Hackerangriffs, bei dem sich Angreifer Zugang zu den Systemen der IT-Infrastruktur der Bezirkskliniken Mittelfranken verschafften und gezielt Daten verschlüsselt wurden, wie in einer Pressemitteilung am 28. Januar 2024 bekannt gegeben wurde. Auch ein großflächiger Angriff auf bayerische Kliniken mit vielen Ausfällen ist ein denkbares Szenario.

Die Staatsregierung wird gefragt:

Antwort

des Staatsministeriums für Gesundheit, Pflege und Prävention im Einvernehmen mit dem Staatsministerium des Innern, für Sport und Integration und dem Staatsministerium für Wissenschaft und Kunst
vom 29.02.2024

Vorbemerkung:
Eine Recherche im Vorgangsverwaltungssystem der Bayerischen Polizei (IGVP-FE) gestaltet sich bei der angegebenen Fragestellung aufwendig, ein entsprechender Katalogwert für Krankenhäuser oder Kliniken ist nicht vorhanden.

Ebenfalls ist „Cyberangriff“ kein klar definierter Begriff. Unter den Begriff „Cyberangriff“ wurden sowohl Verschlüsselungen mittels Ransomware als auch erfolgreiche Phishing-E-Mails sowie Erpressungsmails und Angriffe gegen Telefonanlagen von Krankenhäusern subsumiert. Neben normalen Krankenhäusern bzw. Kliniken wurden auch Spezialpraxen berücksichtigt.

Im Rahmen der im Jahr 2020 von der Staatsregierung ins Leben gerufenen Cyberabwehr Bayern (CAB) werden Fälle von Cybercrime, Cyberspionage oder andere Angriffe auf staatliche IT-Infrastruktur ausgetauscht. Bei der CAB handelt es sich um eine behördeninterne Informations- und Kooperationsplattform für alle mit Cybersicherheitsaufgaben betrauten bayerischen Behörden und Einrichtungen. Zu diesen zählen:

– das Cyber-Allianz-Centrum (CAZ) im Landesamt für Verfassungsschutz,
– die Zentrale Ansprechstelle Cybercrime (ZAC) im Landeskriminalamt,
– die Zentralstelle Cybercrime Bayern (ZCB) bei der Generalstaatsanwaltschaft Bamberg,
– das Landesamt für Sicherheit in der Informationstechnik (LSI),
– das Landesamt für Datenschutzaufsicht (LDA) sowie
– der Landesbeauftragte für den Datenschutz (LfD).

Erkenntnisse zu einer koordinierten Vorgehensweise speziell gegen den Gesundheitssektor in Deutschland liegen den bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben derzeit nicht vor. Ein Zusammenhang einzelner Sachverhalte kann derzeit weder ausgeschlossen noch bestätigt werden. Insgesamt sind Gesundheitseinrichtungen wie Krankenhäuser ein lohnendes Ziel für Cyberakteure, weil mit dem Ausfall regelmäßig weitreichende Auswirkungen verbunden sein können und die Daten sensibel sind.

Bei der Antwort zu Frage 1 werden zunächst die vom Staatsministerium für Wissenschaft und Kunst (StMWK) gemeldeten Daten genannt, die sich aus einer Abfrage bei den Universitätsklinika ergeben haben. Danach folgen die vom Staatsministerium des Innern, für Sport und Integration (StMI) übermittelten Zahlen, denen als Datenquelle das Vorgangsverwaltungssystem IGVP-FE der Bayerischen Polizei sowie Erkenntnisse aus den wöchentlichen Lagebesprechungen der CAB zugrunde liegen und die neben Universitätsklinika auch Krankenhäuser, Kliniken und Spezialpraxen umfassen, sofern bei der Polizei Anzeige erstattet wurde.

1.a) Wie viele Cyberangriffe gab es in den Jahren 2021–2024 auf bayerische Krankenhäuser (bitte aufschlüsseln nach Jahr und Regierungsbezirk)?

Aus einer Abfrage an den Universitätsklinika ergeben sich die folgenden Zahlen (Angaben zu den Regierungsbezirken Niederbayern und Oberfranken erfolgen nicht, da sich dort keine Universitätsklinika befinden):

2021:

1. Oberbayern: 3
2. Oberpfalz: 0
3. Mittelfranken: für 2021 liegen keine Zahlen vor
4. Unterfranken: 0
5. Schwaben: 0

2022:

1. Oberbayern: 3
2. Oberpfalz: 0
3. Mittelfranken: 2
4. Unterfranken: 0
5. Schwaben: 0

2023:

1. Oberbayern: 10
2. Oberpfalz: 0
3. Mittelfranken: 0
4. Unterfranken: 0
5. Schwaben: 0

2024:

1. Oberbayern: 0
2. Oberpfalz: 0
3. Mittelfranken: 0
4. Unterfranken: 0
5. Schwaben: 0

Hingewiesen wird darauf, dass in keinem Fall ein erfolgreicher Cyberangriff vorlag und dass nicht bei jedem erfolgten Cyberangriff eine Anzeige erstattet wurde.

