Cyberangriffe auf Kliniken - die Hacker haben massiv aufgerüstet - Teil 2

26.09.2025, Unternehmens-Blog

Bereits in Teil 1 des Interviews mit Prof. Christian Dörr, Leiter der Abteilung Cybersecurity im Hasso-Plattner-Institut, hat er die Ursachen der verstärkten Cyberangriffen auf Krankenhäuser analysiert und Lösungen vorgeschlagen, wie diese sich am besten davor schützen können. In Teil 2 erfahren wir, wie Cyberattacken in der Regel vonstattengehen und wie verheerend sich diese auswirken können.

Wie laufen Cyberattacken auf Kliniken normalerweise ab?

Häufig sind das Angriffe mit Ransomware, also Schadsoftware, die Daten verschlüsselt und so den Zugriff auf diese Daten unterbindet, um eine hohe Summe für die Entschlüsselung zu fordern. Meist verschicken die Täter als harmlose Links oder Mailanhänge getarnte Phishing-Mails, die sich arglose Mitarbeiter auf ihren Computer herunterladen. Anschließend sucht die Software automatisch nach weiteren Systemen, Servern und sensiblen Daten, verschlüsselt Letztere mit einem Algorithmus und verschickt danach eine Lösegeldforderung mit der Drohung, bei

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

Zahlungsverweigerung alle Daten zu löschen.

Der Mensch ist demnach die größte Schwachstelle?
Genau. Die Auswertung von zigtausend Berichten von Polizei und Sicherheitsagenturen ergab, dass zu rund 80 Prozent der Faktor Mensch das Problem ist. Ich versuche es positiv zu formulieren: Der Mensch ist die beste Firewall.

Wonach richten sich die Höhen der geforderten Lösegeldsummen?
Die Täter sind meist sehr gut über die wirtschaftliche Situation informiert. Sie lesen Unternehmensbilanzen, Pressemitteilungen oder Börsenberichte, kennen deshalb den Umsatz des Opfers und wissen, welche Beträge die Unternehmen realistischerweise zahlen können. Wir wissen von sieben- bis achtstelligen Beträgen. Manche Erpresser haben Versicherungen gehackt, die Policen gegen Hackerangriffe angeboten hatten, ermittelten dort die versicherten Unternehmen und die maximalen Deckungssummen. Anschließend hackten sie die versicherten Konzerne und forderten genau die versicherte Summe. Die Firma zahlte – der finanzielle Schaden war ja gedeckt. Inzwischen sind diese Versicherungen weitgehend vom Markt verschwunden. Sie wurden einfach unbezahlbar. Sicher ist aber: Die andere Seite hat massiv aufgerüstet, und das ist vielen potenziellen Opfern nicht klar.

Was passiert, wenn jemand zahlt?
Polizei und Staatsanwaltschaft raten davon ab. Unter anderem, weil eine Zahlung das Risiko erhöht, künftig angegriffen zu werden. Wir nennen das „Double Attack“. Die Klinik hat gezahlt, die Täter schalten die Daten frei, verkaufen aber den Zugang zu dem IT-System an andere Erpresser. Dieser verschlüsselt die Daten nach einer gewissen Zeit erneut und es folgt die nächste Erpressung.

Schützt ein Back-up vor Verschlüsselung und Verlust von Daten?
Ein Back-up schützt davor, dass Sie Ihre Daten verlieren. Es schützt nicht vor Erpressung. Die Täter drohen einfach, die Daten zu veröffentlichen. Werden hochsensible Angaben weltweit sichtbar – etwa von Menschen in psychiatrischer Behandlung oder auch die Gehälter aller Klinikmitarbeiter, ist das Image der Einrichtung nachhaltig beschädigt.

