Foto: Althammer & Kill

Digitalisierung in der Pflege

Schutz der Patienten-Daten wird immer wichtiger

von Simon Lang (Produktmanager)
und Maximilian Klose (Berater für Cloud- & Cyber-Security)

Viele Prozesse sollen künftig auch in der Altenpflege digitalisiert werden. Das sorgt für Straffung von Arbeitsprozessen, Entlastung von Mitarbeitenden und neue Formen des Arbeitens. Viele Pflegeorganisationen haben allerdings noch an vielen Stellen Nachholbedarf.

Insbesondere beim Ausbau der Infrastruktur (Hard- und Software) und der Schulung und Sensibilisierung von Mitarbeitenden. Dies ist jetzt besonders wichtig, denn der Gesundheitssektor soll aufholen was die Digitalisierung angeht – so will es die Bundesregierung und setzte im vergangenen Jahr das „Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz" in Kraft. Systeme wie bspw. elektronische Patientenakten und medizinische Gerätschaften werden zum Einsatz kommen, die miteinander verbunden sind und untereinander Daten austauschen.

Die steigende Digitalisierung ruft auch vermehrt Cyber-Kriminelle auf den Plan. Die Zahl an Cyber-Attacken auf Unternehmen und Organisationen steigt seit Jahren stetig an. Bis zu 553.000 neue Schadprogramm-Varianten pro Tag verzeichnete das Bundesamt für Sicherheit in der Informationstechnik (BSI) zuletzt. Besonders Ransomware macht Probleme. Diese verschlüsseln die Festplatten der Opfer und machen sie dadurch handlungsunfähig – erst durch Zahlung eines Lösegeldes, ist ein „weiterarbeiten" möglich. Einer Bitcom-Studie

zufolge waren 88 % der Unternehmen in den letzten beiden Jahren von Datenklau, Spionage und Sabotage betroffen, eine Schadensumme von 220 Milliarden Euro pro Jahr!

„In unserer täglichen Praxis sehen wir, dass sich das Sozial- und Gesundheitswesen als Ziel von Cyberangriffen besonders anbietet", sagt Thomas Althammer, Geschäftsführer der Althammer & Kill GmbH & Co. KG. „Denn gerade in diesem Bereich nimmt die Masse an elektronischen Daten stetig zu, um Betreuungen und Behandlungen von Patientinnen und Patienten effizienter gestalten zu können. Diese Daten sind sehr sensibel, handelt es sich doch um persönliche Informationen zum Patienten und seiner Gesundheit." Viele dieser schützenswerten Daten bedeuten für Angreifer eine größere „Verhandlungsmasse" – die Lösegeldforderungen fallen dementsprechend höher aus.

Ist die Budgetierung der IT- und Security-Abteilungen zu knapp bemessen, können Lücken entstehen, die von Cyber-Kriminellen erkannt und ausgenutzt werden. Dem „Allianz Risk Barometer 2022" zufolge sehen inzwischen 44 % der befragten Verantwortlichen Angriffe auf ihre IT-Systeme als das größte Geschäftsrisiko, noch vor Betriebsunterbrechungen und Naturkatastrophen!

Die aktuellen Fälle von Diebstahl und Missbrauch von Identitäten zeigen, dass die digitale Eigenverantwortung (Security Awareness) jedes einzelnen Mitarbeitenden einen wesentlichen Bestandteil der nachhaltigen Informations- und IT-Sicherheit darstellt. Gerade weil IT-Systeme laufend aktualisiert werden, führt der einfachste Weg einer erfolgreichen Cyber-Attacke über die Nutzer von Webanwendungen, Plattformen und Apps. „Verantwortliche müssen sich bewusst machen, dass bis zu 95 % der erfolgreichen Angriffe durch menschliche Fehler ermöglicht werden", so Althammer weiter. „Nur geschulte Mitarbeitende sind aufmerksam und fallen auf z. B. Phishing- oder Spear Phishing-Mails nicht herein."