Die Bayerische Polizei hat folgende Zahlen übermittelt:

– 2021: 6 Fälle
– 2022: 6 Fälle
– 2023: 9 Fälle
– 2024: 1 Fall

Hinweis zu den letztgenannten Zahlen: Als Datenquelle für die Beantwortung wurden das Vorgangsverwaltungssystem IGVP-FE der Bayerischen Polizei sowie Erkenntnisse aus den wöchentlichen Lagebesprechungen der CAB verwendet. Die zugrunde liegenden Falldaten sind dynamischen Veränderungen unterworfen. Somit sind statistische Auswertungen und Analysen nicht möglich, sondern als Lageerkenntnisse zu werten, die stets nur den aktuellen Erfassungsstand zum Zeitpunkt der Abfrage wiedergeben. Diese Erkenntnisse können sich in Bezug auf rückwirkende Zeiträume durch laufende Ermittlungen und Qualitätssicherungsmaßnahmen kontinuierlich ändern. Gleichwohl lassen sich anhand der jeweiligen Entwicklungen Tendenzen feststellen und zueinander in Verhältnis setzen. In diesen Zahlen enthalten sind neben Krankenhäusern, Kliniken und Spezialpraxen auch Universitätskliniken, sofern bei der Polizei Anzeige erstattet wurde.

Eine Aufschlüsselung nach Regierungsbezirken ist technisch nicht möglich. Als Alternative können die Vorgänge auf die Präsidien der Bayerischen Landespolizei und das Landeskriminalamt (BLKA) aufgeschlüsselt werden.

– PP München: 4
– PP Mittelfranken: 3
– PP Niederbayern: 2
– BLKA: 4
– PP Oberbayern Nord: 1
– PP Oberbayern Süd: 1
– PP Oberpfalz: 1
– PP Unterfranken: 2
– PP Schwaben Süd/West: 4

1.b) Ist seit Beginn des bewaffneten Konfliktes in der Ukraine eine Zunahme an Cyberangriffen auf bayerische Krankenhäuser zu verzeichnen?

Wie an der Aufschlüsselung nach Jahren unter Frage 1 a zu erkennen ist, besteht eine steigende Tendenz bei der Begehung von „Cyberangriffen“ auf Krankenhäuser oder Kliniken, welche aufgrund der geringen Fallzahl nicht aussagekräftig ist. Ebenso kann aus der Datenlage keine Aussage zur Kausalität im Hinblick auf den Angriffskrieg getroffen werden.

2.a) Wie viele Fälle aus den Jahren 2021–2024 sind der Staatsregierung bekannt, in denen durch Schadsoftware oder Hackerangriffe der Betriebsablauf von Kliniken und Krankenhäusern beeinträchtigt wurde (bitte aufschlüsseln nach der Art der Beeinträchtigung)?

Im angefragten Zeitraum wurden bezüglich der Universitätsklinika keine Fälle bekannt, im Übrigen kamen vier Fälle von Computersabotage zur Anzeige. Eine Auswertung dahin gehend, inwieweit der Betriebsablauf dadurch beeinträchtig wurde, ist nicht möglich. Im Übrigen darf auf die Vorbemerkung verwiesen werden.

2.b) Sind der Staatsregierung Fälle bekannt, in denen eine Cyberattacke auf eine Klinik Auswirkungen auf den Gesundheitszustand der Patientinnen und Patienten hatte?

Den Sicherheitsbehörden liegen hierzu keine Erkenntnisse vor. Im Übrigen darf auf die Vorbemerkung verwiesen werden.

3. Wie schätzt die Staatsregierung den aktuellen Zustand der IT-Sicherheit und -Infrastruktur in bayerischen Krankenhäusern ein (bitte aufschlüsseln nach Regierungsbezirk)?

Die Staatsregierung schätzt den aktuellen Zustand der IT-Sicherheit und -Infrastruktur in bayerischen Universitätsklinika, nicht zuletzt angesichts der oben dargelegten Befunde, als gut ein. Die Staatsregierung ist sich bewusst, dass es sich um einen kritischen, sensiblen Bereich handelt, der eine stetige Anpassung und Adaption der Schutzmaßnahmen erfordert.

