Wenn Hacker töten können

Angriff aus dem Netz Kliniken werden von Cyberattacken bedroht. Die Folgen können fatal sein: Denn Patientendaten und Leben sind in Gefahr

Deutschen Krankenhäusern droht eine Gefahr aus dem Internet. Daten von Patientinnen und Patienten können im Netz landen, schlimmstenfalls können Menschen sterben: durch Cyberattacken. Schon seit Jahren ist die sogenannte Kritische Infrastruktur (KRITIS) solchen Angriffen ausgesetzt. Dazu gehören Einrichtungen wie Kraftwerke, Behörden, aber auch Krankenhäuser ab einer bestimmten Größe. Das Bundeskriminalamt und das Bundesamt für Sicherheit in der Informationstechnik warnen in ihren Jahresberichten regelmäßig vor Cyberangriffen. Und eine Anfrage der FDP an die Bundesregierung von 2020 ergab: Im Jahr 2018 gab es elf, ein Jahr später 16 und 2020 mindestens 43 Attacken auf Gesundheitsdienstleister wie Krankenhäuser.

Ein bekanntes und einzigartiges Beispiel ist die Attacke auf das Uniklinikum Düsseldorf im Jahr 2020. Damals stellte sich zum ersten Mal in Deutschland die Frage: War eine Cyberattacke für den Tod eines Menschen verantwortlich? Wegen einer Schadsoftware musste das Haus seine IT herunterfahren, Rettungswagen konnten die Notaufnahme nicht ansteuern. Eine Patientin wurde daher etwa eine halbe Stunde nach Wuppertal transportiert. Sie starb kurz nach der Ankunft im Krankenhaus. Zwar stellten Behörden fest, dass die Patientin so oder so gestorben wäre. Für den Sicherheitsexperten Michael Wiesner ist das aber kein Grund zur Beruhigung. „Jeder Angriff auf ein Krankenhaus bedeutet Gefahr für Leib und Leben“, sagt er. „Darum ist es für mich besonders kritisch, wenn Kliniken erfolgreich attackiert werden.“

„Jeder Angriff auf ein Krankenhaus bedeutet Gefahr für Leib und Leben. Darum ist es besonders kritisch, wenn Kliniken erfolgreich attackiert werden“

Michael Wiesner,
IT-Sicherheitsexperte und Sprecher der AG KRITIS

Wiesner ist Mitglied der Arbeitsgemeinschaft KRITIS – Fachleute, die sich für die Absicherung Kritischer Infrastruktur einsetzen. Er beschreibt, wie Kriminelle oft vorgehen: Angreifer verschicken Phishing-Mails an alle möglichen Empfänger. Solche Nachrichten sollen Betroffene dazu bringen, Anmeldedaten weiterzugeben oder Schadsoftware auf Klinikrechner zu laden. Ist das geschehen, verschlüsselt sie alle Daten im Netzwerk. Für die Belegschaft bedeutet das: Das IT-System fällt aus, wichtige Programme sind nicht mehr erreichbar. Unterlagen wie OP-Listen, Röntgenbilder oder welche Medikamente jemand bekommt, lassen sich nicht einsehen.

Um das System wieder nutzen zu können, müssen Betroffene Lösegeld zahlen, oft in Bitcoin. Deshalb heißen diese Angriffe Ransomware-Attacken („ransom“, Englisch für Lösegeld). „Ziel der Angreifer ist es, mit möglichst großem Profit und niedrigem Aufwand zu hacken“, so Wiesner. „Krankenhäuser sind lohnenswerte Ziele, denn der Aufwand ist meist gering.“ Die Gründe dafür: IT-Abteilungen sind oft unterbesetzt und überarbeitet, zudem sei nicht immer genug Geld für aktuelle Sicherheitssysteme da. Auch sei die Belegschaft oft nicht entsprechend geschult, um Phishing-Mails zu erkennen.

Seit einiger Zeit bleibt es nicht beim Verschlüsseln: Kriminelle kopieren Daten und drohen, sie im Darknet zu veröffentlichen oder zu verkaufen. Gegen diese Erpressung hilft keine Datensicherung der Systeme. Denn wenn Patientendaten im Netz landen, bedeutet das: Kriminelle können Betroffene erpressen oder Identitätsdiebstahl begehen. Sie können zum Beispiel persönliche Daten ihrer Opfer nutzen, um online einzukaufen. Die Rechnung erhalten Betroffene. Zumindest in den USA waren Kliniken von Datendiebstahl betroffen und bereit, Lösegeld zu zahlen. „Am Ende zahlt man also Millionen, um wieder auf seine Daten zugreifen zu können und noch mal Millionen, damit sie nicht ins Netz gestellt werden“, sagt Wiesner.

Auch IT-Experte Markus Holzbrecher-Morys von der Deutschen Krankenhausgesellschaft sieht Gefahren für das deutsche Gesundheitssystem durch Cyberattacken. „Anzahl und Qualität der Attacken sind in den vergangenen Jahren gestiegen“, sagt er. Er betont aber auch, dass nicht nur Kliniken, sondern generell die Kritische Infrastruktur im Fokus von Kriminellen sei: „Uns sind keine Hinweise bekannt, dass Krankenhäuser verstärkt betroffen sind.“

Um Daten und Leben zu schützen, hat der Staat verschiedene Gesetze erlassen. So verpflichtet das IT-Sicherheitsgesetz 2.0, dass Betreiber von Gesundheits-Infrastruktur ihre IT-Systeme nach „Stand der Technik“ absichern. Davon betroffen sind Kliniken, die im Jahr 30 000 Fälle vollstationär behandeln. Und das Patientendaten-Schutz-Gesetz soll garantieren, dass auch kleinere Häuser ihre IT-Sicherheit erhöhen. Das ergänzt im Sozialgesetzbuch V unter anderem, dass seit 1. Januar Maßnahmen zur IT-Sicherheit in allen Krankenhäusern verpflichtend umgesetzt werden müssen.

Solche Maßnahmen kosten, darum hatte die Große Koalition das Krankenhauszukunftsgesetz initiiert: Bund und Länder sollen etwa 4,3 Milliarden Euro für die Digitalisierung von Krankenhäusern bereitstellen. 15 Prozent müssen zwingend für IT-Sicherheit aufgewendet werden. Holzbrecher-Morys sieht die Förderung als wichtigen Impuls. Allerdings sei das Geld zu wenig, um den über Jahre aufgebauten Investitionsstau in Krankenhäusern auszugleichen.

Zudem müsse man laufende Kosten beachten: Fachleute müssen regelmäßig Sicherheitssysteme prüfen und updaten. Holzbrecher-Morys betont darum die Wichtigkeit sogenannter Awareness-Trainings („awareness“, Englisch für Bewusstsein). In Schulungen lernt man, Betrugs-Mails auszumachen. „Manche Phishing-Mail ist so gut gemacht, dass man sie nicht erkennt“, sagt Holzbrecher-Morys. „Ich kann nicht oft genug betonen, wie wichtig Awareness ist.“ ***Ali Vahid Roodsari*** ■

Illustration: W&B/Nina Schneider