Sicherer Datenaustausch im Gesundheitswesen

Kliniken stärken ihre Cyberabwehr mit Datenschleusen

Cyberangriffe sind für den medizinischen Sektor eine ernsthafte Gefahr. Die größte Bedrohung lauert beim Datenaustausch, ob durch mobile Devices wie USB-Sticks oder File- und Cloud-Shares. Viele Kliniken und Labore sind sich nicht bewusst, dass auf diesem Weg Malware unbemerkt ins eigene Netzwerk gelangen und massive Schäden anrichten kann. Datenschleusen stärken die Sicherheit deutlich, und zwar kostengünstig und ohne großen Aufwand.

Patientendaten werden digital auf Computern gespeichert, immer mehr medizinische Geräte sind ans Internet angeschlossen, Roboter unterstützen bei minimal-invasiven Eingriffen. Ob im OP und Labor, in der Pflege und Verwaltung: Die Digitalisierung im Gesundheitsbereich schreitet voran, während die Sicherheit oft hinterherhinkt. Dabei ist die Gefährdungslage in Deutschland so hoch wie noch nie. Cyberangriffe auf Krankenhäuser stellen eine große Gefahr dar, betonte Claudia Plattner, die neue Präsidentin des Bundesamts für Sicherheit in der Informationstechnik (BSI), bei ihrer Antrittspressekonferenz. Dringen Cyberkriminelle in die IT ein, verschlüsseln Server und erpressen Lösegeld, verursacht das in der Industrie hohe finanzielle Schäden. Bei Krankenhäusern stehen im schlimmsten Fall sogar Menschenleben auf dem Spiel, wenn etwa Ransomeware die IT einer Abteilung lahmlegen und deswegen Patienten nicht behandelt werden könnten.

Eine der größten Cybergefahren, die seit Jahren die Top-10-Liste der Bedrohungen des BSI anführt, sind Wechseldatenträger, die Schadprogramme und Viren einschleusen. Doch wie gelangen sie ins Krankenhaus? Beispielsweise mit einem Servicetechniker, der die Updates für die von ihm gewarteten Geräte auf einem USB-Stick mitbringt. Nicht abwegig ist die Vorstellung, dass er den Stick einmal kurz mit seinem privaten Rechner verbindet, um sich ein wenig Musik für die Autofahrt runterzuladen. Dass sich dadurch ein schädliches Programm auf dem USB-Stick einnisten kann, ist ein Risiko, dessen sich kaum jemand bewusst ist. Beim Aufspielen des Updates überträgt sich das Virus dann auf das Gerät und breitet sich von dort unbemerkt im Netzwerk des Krankenhauses aus. Dabei hat es leichtes Spiel, denn die Endpunkte der Betriebstechnik, vom Röntgengerät bis zur Klimaanlage, werden häufig ohne aktiven Virenschutz betrieben.

Klare Sicherheitsregeln mit Technik kombinieren

Das geschilderte Szenario und daraus resultierenden Schäden sind durchaus vermeidbar. Das setzt voraus, dass die medizinische Einrichtung eine Sicherheitsrichtlinie besitzt, die den wechselseitigen Datenstrom in und aus der eigenen Infrastruktur klar definiert. Das Einfachste wäre, den Datenaustausch einfach zu verbieten. Aber das ist für Kliniken keinesfalls praktikabel – man denke nur an Patienten, die zur Untersuchung Röntgenbilder, Arztbriefe und Fotos in digitaler Form mitbringen.

Der bessere Weg ist es, die Sicherheitsrichtlinie mit einer technischen Lösung zu kombinieren, die den gesetzlichen Vorgaben entspricht. Das gilt insbesondere für Krankenhäuser, die aufgrund ihrer Auslastung mit mehr als jährlich 30.000 vollstationären Patientinnen und Patienten zu den Kritischen Infrastrukturen (KRITIS) zählen. Sie sind verpflichtet, sich nach ISO 27001 zu zertifizieren, und dabei mögliche Gefährdungen, die das BSI in seinem IT-Grundschutz-Kompendium aufzählt, für die eigene Infrastruktur festzulegen und Vorsorge zu treffen. Der Einsatz einer Datenschleuse ist eine zulässige Maßnahme – und das für verschiedene Gefährdungen u. a. Datenverlust, Missbrauch von Berechtigungen, Diebstahl von Geräten und Datenträgern, Offenlegung schützenswerter Informationen, Verstoß gegen Gesetze und Regelungen sowie der Manipulation von Informationen.

