Cyberangriffe auf Kliniken - die Hacker haben massiv aufgerüstet - Teil 3

02.10.2025, Unternehmens-Blog

Während in Teil 1 des Interviews mit Prof. Christian Dörr, Leiter der Abteilung Cybersecurity im Hasso-Plattner-Institut, Ursachen von Cyberangriffen auf Krankenhäuser analysiert und Lösungen vorgeschlagen wurden, ging es in Teil 2 um Herkunft und Motivation der Täter. In nachfolgenden dritten Teil spricht der Fachexperte darüber, warum es trotzdem so viele Kliniken erwischt und wie

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

auch kleinere Akteure wie MVZs oder Einzelpraxen Schutzmaßnahmen ergreifen können.

Warum werden, obwohl Ursachen von Cyberangriffen und Herkunft der Täter weitgehend bekannt sind, hierzulande in steigender Zahl Kliniken zum Opfer von Hackern?

Ich habe ja schon erwähnt, dass Kliniken erstens naturgemäß durchlässige Systeme sind und zweitens der Cybersicherheit noch nicht überall die nötige Priorität eingeräumt wird. Ich habe Kliniken gesehen, in denen man über das Besucher-WLAN mit ein paar Klicks ins medizinische IT-System gelangen konnte. Ein weiteres Problem ist der Mangel an Fachkräften. Die Zahl der Studiengänge für Cybersicherheit in Deutschland kann man an zwei Händen abzählen. Unis in Bochum, Darmstadt, Lübeck, München und im Saarland bieten entsprechende Ausbildungen an. Dazu kommen ein paar Fachhochschulen. Am Hasso-Plattner-Institut bilden wir jährlich 30 Leute aus. Zusammengenommen sind das bundesweit etwa 1.500 Absolventinnen und Absolventen. Allein für die Kliniken benötigen wir rund 4.000 Spezialistinnen und Spezialisten. Für eine flächendeckende Sicherheit in Verwaltung, Industrie, Bildung und Energie schätzungsweise zwischen 10.000–15.000 zusätzliche Fachkräfte.

Selbst wenn genügend Fachkräfte verfügbar wären: Eine Klinik oder ein Klinikverbund kann sich eigene Cyber- Sicherheitsexperten leisten. Aber was ist mit einem kleinen Medizinischen Versorgungszentrum (MVZ) oder einer Einzelpraxis?

Das ist richtig. Kleine Akteure haben diese Ressourcen nicht. Ihnen muss ich Lösungen anbieten, die so sicher sind, dass sie damit auch ohne eigene IT-Abteilung arbeiten können. Man könnte das so regeln, dass nur noch Geräte zugelassen werden, die bestimmte Sicherheitsstandards erfüllen. Das ist bei Medizinprodukten, die schon jetzt hohe Zulassungshürden haben, aber sehr komplex. Als Nutzer können Sie nicht mal schnell ein Update machen, wenn Sie eine Sicherheitslücke entdecken. Sie müssen sich an den Hersteller wenden, der das übernimmt und sein Produkt dann erneut zertifizieren lassen muss. Trotzdem führt kein Weg daran vorbei, kleinere Akteure im Gesundheitssektor mit sicheren Geräten auszustatten – und dabei sind die Gerätehersteller gefragt.

Braucht es dazu mehr Regularien?

Die braucht es. Aber darüber hinaus noch mehr. Dank des Krankenhaus Zukunftsgesetzes gibt es Fördermittel für Cybersicherheit. Wir wissen aber, dass die Beträge oft nicht abgerufen werden. Wir benötigen viel umfassendere Vorgaben – die nicht nur die KRITIS-Kliniken betreffen, sondern den gesamten Gesundheitssektor.

Praxen, MVZ oder kleinere Kliniken könnten sich zu Verbünden zusammenschließen und ihre IT auch von einem externen Dienstleister betreuen lassen. Was halten Sie davon?

Theoretisch eine gute Idee. Praktisch funktioniert das nicht. Unsere Studie hat gezeigt, dass die Sicherheitsvorfälle in solchen Modellen nicht abgenommen haben. Eher im Gegenteil.

Worin sehen Sie die Ursachen?

Die Einrichtungen haben ihre IT an Profis ausgelagert und waren davon überzeugt, sich nun selbst um nichts mehr kümmern zu müssen. Offensichtlich ein Trugschluss. Deshalb plädiere ich ja für eine klare Gesetzgebung durch Bund und Länder.

Auf wie viel Zustimmung stoßen Sie mit Ihrer Forderung nach mehr Regulierung?

Das kommt darauf an, mit wem ich spreche. Geschäftsführer von Kliniken stimmen in der Regel zu. Die sagen: Wenn ich mich auf einen gesetzlichen Auftrag berufen kann, lassen sich entsprechende Änderungen schnell etablieren. Ähnlich sehen das die Sicherheitsbeauftragten, die in ihren Einrichtungen ja oft gegen Windmühlen kämpfen. Die Beschäftigten auf den Stationen sehen Vorschriften naturgemäß kritischer, weil sie höheren Aufwand fürchten.

Wie wollen Sie Ärzte und Pflegepersonal, die oft schon jetzt unter hoher Arbeitsbelastung stehen, von höheren obligatorischen Sicherheitsanforderungen überzeugen?

Mit smarten, praktikablen Lösungen. Wir brauchen nicht noch größere Papierberge, sondern eindeutige Zuständigkeiten und nutzerfreundliche Software und Geräte. Ob wir wollen oder nicht – die Angreifer

rüsten in einem extrem hohen Tempo auf und wenn wir nicht mithalten, ist unsere Infrastruktur, vor allem der Gesundheitssektor, gefährdet.

Hier geht es zu Teil 1 und Teil 2 des Interviews.

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