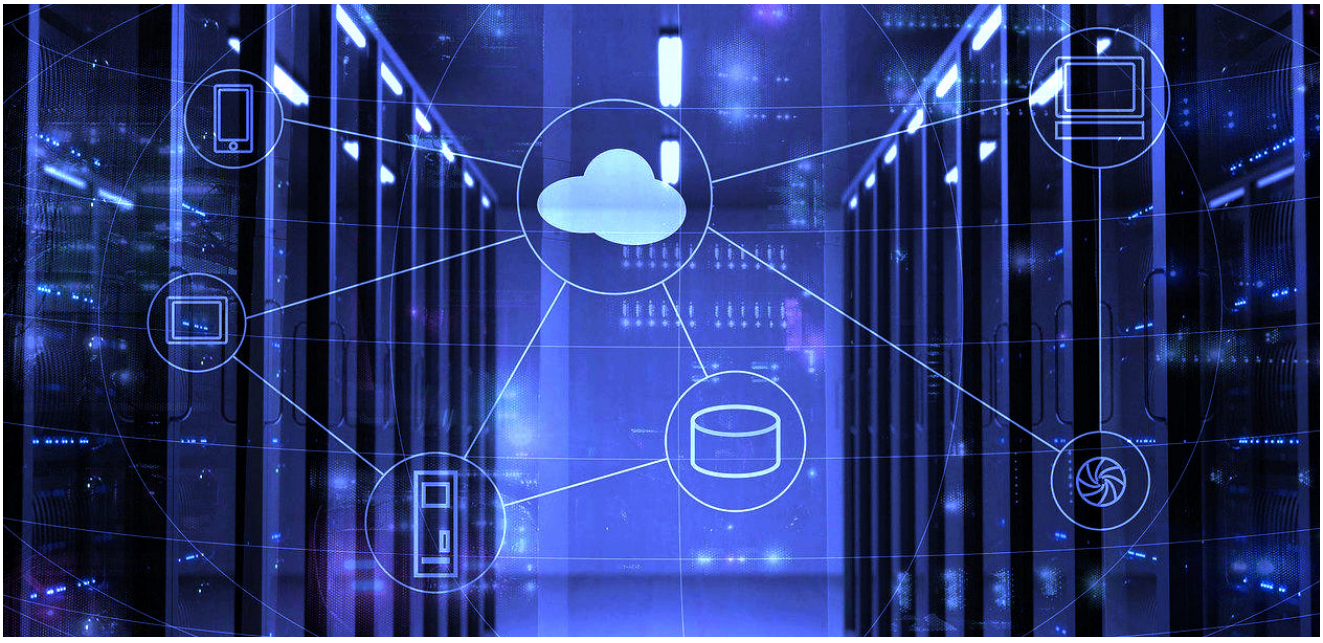
Vernetzt? Aber sicher!

Moderne Netzwerklösungen für die Klinik

Ohne den Austausch elektronischer Daten läuft heute nichts mehr in der Medizin. Performance und Sicherheit bilden die wichtigsten Voraussetzungen, um einen reibungslosen Netzwerkverkehr zu gewährleisten. Doch gerade an der Sicherheit hapert es in vielen Krankenhäusern, weil dieser Aspekt einer kontinuierlichen Anpassung an ständig neue Gefahren bedarf. Welche kurz- und langfristigen Lösungen es gibt, um eine moderne IT-Infrastruktur im Krankenhaus aufzubauen, weiß Alexander Fücker, Sales Support & Solution Architect bei Sectra Medical Systems. Dabei macht er deutlich: "Einfache Sicherheit gibt es nicht."



Wie bereits eine kleine Schwachstelle zum größtmöglichen Schaden führen kann, zeigt der aktuelle Fall einer großen Klinik in Nordrhein-Westfalen. Unbekannte Hacker hatten ein Schadprogramm in das IT-System eingeschleust und den Krankenhausbetrieb im September 2020 über mehrere Tage hinweg lahmgelegt. Der Zugriff auf gespeicherte Daten war nicht mehr möglich. Angriffspunkt für die Cyberkriminellen bot eine kommerzielle Zusatzsoftware.

Auch Sectra war in das Geschehen involviert, da das Unternehmen das PACS für die Radiologie der Klinik bereitstellt. "Unsere Mitarbeiter waren schnellstmöglich vor Ort und rund um die Uhr im Einsatz. Das Wichtigste war, zunächst einmal ein Notsystem zum Laufen zu bringen, damit die Radiologen überhaupt ihre Arbeit weiterführen konnten," berichtet Fücker. "Danach musste alles komplett neu eingerichtet werden, weil man nie genau weiß, ob sich der Virus doch noch irgendwo in der alten Hard- oder Software versteckt. Glücklicherweise konnten die verloren gegangenen Daten aber wiederhergestellt werden, da es ein Offline-Backup gab."

