Datensicherheit – nicht nur die Software, auch der Mitarbeiter zählt

▶ Zunehmend setzt sich im Gesundheitswesen die Erkenntnis durch, dass Cyberattacken eine sehr reale Bedrohung sind. Leistungserbringer müssen daher die Sicherheit aller medizinischen Daten gewährleisten.

Bei Sectra haben die Angriffe auf Gesundheitseinrichtungen im Unternehmen selbst zu Veränderungen geführt: Sectra Communications – der Geschäftsbereich, der Lösungen und Leistungen im Bereich Cybersicherheit anbietet – arbeitet jetzt wesentlich enger mit den Teilen des Unternehmens zusammen, die IT-Lösungen für die medizinische Bildverarbeitung entwickeln. Dem Unternehmen ist dabei besonders wichtig, die Integrität und Vertraulichkeit von Daten zu sichern und gleichzeitig die Möglichkeit zu bewahren, Daten ohne Beeinträchtigung der Sicherheit auszutauschen.

Simo Pykälistö leitet den Sectra-Geschäftsbereich Cybersecurity. Kunden kommen typischerweise aus der Rüstungsindustrie und aus Branchen, die kritische Infrastrukturleistungen erbringen. In letzter Zeit greifen allerdings zunehmend Player aus dem Gesundheitswesen auf die mehr als 40-jährige Cybersecurity-Erfahrung von Sectra zurück. Pykälistö, der für das Produktportfolio sichere Kommunikation und Zusammenarbeit zeichnet, betont die Schlüsselrolle seiner Sicherheitslösungen im Krankenhaus.

Gewappnet auch bei Verbindungsausfällen

Sectra bietet Lösungen für den sicheren mobilen Datenzugriff und überwacht und sichert besonders wichtige Netzwerke für Behörden, Energieversorger und andere Unternehmen, die auf eine sichere Kommunikation angewiesen sind, wie etwa Krankenhäuser. Kern der mobilen Lösungen ist – wie bei allen Unternehmen in dieser Branche – die VPN-Technologie (Virtual Private Network). Das Sectra Mobile VPN ist für iOS- und Android-Geräte konzipiert und kann auf der Android-Plattform über eine besondere Mikro-SD-Karte sogar noch enger verankert werden. Auch bietet der besondere VPN-Ansatz von Sectra ein besseres Roaming als andere Anbieter: „Ganz gleich, ob Daten im Krankenhaus auf einem

SECTRA
Knowledge and passion

Smartphone, einem Tablet oder an einer Workstation verwendet werden – sie sind immer sicher“, erklärt Pykälistö.

Wird die sichere Verbindung unterbrochen, stellt das VPN-System von Sectra diese automatisch wieder her, sobald ein Signal verfügbar ist – und zwar, ohne dass sich der Nutzer erneut einloggen muss. „Das unterscheidet unsere Lösung von dem klassischen VPN-Angebot“, berichtet der Sicherheitsspezialist und fährt fort: „Sogar bei einem kompletten Verbindungsabbruch macht das System da weiter, wo es aufgehört hat, sobald das Signal wieder da ist. Das ist besonders für Krankenhäuser wichtig, die auf ständige Verfügbarkeit angewiesen sind. Sie brauchen ein System, das praktisch und zuverlässig ist und rund um die Uhr funktioniert.“

„Viele unserer Kunden in Gesundheitseinrichtungen nutzen unsere Lösung jetzt schon für Kriseninformationen, sie kann aber auch jederzeit für die Übertragung von Patientenakten, -bildern oder Informationen aus der Verwaltung eingesetzt werden“, erläutert Pykälistö. Diese Anwendung ist eine Weiterentwicklung der Softwarelösungen für Sicherheitskräfte, Polizei und Energieversorger, die trotz Remote-Zugriffs ein Höchstmaß an Sicherheit bei der Datenübertragung benötigen. Der Schutz von Patientendaten ist von entscheidender Bedeutung – entsprechend hoch sind die Strafen bei Verstößen gegen diese Sicherheitsvorschriften. In der Konsequenz genießen Übertragung und Speicherung von Daten in jedem Krankenhaus heute eine hohe Priorität.
Das ist keine Überraschung, denn Berichte über Cyberattacken auf Gesundheitseinrichtungen und medizinische Datenlecks gab es in den vergangenen Jahren zuhauf – der Schaden, der dadurch angerichtet wurde, ist vielen Betreibern eine effektive Warnung.

Ganzheitlicher Ansatz statt Flickenteppich

Damit die Sicherheit in Krankenhäusern auch umfassend gewährleistet ist, legt Sectra großen Wert auf die Schulung der IT-Teams in Krankenhäusern. „Denn es geht nicht nur darum, unsere Software korrekt zu implementieren, sondern vielmehr bei allen das Bewusstsein für die Bedeutung einer sicheren Kommunikation zu schärfen“, so Pykälistö. Der IT-Spezialist drängt darauf, die Schulung von Krankenhauspersonal im Bereich sicherer Datenübertragung deutlich auszubauen.

Für Pykälistö lässt sich die IT-Sicherheit in vielen Krankenhäusern erheblich verbessern, wenn ein ganzheitlicher Ansatz verfolgt wird, statt nur zu schauen, wie Sicherheit an einzelnen Geräten gehandhabt wird. So wird sichergestellt, dass Schlupflöcher frühzeitig erkannt und gestopft werden. Das betrifft vor allem die Frage, wie Daten zwischen Geräten und Systemen übermittelt werden – kurz: die allgemeine Sicherheitskultur. Man müsse, unterstreicht Pykälistö, „die Gefahr von Cyberangriffen für das Krankenhaus als Ganzes verstehen und einen umfassenden Sicherheitsplan erstellen, der auch die entsprechende Schulung der Mitarbeiter zur sicheren Datenübertragung umfasst“.

Vor diesem Hintergrund, da ist sich Pykälistö sicher, ist das Gesundheitswesen ein Gebiet auf dem Sectra Communications künftig noch sehr viel aktiver sein wird.

Simo Pykälistö

ist seit 2016 President Sectra Communication AB, der Geschäftsbereich für sichere Kommunikation, der sich auf IT-Sicherheit und Verschlüsselung spezialisiert hat.

Der in Finnland geborene Sicherheitsexperte absolvierte seine Ausbildung im Finanzwesen in den USA, bevor er nach Schweden zog. Pykälistö ist seit 2003 für Sectra tätig und bringt seine Erfahrung aus der Arbeit für den finnischen Sicherheitsberater EXP Analytics Oy in das Unternehmen ein.

Sectra Medical Systems GmbH • info.de@sectra.com • sectra.com/dach

SECTRA
Knowledge and passion