Cyberangriffe auf Kliniken - die Hacker haben massiv aufgerüstet – Teil 1

19.09.2025, Unternehmens-Blog

Cyberangriffe auf Krankenhäuser nehmen rasant zu – mit teils dramatischen Folgen für Versorgung, Finanzen und Vertrauen. Im Interview erklärt Prof. Christian Dörr, Leiter der Abteilung Cybersecurity im Hasso-Plattner-Institut, warum der Gesundheitssektor besonders gefährdet ist, wie Angreifer arbeiten und welche Maßnahmen dagegen notwendig sind.

Herr Prof. Dörr, das Hasso-Plattner-Institut arbeitet derzeit an einer Studie über IT-Sicherheit im Gesundheitssektor. Wie ist der aktuelle Stand?

AOK Systems GmbH | Kortrijker Str. 1 | 53177 Bonn | Tel: 0228 843 0 | Fax: 0228 843 1111 | aok-systems@sys.aok.de
Geschäftsführung: Georg Büttner | Vorsitzende des Aufsichtsrates: Dr. Carola Reimann
USt.-ID-Nr.: DE 1964 87 059 | Handelsregister: Bonn HRB 17142

Unser Ansatz ist es, mit verschiedenen Akteuren des Gesundheitswesens zu sprechen, um Schwachstellen und Lösungsansätze im Bereich Cybersicherheit zu identifizieren. Dazu zählen unter anderem Klinikdirektoren und Sicherheitsbeauftragte. Ein Ergebnis: Rund 30 Prozent aller Kliniken in Deutschland hatten bereits mindestens einen Sicherheitsvorfall und seit 2017 steigt die Zahl der Attacken extrem an. Die Studie wird voraussichtlich im Herbst veröffentlicht. Schon jetzt können wir sagen, dass sich die Sicherheitsarchitektur in diesem Sektor in den kommenden Jahren dramatisch verändern wird.

Was sind die Gründe?
Die Stichworte sind Datensicherheit und Datenaustausch. Wir haben auf der einen Seite die IT-Systeme der Krankenhäuser, die sich untereinander immer stärker vernetzen. Auf der anderen Seite sind die Arztpraxen, die unter anderem eine Nachsorge der aus den Kliniken entlassenen Patienten sicherstellen – das heißt, eine zunehmende Vernetzung zwischen stationärem und ambulantem Sektor. Hinzu kommt: die Spezialisierung im Gesundheitswesen wird den Datenaustausch zwischen Kliniken, Fach- und Hausärzten weiter verstärken. Oft vergessen wird auch der Einsatz sogenannter Wearables. Also kleiner elektronischer Geräte – etwa Smartwatches – zur Gesundheitsüberwachung, die wir am Körper tragen und die ebenfalls jede Menge Daten erfassen und weiterleiten. Das heißt: Hackerangriffe auf Kliniken, die wir derzeit gehäuft beobachten, betreffen nicht nur die jeweilige Klinik, sondern weitere Kliniken, Praxen und auch die Patienten direkt.

Wie lassen sich diese sensiblen Datenflüsse sichern?
Lange Zeit folgte die IT-Sicherheit dem Perimeter-Modell. Das funktioniert vereinfacht gesagt so: Man geht davon aus, dass innerhalb eines Netzwerks alles sicher ist, wenn die Grenzen dieses Netzwerks durch Firewall, VPN und andere Maßnahmen geschützt werden. Stellen Sie sich das wie einen Wassergraben vor, der eine Burg umschließt. Sobald jemand jedoch den Wassergraben überwunden hat, kann er sich frei auf dem Burggelände bewegen. Nun ist ein Krankenhaus naturgemäß sehr durchlässig. Das lässt sich nicht vermeiden, denn es findet ein permanenter Datenaustausch innerhalb der Klinik mit den genannten Akteuren von außerhalb statt. Medizinische Geräte senden routinemäßig Daten zur Analyse in eine Cloud, medizinisches Personal muss regelmäßig auf Datenbanken zugreifen und die elektronische Patientenakte (ePA) verfügt auch über viele Schnittstellen. Die Angriffsfläche ist enorm.

Was ist die Alternative zum Perimeter-Modell?
Erst einmal muss ich wissen, welche Geräte sich überhaupt in meiner Klinik befinden und wie diese miteinander kommunizieren. Schon diese Bestandsaufnahme ist komplexer, als es vielleicht scheint. So ist für die Neuanschaffung meist die Einkaufsabteilung zuständig oder der Klinikdirektor. Ich habe mit IT-Chefs gesprochen, die gar nicht wussten, welche Geräte sie im Krankenhaus haben. Notwendig ist also zunächst ein Überblick auf das Gesamtsystem, das heißt ein zentrales Sicherheitsmanagement.