Wer sind die Täter?
Wir beobachten im Netz tagesaktuell mehr als 100 Hackergruppen und unterscheiden zwischen verschiedenen Täterprofilen. Da gibt es die unzufriedenen Mitarbeiter, die ihren Arbeitgeber schädigen wollen. Es gibt Script-Kiddies, junge Hacker, die ihre Reputation in der Hackerszene aufpolieren möchten. Andere verstehen sich als Aktivisten, die politische Botschaften platzieren wollen. Es gibt Akteure, die im Auftrag fremder Staaten Unsicherheit erzeugen sollen. Dann sehen wir Cyberterroristen, denen es nur um Zerstörung geht. Große Hackergruppen bestehen aus hoch spezialisierten Leuten, organisiert in einem pyramidenförmig angelegten Ökosystem. An der Spitze sind Millionäre, darunter agieren die Programmierer und am Ende arbeiten Laufburschen, die den gesamten Tag Mails schreiben. Letztere Aufgaben übernimmt zunehmend Künstliche Intelligenz (KI). Damit

eröffnen sich völlig neue Möglichkeiten für Erpresser.

Welche?
Berühmt wurde der Fall einer Bank in Hongkong. Ein Buchhalter bekam vom vermeintlichen Finanzchef per Mail den Auftrag, 25 Millionen US-Dollar auf ein Konto zu überweisen. Selbstverständlich wollte sich der Buchhalter rückversichern. Also organisierte er eine Zoom-Konferenz mit Geschäftsführer, Finanzchef und anderen Mitarbeitern. Insgesamt vier oder fünf Leute. Das Problem: Er war der einzige echte Mensch und konferierte mit KI-generierten Deepfakes, die täuschend echt Aussehen und Stimmen seiner Kollegen imitierten. Tatsächlich verbargen sich dahinter Hacker-Kids. Diesen überwies der Mann am Ende die 25 Millionen.

IP-Adressen lassen sich verschleiern. Woher weiß man, woher die Hacker angreifen?
Eine IP-Adresse hat ungefähr den Integritätswert einer Postkarte. Die kann ich auch mit beliebigem Absender verschicken. Beispielsweise können Hacker zunächst ein System kapern und von dem dortigen Mailserver ihren Angriff starten. So verdächtigt der Angegriffene einen falschen Absender als Angreifer.

Woher stammen dann Gewissheiten, dass Cyberattacken aus Russland oder China kommen?
Gewissheiten gibt es nicht, aber Wahrscheinlichkeiten. Ein Indikator ist die mögliche Motivation. Wird der örtliche Handwerksbetrieb um ein paar Hundert Euro erpresst, sind staatliche Akteure, Politaktivisten oder Cyberterroristen als Täter unwahrscheinlich. Skript-Kiddies wären dagegen eine realistische Option. Ein Hackerangriff auf die Bundesregierung kurz nach der Verabschiedung von Hilfsgeldern für die Ukraine lässt auf einen staatlichen Akteur schließen. Krankenhäuser waren zunächst ebenfalls im Visier von staatlich finanzierten Hackern. Dabei geht es darum, das Vertrauen der Bevölkerung eines anderen Landes in lebenswichtige Institutionen zu unterminieren. Irgendwann haben einige Hacker gemerkt, dass sich im Gesundheitssektor viel Geld erpressen lässt und operieren seitdem unabhängig von Regierungen auf eigene Rechnung.

Existieren, abgesehen von der Motivation, noch weitere Indikatoren, die auf die Herkunft der Hacker schließen lassen?
Sicher. Ein weiterer Hinweis ist die Methodik. Das ist wie in der realen Welt. Dort versucht der Kriminalkommissar auch von der Art des Einbruchswerkzeugs oder dem Einbruchsweg auf den Täter zu schließen. Bei Cyberangriffen analysieren wir ebenfalls die verwendeten Tools und Strategien.

Also eine Mischung aus Motivation und Vorgehen?
Genau! Wir nennen das Prinzip TTP – Tactics, Techniques and Procedures. Tactics untersucht die übergeordneten Ziele der Angreifer, Techniques die Umsetzungsmethode und Procedures die konkrete Vorgehensweise. Am Hasso-Plattner-Institut haben wir mal eine KI darauf trainiert, die Arbeitsweise einer bestimmten Hackergruppe zu untersuchen. Die KI ermittelte aufgrund der Zeitverschiebung, dass die Täter offenbar von China aus arbeiten. Sie erkannte, wann die Leute Mittagspause machten, und konnte sogar feststellen, wann einzelne Akteure Urlaub hatten. Sind das gerichtsfeste Beweise, wer hinter den Angriffen steckt? Selbstverständlich nicht. Aber starke

Indizien.

Hier geht es zu Teil 1 und Teil 3 des Interviews.

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