Beim Phishing werden bspw. Passwörter oder Identitäten erschlichen, beim Spear Phishing sind diese Mails sehr gezielt auf eine bestimmte Organisation abgestimmt. Im beruflichen Kontext wird es dann gefährlich, wenn durch den Zugang zu Systemen Informationen abgesogen oder Schadsoftware platziert werden kann. 207 Tage dauert es durchschnittlich, bis ein Angriff entdeckt wird, weiß Althammer, und in dieser Zeit kann viel Schaden entstehen.

Was also tun, um in der eigenen Organisation die IT-Sicherheit zu steigern?

„Eines ist klar, 100%ige Sicherheit kann es nicht geben, aber zahlreiche Maßnahmen senken das Risiko einer Cyber-Attacke deutlich", sagt Althammer.

Der Mensch im Mittelpunkt

Für Mitarbeitende in Pflege & Gesundheit liegt primär das Wohlergehen der Patienten im Fokus. Diese Berufsgruppe hat bisher oft wenig Berührungspunkte mit dem richtigen Umgang mit IT-Anwendungen. Deshalb sind sie für Hacker ein willkommenes Ziel. Wer versehentlich einen unbekannten Link von einem vermeintlich bekannten E-Mail-Absender

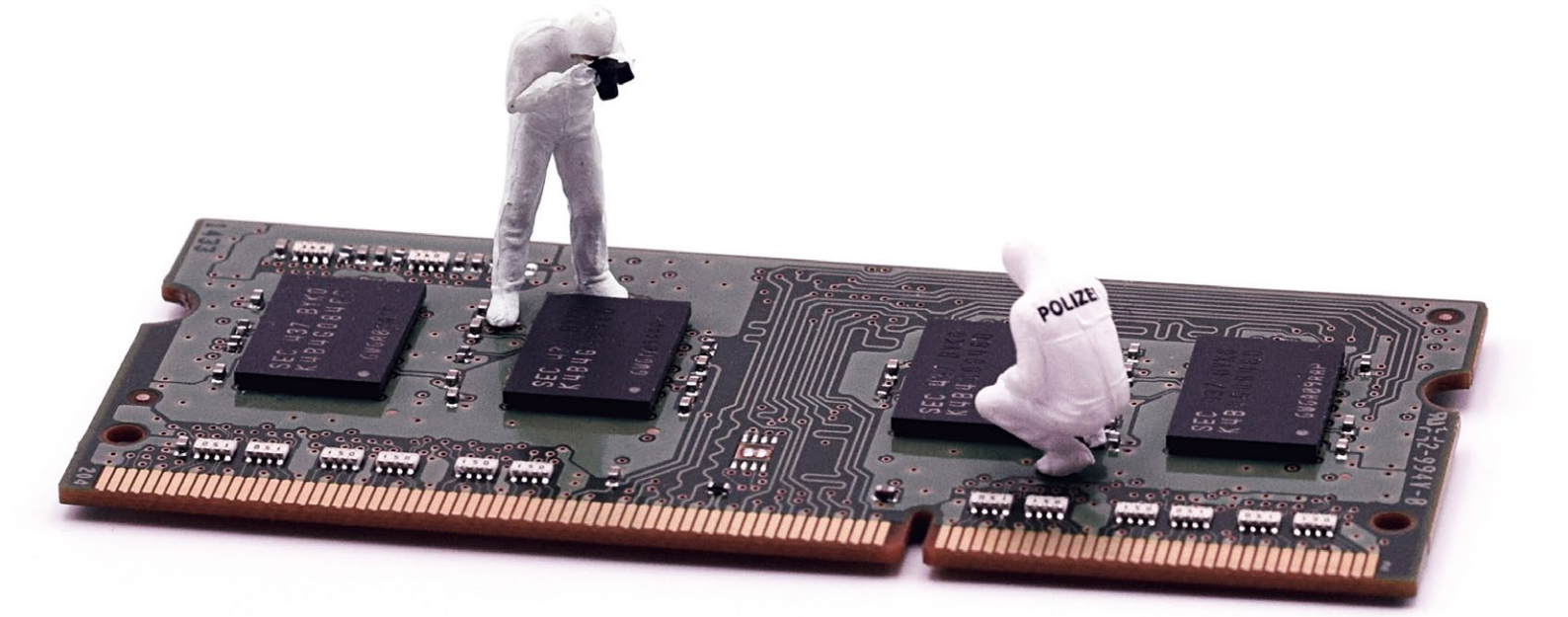

Foto: Althammer & Kill

anklickt, schafft eine neue Lücke für Angriffe. Um Fehlverhalten zu minimieren und Mitarbeitende auf die Gefahren aufmerksam zu machen, sind sogenannte Security Awareness Maßnahmen unabdingbar.

Dabei werden anhand von Simulationen real existierende Attacken nachgebildet, deren Ergebnis ausgewertet und passgenaue Schulungs- und Sensibilisierungskonzepte (Poster, Plakate, etc.) ausgearbeitet. Besonders dafür geeignet sind Phishing-Kampagnen. (Phishing = Angreifer versuchen Zugangsdaten von Mitarbeitenden einer Organisation zu erschleichen. Dazu werden täuschend echte E-Mails versendet, oftmals mit der Aufforderung, einen Link anzuklicken und Zugangsdaten einzugeben.)

