Frage ist nicht ob, sondern wann

Cyber-Attacken auf Kliniken häufen sich

FRANKFURT

Die Daten von Krankenhäusern sind sensibel – und damit wertvoll. Das macht sie zu einem attraktiven Ziel für Hacker und Erpresser. In Frankfurt wurde eine solche Attacke frühzeitig entdeckt. Die Auswirkungen für die Mitarbeiter sind dennoch groß.

Im Frankfurter Universitätsklinikum gibt es derzeit „rot“ und „grün“ markierte Rechner. Alle Rechner im bisherigen System sind mit einem roten Punkt versehen. Nach und nach werden nun einzelne grüne Rechner in einem neuen Netzwerk in Betrieb genommen, um mit der Außenwelt kommunizieren zu können. Die als rot definierten Computer dürfen nur innerhalb des Hauses benutzt werden, die mit grünen Aufklebern können nach draußen kommunizieren. Beide Systeme müssen noch wochenlang getrennt bleiben – denn Hessens größtes Krankenhaus ist Opfer eines Hackerangriffs geworden.

Ende vergangener Woche entdeckte ein Mitarbeiter bei einer Routinekontrolle einen Account, der umfangreiche Zugriffsrechte hatte, aber nicht dafür legitimiert war. Der Mitarbeiter schlug Alarm, die Aufsichtsbehörden wurden informiert, ein Krisenstab eingerichtet, Fachfirmen für IT-Forensik zur Hilfe gerufen. Als erste Maßnahme wurde das Krankenhaus vom Internet abgeschnitten. „Wir sind jetzt im Datenverkehr eine Insel“, sagt der Ärztliche Direktor Jürgen Graf.

Die gute Nachricht: Nach bisheriger Kenntnis wurden keine Daten verschlüsselt oder ausgelesen, es gibt bislang keine Forderung von Erpressern – vermutlich, weil der Angriffsversuch so früh entdeckt wurde. „Der unmittelbare Schaden mag gering sein“, sagt Graf, „die grundlegenden IT-Systeme innerhalb des Universitätsklinikums funktionieren weiterhin, so dass die Krankenversorgung fortgesetzt werden kann. Aber die Auswirkungen sind trotzdem beträchtlich.“

Konkret betroffen ist alles, was auf Kontakt zur Außenwelt angewiesen ist: Über Patienten, die mit minder schweren Beschwerden vom Rettungswagen eingeliefert werden, bekommen die Ärzte vorher keine Informationen. Terminabsprachen für eingeplante Patienten laufen über Telefon. Krankenkassenkarten können nicht elektronisch eingelesen werden, Rechnungen und Abrechnungsdaten können nicht eingereicht werden, Materialbestellungen können nicht automatisiert aufgegeben werden. „Für all diese Prozesse muss sich das Universitätsklinikum alternative Lösungen suchen – das kostet Zeit“, sagt Graf.

„In den vergangenen Jahren hat das Bewusstsein für IT-Sicherheit im Gesundheitswesen deutlich zugenommen“, sagt Professor Thomas Friedl vom Fachbereich Gesundheit der Technischen Hochschule Mittelhessen. Das frühzeitige Entdecken dieser Cyberattacke sei ein positives Zeichen für die steigende Wachsamkeit.

Zeitgleich wachsen auch die Angriffe auf IT-Systeme: Nach den Meldedaten des Bundesamts für Sicherheit in der Informationstechnik verzeichnete der Gesundheitssektor von Juni 2021 bis Mai 2022 die höchste Anzahl an Hackerangriffen. Grund dafür ist die zunehmende Digitalisierung im Gesundheitswesen.

Warum Krankenhäuser ein beliebtes Ziel von Cyberattacken sind, erklärt Friedl mit dem hohen Wert der gehackten Daten. Auch die Sammlung von hochsensiblen Informationen an einem einzigen Ort stellt Friedl zufolge ein erhöhtes Angriffsrisiko dar. Um Krankenhäuser vor Cyberangriffen zu schützen, empfiehlt der IT-Experte eine dezentrale Verwaltung von Patientenakten und anderen hochsensiblen Daten. Dafür müssten ausreichend finanzielle Mittel zur Verfügung stehen. Aber Technik allein reiche für den Schutz vor IT-Angriffen nicht aus, betont Friedl: „Damit Sicherheitssysteme funktionieren, bedarf es eines Systemes mit viel Hirn“, sagt er. Verbindliche jährliche Datenschutzschulungen könnten zusätzlich das Klinikpersonal für Cyber-Angriffe sensibilisieren.

