

Cyberangriffe auf Krankenhäuser

Auskünfte der Bundesregierung machen kaum schlauer

Die politisch vorangetriebene Digitalisierung im Gesundheitswesen weckt Begehrlichkeiten auch bei kriminellen Hacker*innen. Zu Opfern von Cyberangriffen via Internet werden immer mal wieder Krankenhäuser. Über das Ausmaß und die konkreten Folgen, auch für die Versorgung von Patient*innen, weiß die Bundesregierung offenbar nicht viel.

Anfang 2024 wurde bekannt, dass drei Krankenhäuser im westfälischen Soest von Hacker*innen angegriffen worden waren. Was unter anderem dazu führte, »dass die Rettungsleitstelle über längere Zeit Krankentransportwagen umleiten musste, die normalerweise zu den betroffenen Krankenhäusern gefahren wären«. Zu lesen ist das in einer Kleinen Anfrage der CDU/CSU-Fraktion im Bundestag, die der Soester Fall scheinbar alarmiert hat. Dabei ist den Fragesteller*innen grundsätzlich klar: »Cyberangriffe führen zu teils erheblichen wirtschaftlichen Schäden von Krankenhäusern und bedrohen die Versorgungsangebote sowie die vertraulichen Daten der Patientinnen und Patienten.«

Genauer wollten die Unionspolitiker*innen nun von der Bundesregierung erfahren. Die Antworten auf 21 Einzelfragen übermittelte das Bundesgesundheitsministerium (BMG) am 28. März. Vorweg erklärt das BMG: Bei mehr als 30.000 vollstationären Fällen pro Jahr gilt ein Krankenhaus als »kritische Anlage« gemäß Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI). Krankenhäuser dieser Mindestgröße seien verpflichtet, den »Stand der Technik« umzusetzen und eventuelle »Cybersicherheitsvorfälle« an das BSI zu melden – kleinere Kliniken müssen das aber nicht.

Die auf dieser Basis erstellte Statistik weist für die Jahre 2018 bis 2023 insgesamt 224 »informationstechnische Angriffe« aus, im ersten Quartal 2024 (Stand: 18. März) waren erst drei Vorfälle aus größeren Krankenhäusern an das BSI gemeldet worden. Wer sich für Details zu den Vorfällen interessiert, wird aus den Antworten des BMG allerdings kaum schlauer. Zur Frage der Unionsabgeordneten, auf welche Weise die Cyberangriffe durchgeführt wurden, erklärt das BMG: »Hierzu werden keine Informationen durch das BSI erhoben«, da die Behörde dafür nicht gesetzlich beauftragt sei.

Zur Frage, welche Gefahren der Bundesregierung durch Cyberangriffe bekannt seien, erklärt das BMG: »Üblicherweise wird durch Verschlüsselung von Daten durch Ransomware die Arbeitsfähigkeit von Krankenhäusern gestört und durch

die Exfiltration von Daten die Vertraulichkeit von Patientendaten kompromittiert.« Zudem verweist die Regierungsantwort auf Ausführungen, die im Jahresbericht 2023 des BSI nachzulesen sind. Ein Ransomware-Angriff, erklärt das BSI dort, sei »eine Form der digitalen Erpressung«. Cyberkriminelle nutzen laut BSI Fehler wie falsche Bedienungen, veraltete Softwareversionen oder mangelhafte Datensicherungen aus; sie verschlüsseln Daten ihrer Opfer und verlangen ein Lösegeld für die Entschlüsselung. Häufig werde die Erpressung »mit der Drohung einer Veröffentlichung zuvor gestohlener Daten kombiniert«, schreibt das BSI. Das Lösegeld fungiere »in der Regel auch als Schweigegeld«.

»Keine Erkenntnisse«

Gefragt von den Unionspolitiker*innen, wie lange ein Krankenhaus durchschnittlich pro Cyberattacke für die Versorgung von Patient*innen ausfalle, erklärt die Bundesregierung, dazu habe sie »keine Erkenntnisse«; auch nicht zur Frage, wie sich Cyberangriffe auf die Arbeit von Ärzt*innen und anderer Klinikbeschäftigter in der Praxis auswirken. Ebensovienig zum Ausmaß der wirtschaftlichen Schäden für die betroffenen Krankenhäuser.

Nach eigenen Angaben weiß die Bundesregierung auch nichts zum Hintergrund der Hacker*innen und über deren Motive. Die Unionsabgeordneten hatten sich ausdrücklich auch danach erkundigt, »welche Rolle bei den Cyberangriffen ausländische Nachrichtendienste spielen, die die kritische Infrastruktur in Deutschland destabilisieren wollen«.

Zur Frage, ob die Bundesregierung damit rechne, dass sich die »Situation weiter verschärfen« und die geplante Krankenhausreform »zu gezielteren Cyberangriffen auf die Maximalversorgungskrankenhäuser« führen werde, schreibt das BMG, dass die Regelungsinhalte der Reform die IT-Sicherheit der Kliniken nicht betreffen.

Klaus-Peter Görlitzer 🗣️

Kontinuierlich beobachtet wird das heikle Thema »Cybersicherheit« auch vom Verein Patientenrechte und Datenschutz. Auf seiner Homepage steht eine informative Übersicht zu Datenpannen, Datenlecks und Ransomware-Angriffen in Einrichtungen des Gesundheitswesens, die in den vergangenen Jahren bekannt wurden. Die Datenschutz-Aktivist*innen skizzieren auf <https://patientenrechte-datenschutz.de> über 40 Fälle, verbunden mit dem Hinweis: »Vermutlich ist diese Auflistung unvollständig.«

Klinikschließungen und Patientenrechte

Hackerangriffe sind eine latente Gefahr für alle Krankenhäuser, aber manchen droht noch Schlimmeres: Insolvenz und Schließung. Kommt es so weit, können auch der Schutz persönlicher Gesundheitsdaten und die Informationsrechte ehemaliger Patient*innen gefährdet sein. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat im Mai eindringlich gefordert, Regelungslücken im Zusammenhang mit Klinikschließungen zu beseitigen. Zum Hintergrund erklärten die Datenschützer*innen: »Nur sofern ein Insolvenzverfahren läuft, können Patientinnen und Patienten regelmäßig über den Insolvenzverwalter Einsicht in ihre Akte erlangen. Sobald das Insolvenzverfahren jedoch beendet ist oder mangels Masse nicht eröffnet wird, ist aufgrund fehlender Regelungen offen, durch wen und unter welchen technischen Anforderungen Krankenhausakten aufzubewahren, datenschutzkonform zu löschen und wie Patientenrechte zu gewährleisten sind.« Die Unklarheiten seien »auch im Interesse einer im Einzelfall gebotenen medizinischen Weiterbehandlung nicht hinzunehmen«, denn Patient*innen haben grundsätzlich einen Anspruch auf Zugang zu sie betreffenden Behandlungsdokumentationen. Die behördlichen Datenschützer*innen haben die Gesundheitsministerkonferenz per Entschließung vom 15. Mai aufgefordert, zeitnah »Lösungsmöglichkeiten« zu erarbeiten und endlich für Rechtssicherheit zu sorgen. Alle Krankenhäuser müssten verpflichtet werden, »Konzepte zur weiteren Verwahrung der Patientenakten für den Fall der Insolvenz oder der ungeplanten Schließung anzufertigen«.