NACHRICHTEN

IT-Sicherheit in der Pflege: Erpressungsversuche im Gesundheitswesen nehmen zu

„Es kann jede und jeden treffen“

Die Digitalisierung schreitet voran, doch der Einsatz komplexer IT birgt auch Gefahren. Denn Cyberkriminalität stellt auch für Pflegeeinrichtungen eine Bedrohung dar. Wie Sie Angriffe und Erpressungsversuche abwehren, erklärt IT-Experte Thomas Althammer.

Interview: Steve Schrader

Herr Althammer, weltweit mehren sich die Schlagzeilen über Hackerangriffe im Gesundheitswesen. Im September 2020 etwa konnte die Notaufnahme der Uniklinik Düsseldorf nach einem Übergriff tagelang nicht mehr richtig arbeiten. Warum haben es Cyber-Kriminelle immer öfter auf Einrichtungen des Gesundheitswesens abgesehen?
Das ist aus zweierlei Gründen lukrativ: Zum einen können Angreifer für einen vollständigen Patientendatensatz oder eine digitale Patientenakte deutlich mehr Geld verlangen, als z. B. für gestohlene Kreditkartendaten. Hier gibt es einen florierenden Handel im „Dark Web“, einem abgeschotteten Bereich des Internets.

Foto: Archiv

// Ich habe schon mehrfach Erpressungen in der Branche beobachtet – teils mit kleinen, teils mit großen Auswirkungen. //

Thomas Althammer

Die zweite und aktuell weitaus größere Bedrohung sind zufällige Angriffe, die sich im Gesundheitswesen besonders stark auswirken. Dabei werden Software-Fehler oder Unachtsamkeit im Umgang mit E-Mails ausgenutzt, um in Systeme einzudringen. Hierbei handelt es sich zunächst nicht um gezielte Angriffe, es kann also jede Organisation treffen. Sobald eine erste Lücke identifiziert ist, gehen die Angreifenden dann gezielt weiter vor und versuchen, Systeme umfassend zu kompromittieren. Aufgrund des Erpressungspotentials und der Anfälligkeit heutiger IT-Systeme gerade im Gesundheits- und Sozialwesen können diese Angriffe einen sehr hohen materiellen und immateriellen Schaden verursachen, wie das Beispiel der Düsseldorfer Uniklinik zeigt. Ähnlich hat es beispielsweise die Funke Mediengruppe Ende 2020 erwischt. Viele Tageszeitungen sind über Wochen nur als reduzierte Notausgaben erschienen.

Besonders in Mode ist derzeit die Ransomware. Wie gehen Kriminelle hier vor?
Hierbei handelt es sich schlichtweg um Erpressung. Zunächst ist eine Lücke erforderlich, über die Schadsoftware eingeschleust und aktiviert werden kann. Im Fall des „Phishing“ werden Mitarbeitende durch gut gefälschte E-Mails dazu verleitet, selbst die Schadsoftware zu installieren. Es besteht aber auch die Möglichkeit, schlecht gesicherte IT-Systeme und Software-Fehler zu nutzen, um Verschlüsselungstrojaner zu aktiveren. Dann beginnt die eigentliche Erpressung: Alle erreichbaren Datenträger und Systeme werden verschlüsselt. Erst gegen Zahlung eines Lösegeldes erhält man wieder Zugriff auf die verschlüsselten Daten.

Nun betrifft das Problem insbesondere die großen Kliniken und Verbünde. Wie gefährdet sind aus Ihrer Sicht Pflegeeinrichtungen?
Ich halte Pflegeeinrichtungen für gleichermaßen sehr gefährdet. Auf der einen Seite sind zwar die in der Pflege eingesetzten IT-Systeme weniger komplex als im medizinischen Umfeld. Auf der anderen Seite hinken IT-Budgets und Professionalisierungsgrad von IT-Abteilungen in Sozialwirtschaft und Pflege den Aufwendungen für IT-Sicherheit in Kliniken hinterher. Grundsätzlich gilt, dass sich niemand in Sicherheit wähnen sollte, es kann jede und jeden treffen.

Gibt es hier schon Erpressungsversuche, von denen Sie berichten könnten?
Ich habe schon mehrfach Erpressungen in der Branche beobachtet und begleitet, teils mit kleinen, teils mit großen Auswirkungen. Vor wenigen Wochen wurde auch mein Unternehmen unter Druck gesetzt und auf eine gewisse Art erpresst. Im Fall von Erpressungstrojanern gilt es, so schnell wie möglich die Systeme abzuschalten und zu isolieren. Glücklich ist, wer auf ein funktionierendes Back-up und einen Notfallplan zurückgreifen kann. Doch das klappt nicht immer reibungslos. In den seltensten Fällen finden Notfallübungen statt, in denen eine vollständige Wiederherstellung tatsächlich einmal durchgespielt wird. Das wäre so, als wenn eine Brandmeldeanlagen erstmalig bei einem richtigen Brand auf ihre Funktionsweise getestet wird. Das ist eigentlich undenkbar, in der IT aber leider Realität.