Was ist der nächste Schritt?
Als Nächstes sollten IT-Abteilung und Klinikleitung klare Regeln definieren: Wer darf wann und unter welchen Voraussetzungen auf bestimmte Systeme zugreifen? Verstößt jemand gegen diese Regeln, werden automatisch

AOK Systems GmbH | Kortrijker Str. 1 | 53177 Bonn | Tel: 0228 843 0 | Fax: 0228 843 1111 | aok-systems@sys.aok.de
Geschäftsführung: Georg Büttner | Vorsitzende des Aufsichtsrates: Dr. Carola Reimann
USt.-ID-Nr.: DE 1964 87 059 | Handelsregister: Bonn HRB 17142

Zugriffsrechte entzogen oder Rechner oder Datenbanken abgeschaltet. Das heißt, auch innerhalb der Firewall darf sich nicht mehr ohne Authentifizierung und ohne Überprüfung bewegt werden. Zero Trust heißt diese Weiterentwicklung des Perimeter-Modells. Vertraue niemandem, überprüfe jeden Zugriff. Sollte also jemand die äußere Firewall überwunden haben, bleibt sein Zugriff auf sensible Daten dennoch stark eingeschränkt.

Welche technischen Änderungen sind dafür nötig?
Eine Firewall um die gesamte Klinik-IT bleibt weiter wichtig. Zusätzlich teile ich das IT-System in kleine, voneinander isolierbare Segmente und schütze diese über jeweils eigene Firewalls. Den nötigen Datenaustausch zwischen diesen Bereichen regele ich mit einem Identitäts-Management-System, das nur berechtigten Personen Zugriff gewährt, und einer Multi-Faktor-Authentifizierung, die über ein Passwort und ein zusätzliches Identifikationstool, beispielsweise Fingerabdruck, Gesichtserkennung oder Handy-PIN, sicherstellt, dass sich nur eine berechtigte Person ins System einloggen will. So kann ich die Datenflüsse zwischen Geräten kontrollieren und falls ein Rechner kompromittiert wird, verursacht das nur einen lokalen Schaden, betrifft vielleicht zwei oder drei Computer, aber nicht die Gesamt-IT.

Können Sie das an einem Beispiel erklären?
Sicher. Nehmen wir einen Kernspintomografen. Der muss mit dem PC des Radiologen kommunizieren, vielleicht mit der Patientendatenbank, eventuell mit dem Abrechnungssystem. Diese überschaubare Umgebung schütze ich mit einem eigenen Sicherheitssystem. Bemerke ich, dass der Kernspintomograf beginnt, nach anderen Geräten außerhalb seines Netzwerks zu suchen, verhindert dies die Firewall, weil es sehr wahrscheinlich ist, dass etwas nicht stimmt.

Eine solche Umstellung kostet Geld. Ist das realisierbar bei der chronischen Unterfinanzierung vieler Kliniken?
Cybersicherheit kostet. Das stimmt. Aber ein Cybersicherheitsvorfall wird deutlich teurer. Zunächst brauchen Sie externe Spezialisten, die die IT nach einem Cyberangriff erneuern. Die Honorare solcher Experten erreichen im Verlauf von zwei, drei Monaten schnell Millionenbeträge. Für einen Bruchteil dieser Summen hätte man präventiv in die IT-Sicherheit investieren können. Ein weiterer Kostenfaktor: Die Klinik ist wochenlang offline, kann keine oder weniger Patienten aufnehmen. Vielleicht lässt sich ein Großteil der geplanten Operationen nachholen, kaum kompensieren lässt sich dagegen der Reputationsverlust. Patienten meiden die Einrichtung, möglicherweise über Jahre, weil sie um die Sicherheit ihrer persönlichen Daten fürchten. Gleichzeitig finden Sie weniger hoch qualifiziertes Personal aufgrund des schlechten Images der Klinik. In unserer Studie berichten wir über Krankenhäuser, die nach einem Cyberangriff Konkurs anmelden mussten.

Hier geht es zu Teil 2 und Teil 3 des Interviews.

Bild: Hasso-Plattner-Institut

AOK Systems GmbH | Kortrijker Str. 1 | 53177 Bonn | Tel: 0228 843 0 | Fax: 0228 843 1111 | aok-systems@sys.aok.de
Geschäftsführung: Georg Büttner | Vorsitzende des Aufsichtsrates: Dr. Carola Reimann
USt.-ID-Nr.: DE 1964 87 059 | Handelsregister: Bonn HRB 17142

Autor/in: Eva Franz, Marketing Managerin, AOK Systems GmbH