Für den Bereich der Plankrankenhäuser ist darauf hinzuweisen, dass diese eigenständige Unternehmen und nicht Bestandteil der Staatsverwaltung sind. Daher entscheiden sie über ihre innerbetrieblichen Angelegenheiten in eigener Verantwortung. Dies gilt auch dafür, mit welchen technischen Lösungen sich Krankenhäuser vor möglichen Cyberangriffen schützen und damit die gesetzlichen Vorgaben nach § 75c Sozialgesetzbuch (SGB) Fünftes Buch (V) – Pflicht, nach dem Stand der Technik angemessene Vorkehrungen zum Schutz der informationstechnischen Systeme zu treffen – einhalten. Dem Staatsministerium für Gesundheit, Pflege und Prävention (StMGP) liegen keine Anhaltspunkte vor, dass diese Verpflichtung von den Krankenhäusern nicht beachtet wird.

4. Wie wird gerade im Krankenhausbereich sichergestellt, dass IT-Sicherheit bei Förderprojekten immer mitgedacht wird?

5.a) Was hat die Staatsregierung bisher unternommen, der Bedrohung durch Cyberattacken auf Krankenhäuser entgegenzuwirken?

5.b) Wie unterstützt die Staatsregierung Krankenhäuser, welche Opfer eines Hackerangriffs geworden sind?

5.c) Plant die Staatsregierung vor dem Hintergrund des konkreten Falls der Bezirkskliniken Mittelfranken zusätzliche Maßnahmen bzw. die Unterstützung von Maßnahmen gegen Cyberattacken?

Aufgrund des Sachzusammenhangs werden die Fragen 4 bis 5 c gemeinsam beantwortet.

Die Staatsregierung unternimmt große Anstrengungen, um die bayerischen Universitätsklinika auch im IT-Bereich nach Kräften zu unterstützen, und stellt den Universitätsklinika daher umfangreiche Mittel zur Digitalisierung zur Verfügung. Die Förderung durch die Staatsregierung bezieht sich dabei sowohl auf Investitionen im IT-Bereich allgemein als auch auf die IT-Sicherheit der bayerischen Universitätsklinika. Ergänzend hierzu wird die IT-Sicherheit durch die Staatsregierung im Rahmen der Förderung durch den Krankenhauszukunftsfonds unterstützt.

Wie unter Frage 3 ausgeführt sind die bayerischen Plankrankenhäuser gesetzlich verpflichtet, geeignete Maßnahmen zum Schutz der IT-Infrastruktur zu ergreifen. Dabei entscheiden die Krankenhäuser eigenverantwortlich unter Berücksichtigung der individuellen Gegebenheiten und Bedürfnisse vor Ort. Für Investitionen stehen hierzu die pauschalen Fördermittel aus dem Krankenhausförderetat zu Verfügung, die 2024 um 20 Mio. Euro auf insgesamt rd. 316 Mio. Euro erhöht wurden und von den Trägern eigenverantwortlich – etwa auch für Digitalisierungsprojekte – eingesetzt werden können.

Darüber hinaus stehen den Plankrankenhäusern insgesamt rd. 590 Mio. Euro aus dem Krankenhauszukunftsfonds des Bundes zur Verfügung. Die notwendige Ko-Finanzierung in Höhe von rd. 180 Mio. Euro wurde hierbei vom Freistaat Bayern unternommen. Die Mittel aus dem Krankenhauszukunftsfonds sind insbesondere für Investitionen in die IT-Sicherheit vorgesehen. Damit steht den bayerischen Plankrankenhäusern ein erhebliches Mittelvolumen zur Verfügung.

6.a) Wie schätzt die Staatsregierung die Versorgungssicherheit für bayerische Patientinnen und Patienten im Falle eines großflächigen Hackerangriffs auf mehrere Krankenhäuser mit vielen Ausfällen ein?

6.b) Ist die Staatsregierung auf ein solches Szenario ausreichend vorbereitet?

Die Fragen 6a und 6b werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Wie unter Frage 3 ausgeführt, besteht eine gesetzliche Verpflichtung der Krankenhäuser, angemessene Vorkehrungen zu treffen, um die IT-Infrastruktur vor Angriffen zu schützen. Das StMGP geht davon aus, dass aufgrund dieser Verpflichtung auch im Fall eines Angriffs der Betrieb so weit aufrechterhalten werden kann, dass eine Versorgung im Regelfall – ggf. im eingeschränkten Umfang – fortgeführt werden kann. Sollte dies im Einzelfall nicht der Fall sein, ist eine Versorgung der Patientinnen und Patienten gleichwohl sichergestellt. Mit über 400 Krankenhausstandorten von wohnortnaher Grundversorgung bis hochspezialisierter Spitzenmedizin ist die Versorgung in Bayern flächendeckend auf hohem Niveau gesichert.

6.c) Wie stellt die Staatsregierung die Cybersicherheit von übergreifenden Bettenmanagementprogrammen wie z. B. IVENA sicher?

