So schützen sich Spitäler und Gesundheitsdienstleister vor Ransomware

Der externe Zugriff von Mitarbeitenden auf unzureichend gesicherte Unternehmensnetzwerke sorgt für einen Anstieg der Cyberkriminalität in der Schweiz. Unter anderem im Fokus der Angreifer, die darauf aus sind, Lösegeld durch Ransomware-Bedrohungen zu erpressen: Spitäler und Dienstleister aus der Gesundheitsbranche.

Spitäler verwalten sensible Daten und stehen im Visier von Cyberangreifern. Bereits Ende Oktober 2019 war die Gesundheitsbranche in der Schweiz Ziel von Angriffen mit der Schadsoftware Emotet. Im vergangenen Jahr stieg die Anzahl von Ransomware-Bedrohungen weiter an. Die Folgen sind oft gravierend: Der Verlust von Daten aus Krankenakten und eine Unterbrechung der IT-Infrastruktur können für den einzelnen Patienten lebensbedrohlich und für Spitäler rufschädigend sein.

Der Wert, den Krankenakten im Darknet haben, macht Spitäler zu einem interessanten Ziel. Für bis zu 1000 US-Dollar pro Stück lassen sich Patientendaten verkaufen, zum Vergleich Kreditkartennummern hingegen lediglich für 5 Dollar. Trotz dieser Gefahr gibt es viele Schwachstellen: Unkontrolliert gewachsene IT-Strukturen in Verbindung mit veralteten IT-Lösungen tragen dazu bei, dass Spitäler ein leichtes Ziel sind.

Spitäler sind lohnende Ziele – so können sich diese schützen

Für Krankenhäuser ist eine umfassende Sicherheitsstrategie notwendig, die sowohl Präventions- und Erkennungstechnologien wie auch Massnahmen zu einer schnellen und zielführenden Reaktion beinhaltet. Im Zentrum stehen sollten Intrusion-Prevention- und Antivirus-Technologien, die bereits das Eindringen von Schadsoftware verhindern. Da E-Mails nach wie vor die häufigsten Einfallstore sind, ist ein sicheres E-Mail-Gateway-System in Kombination mit einer Web Application Firewall, die Schutz für Webanwendungen bietet, absolut zwingend.

Bild: James Thew / Fotolia.com

Der Autor
Franz Kaiser, Regional VP, Fortinet

Um sicherzustellen, dass nur autorisierte Benutzer auf das Netzwerk zugreifen können, ist die Netzwerkzugriffskontrolle eine perfekte Ergänzung. Das auch im Hinblick auf Mitarbeitende, die von aussen auf die IT-Infrastruktur zugreifen. Eine SIEM-Lösung (Security Information and Event Management) ermöglicht ausserdem eine Echtzeitanalyse von Bedrohungen und bildet diese in Bezug auf das jeweilige Spital ab. Somit können Bedrohungen schneller entdeckt und Schwachstellen im System lokalisiert werden.

Doch auch, wenn modernste Sicherheitswerkzeuge zum Einsatz kommen, darf mit rund 99 Prozent die häufigste Angriffsmöglichkeit nicht ausser Acht gelassen werden: der Mensch. Der Erfolg von Hackern hängt davon ab, ob Anwender auf einen Link klicken, eine Datei herunterladen oder Passwörter preisgeben. Aus diesem Grund sind Cybersecurity-Trainings der Mitarbeitenden im Bezug auf den richtigen Umgang mit digitalen Bedrohungen für Spitäler genauso wichtig wie Hygiene-Schulungen.

Vorbeugen statt heilen

Die Digitalisierung des Gesundheitswesens schreitet unter anderem durch Videosprechstunden weiter voran. In der Schweiz bietet das elektronische Patientendossier viel Potenzial für patientenfreundliche Behandlungsmöglichkeiten. Massnahmen für die Sicherung des IT-Netzwerks, der Geräte und Endpunkte sind daher wichtiger denn je. Spitäler sollten nach automatisierten, integrierten, globalen Cybersecurity-Ansätzen von Anbietern suchen, die die besonderen Belange dieses Bereichs verstehen. Schutzmassnahmen müssen nicht den Grossteil des Budgets eines Krankenhauses verschlingen und erfordern auch kein umfangreiches technisches Wissen – aber die richtige Unterstützung und eine proaktive Einstellung.

Den Beitrag finden Sie auch online
www.netzwoche.ch