Mikrosegmentierung: Geschlossene Gesellschaft

Damit es gar nicht erst zum Totalausfall kommen kann, empfiehlt der IT-Spezialist verschiedene Bereiche des Netzwerks voneinander zu separieren. Der Datenzug-

SECTRA

Knowledge and passion

riff und -transfer von einem Bereich in einen anderen erfolgt dann nur über ein Firewall-Sicherungssystem. Dadurch wird verhindert, dass ein Angreifer, der es geschafft hat, den Schutzmechanismus eines Netzwerks zu durchbrechen auch in alle anderen vordringen kann. Die Umsetzung dieser Technologie ist allerdings in der Praxis nicht ganz einfach. Denn die meisten Klinik-Netzwerke sind historisch gewachsen und nicht auf solch eine Mikrosegmentierung ausgelegt.
Ein weiteres Problem stellen die hohen Kosten und der administrative Aufwand dar. Denn jedes Teilnetz muss einzeln, bis herunter auf die Anwendungs- und Benutzerebene, gepflegt und gehegt werden. "Die Planung, Umsetzung und Betreuung eines segmentierten Netzwerkes ist nichts, was man nebenher betreiben kann", sagt Fücker. "Man muss ständig am Ball bleiben, um die Netzwerk- und Sicherheitsanpassungen auf dem neuesten Stand zu halten. Dafür braucht es gut geschultes Personal, das vielerorts einfach nicht zur Verfügung steht. Eine mögliche Lösung wäre, erst einmal mit den weitest verbreiteten Systemen wie dem KIS oder PACS anzufangen. Darauf aufbauend können nach und nach weitere Sicherheitszonen eingeführt werden, die essentiell erscheinen."

Verantwortungsvolle Mitarbeit

Es gibt aber noch weitere simple Schritte, mit denen sich die Netzwerksicherheit erhöhen lässt. Zum einen, das Personal für das Thema zu sensibilisieren und zum anderen, den Zugriff auf das Internet so weit wie möglich zu beschränken. Dies kann beispielsweise über Positivlisten oder Negativlisten geschehen, in denen genau geregelt ist, welche Webseiten und -dienste aufgerufen werden dürfen und welche nicht. Alexander Fücker gibt allerdings auch zu bedenken, dass sich viele Mitarbeiter durch solche Maßnahmen gegängelt fühlen: "Besser ist es, den Mitarbeitern klar zu machen, welchen Dienst sie den Patienten und dem Krankenhaus erweisen, wenn sie verantwortungsvoll handeln und das Internet wirklich nur dienstlich nutzen."

Angriffsfläche klein halten

Eine weitere Möglichkeit besteht darin, dem Personal ein separates Netzwerk zur Internetnutzung zur Verfügung zu stellen. Dann ist die Versuchung, private Inhalte auf dem Stations-PC statt auf dem eigenen Smartphone zu konsumieren, gar nicht erst gegeben. Im besten Fall erfolgt der Zugriff über eine separate Verkabelung, damit jegliche Verbindung zum Kliniknetzwerk ausgeschlossen ist.

Des Weiteren rät Fücker zu Terminallösungen, die zentral über ein Netzwerk verwaltet werden. An den Rechner-Arbeitsplätzen wird dann lediglich die Benutzeroberfläche der Anwendungen angezeigt. Das hat einerseits den Vorteil, dass Softwareaktualisierungen nur noch von einem einzigen Punkt aus durchgeführt werden müssen und andererseits externe Geräte wie USB-Sticks nicht angeschlossen werden können. Die Angriffsfläche für Malware und Viren wird dadurch erheblich reduziert.

Hundertprozentigen Schutz gibt es aber nicht. Deshalb müssen auch Krankenhäuser stets ein wachsames Auge auf die aktuellen Entwicklungen haben. Oder wie Alexander Fücker es ausdrückt: "Sicherheit ist Aufwand. Doch man sollte bedenken, dass es einen noch viel höheren Aufwand (und finanzielle Mittel) nach sich zieht, die Folgen eines Großangriffs zu beheben."

Alexander Fücker

Alexander Fücker ist Sales Support & Solution Architect bei Sectra Medical Systems. Er ist Spezialist für DICOM und HL7 und konnte seine Expertise in diesen Bereichen bereits bei mehreren IT-Firmen als Product Support Engineer unter Beweis stellen. Er wechselte im Februar 2018 wieder zu Sectra, nachdem er hier bereits von 2004 bis 2009 als Technical Team Manager tätig war.

SECTRA
Knowledge and passion