Die Integrierten Leitstellen (ILS) führen für ihren jeweiligen Zuständigkeitsbereich gemäß Art. 2 Abs. 3 Integrierte Leitstellen-Gesetz (ILSG) einen Behandlungskapazitätennachweis. Der Betreiber der Leitstelle vereinbart hierzu mit den Trägern geeigneter Krankenhäuser Form, Inhalt und Verfahren der dafür notwendigen Meldungen. Der überwiegende Teil der ILS in Bayern nutzt hierzu das Programm IVENA eHealth des Herstellers mainis IT-Service GmbH.

Die Beschaffung und der Betrieb einer Software zur Unterstützung bei der Erfüllung oben genannter gesetzlicher Forderung wird in den 25 bayerischen ILS unterschiedlich gehandhabt. Das Programm wird durch Zweckverbände für Rettungsdienst und Feuerwehralarmierung (ZRF), von einzelnen ILS-Betreibern und sogar von Kliniken beschafft, ausgerollt und betrieben. Das StMI ist in keinem Fall beteiligt und von daher auch nicht in die Thematik der IT-Sicherheit involviert. Eine gemeinsame Verantwortlichkeit für die Verarbeitung im Sinne des Art. 26 Datenschutz-Grundverordnung (DSGVO)

liegt ebenfalls nicht vor, da die Datenhoheit ausnahmslos bei dem jeweiligen Betreiber liegt, an den das StMI gegebenenfalls entsprechende Anfragen richtet.

Das StMI hat daher weder zu datenschutzrelevanten Zwischenfällen noch zu entsprechenden Präventivmaßnahmen Erkenntnisse.

7. Welche Bereiche/Strukturen im medizinischen sowie rettungsdienstlichen Bereich sind, abgesehen von Krankenhäusern, nach Erkenntnissen der Staatsregierung besonders gefährdet und wie plant die Staatsregierung diese bei der Infrastruktur für ihre IT-Sicherheit zu unterstützen?

Arztpraxen, sonstige Gesundheitseinrichtungen sowie Apotheken sind kein Teil der Staatsverwaltung und unterstehen auch keiner generellen staatlichen Aufsicht. Es besteht keine diesbezügliche Meldepflicht gegenüber der Staatsregierung oder der Selbstverwaltung.

Inwiefern Arztpraxen, sonstige Gesundheitseinrichtungen sowie öffentliche Apotheken besonders von Cyber- bzw. Hackerangriffen gefährdet sind, kann die Staatsregierung daher nicht beurteilen. Zudem liegen der Staatsregierung keine spezifischen Angaben betreffend die IT-Sicherheit von Arztpraxen, sonstigen Gesundheitseinrichtungen sowie öffentlichen Apotheken und auch keine Informationen zu erfolgreichen Cyber- bzw. Hackerangriffen vor.

Der Gesetzgeber hat in § 75b SGB V die IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung geregelt. Auf dieser Basis wurde im Bereich der vertragsärztlichen und vertragszahnärztlichen Versorgung durch die Kassenärztliche Bundesvereinigung und die Kassenzahnärztliche Bundesvereinigung jeweils eine Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit erlassen.

Verantwortlich für eine hinreichend sichere IT-Infrastruktur sind mithin in Umsetzung der genannten Richtlinie die einzelnen Arztpraxen vor Ort. Zusätzliche Unterstützungsmöglichkeiten unterfallen nicht dem Zuständigkeitsbereich der Staatsregierung.

Beschaffung, Betrieb und IT-Sicherheit von Hard- und Software des bayerischen Rettungsdiensts obliegen den jeweiligen Durchführenden bzw. den lokalen ZRF. Das StMI ist hieran nicht beteiligt und von daher auch nicht in die Thematik der IT-Sicherheit involviert. Es liegen keine Erkenntnisse zu datenschutzrelevanten Zwischenfällen oder entsprechenden Präventivmaßnahmen vor.

Hinweise des Landtagsamts

Zitate werden weder inhaltlich noch formal überprüft. Die korrekte Zitierweise liegt in der Verantwortung der Fragestellerin bzw. des Fragestellers sowie der Staatsregierung.

Zur Vereinfachung der Lesbarkeit können Internetadressen verkürzt dargestellt sein. Die vollständige Internetadresse ist als Hyperlink hinterlegt und in der digitalen Version des Dokuments direkt aufrufbar. Zusätzlich ist diese als Fußnote vollständig dargestellt.

Drucksachen, Plenarprotokolle sowie die Tagesordnungen der Vollversammlung und der Ausschüsse sind im Internet unter www.bayern.landtag.de/parlament/dokumente abrufbar.

Die aktuelle Sitzungsübersicht steht unter www.bayern.landtag.de/aktuelles/sitzungen zur Verfügung.