Nicht nur eine Intervention von außen erzeugt Schwierigkeiten. Auch Sprachassistenten wie Siri, Alexa oder Cortana können in Pflegeheimen ein Datenschutzleck darstellen. Insbesondere Pflegekräfte müssen sich der Tatsache bewusst sein, dass Sprachassistenten Gespräche im Patientenzimmer aufzeichnen. Die Übermittlung in Drittländer – wie die USA – ist nicht sonderlich sicher und eventuell können Dritte die Daten abrufen. Besonders im Fall von pflegebedürftigen Personen können sensible Daten (wie Gesundheitsdaten) verarbeitet werden.

Richtlinien als Leitplanken der IT-Sicherheit

Wie Passwörter zusammengesetzt und in welchem Rhythmus sie geändert werden müssen, können IT-Richtlinien beantworten. Das gilt auch für das richtige Verhalten bei merkwürdig anmutenden E-Mails.

Immer auf dem aktuellen Stand

Die Vielzahl an Angriffsvektoren, die schnell fortschreitende Technologie und neue Anforderungen an unsere Arbeit, sorgen für eine stetige Weiterentwicklung der IT-Systeme und Anwendungen. Sie müssen deshalb immer auf den neuesten Stand gebracht werden, insbesondere was Sicherheits-Updates angeht.

Den Überblick behalten

Welche IT-Systeme und Anwendungen existieren in der eigenen Organisation?

Nutzen alle dieselben Apps oder gibt es Wildwuchs, z. B. durch von Mitarbeitenden installierte Software?

Um Systeme regelmäßig kontrollieren zu können, müssen die Verantwortlichen eine Liste mit getesteter und freigegebener Hard- und Software führen.

Wenn IT-Systeme sicher und datenschutzkonform konfiguriert werden, ist viel getan. Angreifer wissen, dass die Lücken bei gut konfigurierten Systemen sehr klein sind und es schwer wird, in diese einzubrechen. Ist auf der anderen Seite die Belegschaft geschult und durch simulierte Szenarien sensibilisiert, verringert sich auch das Risiko, durch Unachtsamkeit gegenüber Erpressung, Identitäts- und Datenklau Schaden zu nehmen. Dessen müssen sich Pflegeeinrichtungen stets bewusst sein. Auch ein objektiver Blick von außen kann helfen, Lücken zu entdecken und zu schließen oder im Schadensfall das Ausmaß zu reduzieren.