Wie gut sehen Sie die Einrichtungen hier aufgestellt, um die Angriffe abzuwehren?
Jedes über das Internet erreichbare IT-System wird stets und ständig angegriffen. Die gute Nachricht ist, dass eine Vielzahl von Angriffen abgewehrt wird. Aufgrund der Vielzahl von Angriffsvektoren in Verbindung mit zunehmender Komplexität und Vielfalt IT-basierter Geräte nimmt das Bedrohungs- und Schadenspotential jedoch stark zu. Die Frage ist heute nicht mehr, ob ein Angriff erfolgreich ist. Jedes System ist verwundbar. Mit anderen Worten: Gehen Sie davon aus, dass Sie bereits gehackt sind. Die Frage ist also eher, was kann getan werden, um das Schadensausmaß und die Konsequenzen möglichst gering zu halten und Datenpannen zu vermeiden?

Was raten Sie den Einrichtungen, wenn es zu einem Angriff kommt?
Holen Sie sich möglichst schnell professionelle Hilfe! In erster Linie gilt es natürlich, die IT-Systeme zu schützen bzw. wieder lauffähig zu bekommen. Nach einem Ransomware-Angriff kann je nach konkreten Umständen ein kompletter Tausch der Hardware und eine komplette Neuinstallation der Systeme erforderlich werden. Darüber hinaus gibt es eine Reihe von Gewerken, die ebenfalls einzubeziehen ist. Sie benötigen Projektmagement, Forensik/Spurensicherung, PR- und Krisenkommunikation, Rechtsbeistand sowie einen Versicherungsexperten für die Schadensmeldung bei Ihrer Cybersecurity-Police. Zu bedenken ist auch das Melden einer möglichen Datenpanne bei der Datenschutz-Aufsichtsbehörde innerhalb von 72 Stunden. Versäumnisse können je nach Frist und Sachlage ein Bußgeld nach sich ziehen!

Und wie können sich die Einrichtungen schon im Vorfeld besser schützen?
Die Zeiten, in denen Virenscanner die Systeme abgesichert haben, sind lange vorbei. Es braucht ein umfassendes Informationssicherheitsmanagement. Dazu zählt neben technischen Schutzmaßnahmen insbesondere eine Sensibilisierung der Mitarbeitenden („Security Awareness“), z. B. durch Simulation von Phishing-Kampagnen und gezielten Schulungsmaßnahmen. Des Weiteren sind Back-up und Wiederherstellung kritisch zu prüfen und regelmäßig zu testen. Ich würde mich hier nicht blind auf den Administrator verlassen, sondern dem 4-Augen-Prinzip folgen. Im Rahmen einer unabhängigen Bestandsaufnahme treten so viele Verbesserungspotentiale zu Tage, bei denen im Fall der Fälle vielleicht genau der eine Punkt das Zünglein an der Waage war, um einen Angriff erfolgreich abzuwehren.

Erwin Rüddel will Fachkräfte langfristig im Beruf halten

Fünf Milliarden Euro für Pflegereform

Berlin // Der Vorsitzende des Gesundheitsausschusses im Bundestag, Erwin Rüddel (CDU), will weitere fünf Milliarden Euro in die Pflege investieren, um Fachkräfte zu halten. „Deshalb verhandeln wir im Moment mit dem Finanzminister, dass wir fünf Milliarden zusätzlich bekommen für eine Pflegereform, die letztendlich dazu führen soll, dass also die Pflege besser entlohnt wird und auf der anderen Seite die Eigenanteile der Pflegebedürftigen begrenzt werden“, sagte der CDU-Politiker am 19. April im ARD-Mittagsmagazin. In jüngster Vergangenheit hatten sich Wirtschaftsverbände der Union gegen die geplante Steuerfinanzierung einer Pflegereform gewandt.

In den vergangenen zwei Jahren seien die Löhne für die Pflege in Krankenhäusern im Durchschnitt um rund 14 Prozent gestiegen, in der Altenpflege um rund zehn Prozent, erklärte Erwin Rüddel. „Wir haben für die Altenpflege einmal 13 000 examinierte und 20 000 zusätzliche Hilfskräfte finanziert, wobei es schwierig ist, diese Stellen zu besetzen.“ Arbeit auch am Wochenende, Schichtdienste und die Vereinbarkeit von Beruf und Familie überforderten viele.

Es sei eine gesamtgesellschaftliche Aufgabe, Pflegeberufe attraktiver zu machen. „Also wir haben es nicht geschafft, mehr Menschen für den Pflegeberuf zu begeistern“, gab der CDU-Politiker Versäumnisse zu. „Oder anders ausgedrückt: Wir haben relativ viele, die in den Beruf einsteigen und die Ausbildung machen, dann aber nach einigen Jahren das Handtuch werfen, weil die Belastungen zu groß sind.“ (ck)