„Wenn man mit anderen Krankenhäusern spricht, merkt man: die Gefahr ist da“, sagt Benita Rojewski, Informationssicherheitsbeauftragte des Klinikums Darmstadt. Die Frage, mit der sich die Kliniken beschäftigten, sei nicht ob, sondern wann der Cyberangriff im eigenen Haus passiere, erklärt Rojewski. „Das Problem ist, dass sich Krankenhäuser nun mal nicht zu 100 Prozent schützen können. Es bleibt immer ein gewisses Restrisiko.“

Nicht nur ein Cyber-Angriff kann dazu führen, dass Systeme nicht mehr funktionieren, betont Rojewski. Auch technische Probleme hätten Beeinträchtigungen zur Folge. Für den Ernstfall könnten sich Krankenhäuser vorbereiten. „Wir sensibilisieren unsere Ärztinnen und Ärzte, sich im Team Gedanken über alternative Arbeitsweisen zu machen“, sagt Rojewski. Stift und Papier seien eine mögliche Alternative: „Dem Patienten ist es egal, ob die Laborwerte in der Software oder auf dem Zettel stehen.“

Wird es noch gefährlicher, wenn erst mal die elektronische Patientenakte eingeführt ist? Uniklinik-Direktor Graf glaubt das nicht: Wenn sensible Daten zentral aufbewahrt würden, müsse dieser Server natürlich maximal gut geschützt sein. „Aber 1900 deutsche Krankenhäuser wären damit für Hacker deutlich weniger interessant: Mit unseren Bestelllisten wären wir ja kein attraktives Ziel für Erpressungsversuche.“

UMFRAGE VON BITKOM

74 Prozent der befragten Ärztinnen und Ärzte gaben an, dass ihrer Ansicht nach Kliniken in Deutschland häufig nicht genügend geschützt sind.

66 Prozent sorgten sich konkret vor Cyberangriffen auf Krankenhäuser.

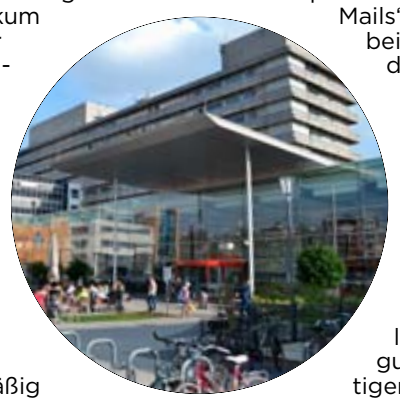
42 Prozent werden an ihrer Klinik regelmäßig zum Thema IT-Sicherheit geschult.(Umfrage des IT-Branchenverbands Bitkom aus dem Jahr 2022. 500 Mediziner wurden befragt.)

> Der Hacker weiß, wenn er hier Erfolg hat, dann wird in aller Regel gezahlt. Denn wenn ich nicht zahle, bekomme ich meine Daten nicht zurück.
>
> **Thomas Friedl**
> Professor im Fachbereich Gesundheit der Technischen Hochschule Mittelhessen

Fotos: dpa, Volker Nies

„BEINAHE TÄGLICH VERDÄCHTIGE MAILS“

Am **Klinikum Fulda** konnten bislang alle Hackerangriffe abgewehrt werden. Das erklärt Barbara Froese, Pressesprecherin des Klinikums Fulda, auf Nachfrage unserer Zeitung. „Das Klinikum Fulda zählt aufgrund seiner Größe zur sogenannten ‚Kritischen Infrastruktur‘ und hat deshalb hohe Anforderungen im Bereich der IT-Sicherheit zu erfüllen. Regelmäßige Prüfungen und Zertifizierung belegen den hohen Stand der IT-Sicherheit. So sind zur Angriffserkennung und -abwehr diverse technische und organisatorische Maßnahmen etabliert, deren Wirksamkeit regelmäßig mit simulierten Angriffen überprüft wird“, sagt Froese. Diese Systeme würden „beinahe täglich Angriffsversuche zum Beispiel in Form verseuchter E-Mails“ erkennen, die an Mitarbeiter und Mitarbeiterinnen des Klinikums gesendet werden. Eine umfassende Sicherheit sei allerdings technisch nicht darstellbar. „Deshalb werden die Sicherheitslage und die implementierten Maßnahmen regelmäßig überprüft – auch durch externe Spezialisten, die uns ein sehr gutes Schutzniveau bestätigen.“ / dan



„SIND UNS DER BEDROHUNG BEWUSST“

Auch das **Herz-Jesu-Krankenhaus** in Fulda sei bislang nicht von Hackerangriffen betroffen oder Ziel von Cyberattacken. „Dennoch sind wir uns der ständig wachsenden Bedrohungen bewusst und arbeiten kontinuierlich daran, unsere Sicherheitsmaßnahmen zu verbessern und auf dem neuesten Stand zu halten“, betont Viktoria Schmitt, Pressesprecherin am Herz-Jesu-Krankenhaus. Der Schutz der Patientendaten habe höchste Priorität. Umfassende Sicherheitsvorkehrungen seien getroffen worden, um potenzielle Cyberbedrohungen abzuwehren. „So wird das Krankenhauspersonal durch regelmäßige Schulungen für mögliche Bedrohungen sensibilisiert, dabei wird das bewusste Verhalten im Umgang mit E-Mails, Links usw. geschult.

„Ein wichtiger Baustein ist auch ein funktionierendes Ausfallmanagement mit alternativen, ‚manuellen‘ Arbeitsprozessen wie papierbasierte Aufzeichnungen, sodass immer darauf geachtet wird, dass die Patientenversorgung in potenziellen Cyberangriffssituationen gesichert ist“, erklärt Schmitt. / dan