Eine Datenschleuse, wie die von der Firma telent entwickelte „InDEx“ (Intelligent Data Exchange), ist ein System, das zu importierende Daten untersucht, bevor sie mit einem internen Netzwerk in Berührung kommen. Die Lösung besteht aus einem speziell für diese Aufgabe entwickelten Rechner in einem robusten Gehäuse mit allen notwendigen Schnittstellen und einer professionellen Software zum Scannen der portablen Medien und Cloud-Files. Den Empfehlungen des BSI folgend, sollte eine Datenschleuse nicht auf demselben Betriebssystem laufen, das ein Krankenhaus bereits verwendet. Ist das typischerweise Windows, bietet eine mit einem speziell gehärteten Unix-System betriebene Datenschleuse ein zusätzliches Plus an Sicherheit.

Die Datenschleuse übernimmt – im übertragenen Sinne – die Aufgabe des Wachpersonals, das Zutrittskontrollen durchführt und nur ungefährliche Gäste einlässt. Findet der Scanner keine Bedrohung, darf das Medium ins Netzwerk hinein. Im zuvor beschriebenen Beispiel des Servicetechnikers wäre das Virus erkannt und der USB-Stick zurückgewiesen worden. In diesem Fall muss ein festgelegter Prozess starten, der vorschreibt, was zu tun ist. So kann die eigene Security Policy festlegen, dass ein infiziertes Medium grundsätzlich nicht verwendet werden darf. Eine andere Möglichkeit wäre, die infizierte Datei mithilfe der Datenschleuse zu löschen und das Scanergebnis anschließend nochmals zu bewerten. Für den Fall, dass eine nicht benötigte Datei als infiziert eingestuft wurde, die aktuell erforderliche Datei aber als sauber, könnte diese über die Datenschleuse auf ein im besten Fall inventarisiertes Medium kopiert werden, das dann zugelassen wird.

Datenschleusen werden stündlich aktualisiert

Die Methoden der Cyberkriminellen werden immer ausgefeilter und sie liefern sich mit Antivirus-Herstellern ein hartes Kopf-an-Kopf-Rennen. Um ein Schadprogramm aufzuspüren, muss die Antiviren-Software die individuelle Signatur jedes einzelnen Virus kennen. Bei täglich mehr als 260.000 neuen Malware-Varianten, laut BSI, ist das eine enorme Aufgabe. Wirksam schützen können nur Antiviren-Programme, die immer auf den neuesten Stand gebracht werden. Im Office-Umfeld geschieht das meistens einmal pro Tag. Datenschleusen schützen wesentlich effektiver, da sie Antiviren-Programme bündeln und so quasi zum Multiscanner werden. Je mehr Programme eingesetzt werden, desto wahrscheinlicher ist, dass eines von ihnen im Wettlauf gegen die Cyberkriminellen die Nase vorn hat. Außerdem aktualisiert die Datenschleuse stündlich die Signaturen über eine verschlüsselte Verbindung mit dem Signaturserver, der im eigenen Firmennetz oder bei einem Dienstleister betrieben werden kann. Mit einem Rundum-Service, der zusätzlich zum Signaturen-Update auch Maintenance, Monitoring, Fernwartung und Patchmanagement beinhaltet, ist die Datenschleuse wartungsarm. Zudem entlastet sie das eigene Sicherheitspersonal, da die Datenschleuse jeden Vorgang protokolliert, Reportings für Zertifizierungen erstellt und sich über ein Security Incident and Response System (SIEM) darstellen lässt. Damit ist es ein Baustein in einer ganzheitlichen Sicherheitsstrategie, der sich nahezu im Handumdrehen umsetzen lässt, und im Vergleich zu anderen Maßnahmen für wenig Budget das Sicherheitsniveau einer medizinischen Einrichtung deutlich erhöht.

Karin Eichholz, Lead Software Consultant, Technologie Center, telent GmbH