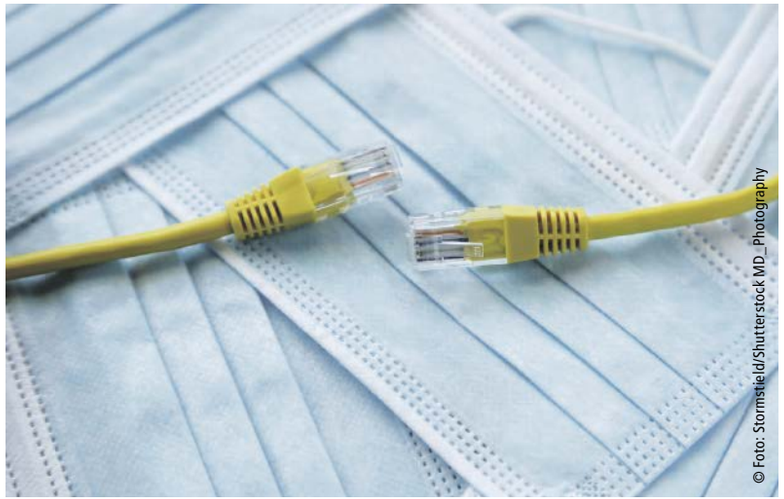
Cybersicherheit: Krankenhäuser mehr denn je an der Frontlinie

Obwohl der Gesundheitssektor nachweislich ein vorrangiges Ziel für Hacker ist, hinkt diese Branche weit hinterher bei Wahrnehmung und Eindämmung von Cyberrisiken.

Neue im Gesundheitswesen eingesetzte Technologien wie Telemedizin, Terminbuchungsplattformen und Chatbots sind vernetzte und oft in der Cloud angesiedelte Anwendungen, die an verschiedenen Stellen in die Informationssysteme einfließen, wodurch deren Angriffsfläche ausgedehnt wird. Eine Entwicklung, die mit einem weiteren technischen Durchbruch Hand in Hand geht: die Vernetzung medizinischer Geräte, von der Insulinpumpe bis hin zum Defibrillator. Die Kehrseite dieses überaus willkommenen technischen Fortschritts im Krankenhaus ist allerdings die Tatsache, dass die Barriere zwischen dem administrativen Informationssystem und der Betriebsumgebung eines Krankenhauses angesichts der Heterogenität der vernetzten Geräte und der eingesetzten Anwendungen immer dünner und die Durchlässigkeit der verschiedenen Netzwerke zur gefährlichen Schwachstelle für die gesamte Infrastruktur wird.

Unzureichende Segmentierung der Netze mit unterschiedlichem Grad an Vertraulichkeit oder Kritikalität, mangelnde Berücksichtigung der OT-Umgebungen eines Krankenhauses bei der Implementierung von Sicherheitsmaßnahmen, dürftiger Schutz der zunehmend digitalen Patientenakten sind oft die Folge, mit gravierenden Auswirkungen, auch auf Menschenleben. Wenn man dazu noch die immer größere



© Foto: Stormshield/Shutterstock MD_Photography

Offenheit der Gesundheitsinformationssysteme gegenüber externen Organisationen oder anderweitigen medizinischen Einrichtungen hinzufügt, wird die Bedrohung, die auf dem Gebiet lastet, systemisch. Und es war noch gar nicht die Rede von Datendiebstahl und -lecks oder der Wahrung der Integrität von Gesundheitsdaten während der Verarbeitungs-, Speicher- und Austauschphase. Ein Thema für sich, denn laut dem europäischen Cybersecurity-Hersteller Stormshield sind Ransomware und Health-Data-Mining die häufigsten und für Cyberkriminelle lukrativsten Attacken gegen Krankenhäuser.

Höchste Zeit für eine Steigerung der Cyberresilienz

Wie viele von Cyberkriminellen ausbeutbare Einfallstore Krankenhäuser aufweisen, ist weitestgehend bekannt. Umso komplizierter deshalb die Gewährleistung der Cyberresilienz, denn besonders in dieser Branche darf man nicht nur wissen, ob man gerade angegriffen wird, sondern man muss Angriffe antizipieren können. Das erfordert in erster Linie ausreichendes interdisziplinäres (IT/OT-)Fachwissen, um Signale oder Vorläufer eines Cyberangriffs zu identifizieren. Die genaue Festlegung und Implementierung technischer und organisatorischer Sicherheitsmaßnahmen zur Eindämmung und Ausmerzung von Bedrohungen gehört im zweiten Schritt ebenfalls dazu, wie die tief greifende Analyse jedes Vorfalls, um die Sicherheit weiter zu verbessern.

Hier bietet der Hersteller mit seinen Lösungen zum Schutz von IT- und OT-Netzwerken (Stormshield Network Security), Workstations (Stormshield Endpoint Security) und Daten (Stormshield Data Security) Werkzeuge an, die darauf ausgerichtet sind, das Sicherheitsniveau kritischer Infrastrukturen zu erhöhen, mit dem Ziel, die für den Betrieb eines Krankenhauses lebenswichtige Ausrüstung (IT/OT) in Echtzeit selbst vor unbekannten Bedrohungen zu schützen, ein gutes Maß an Operativität während eines Cyberangriffs zu gewährleisten und eine rasche Rückkehr zur Normalität zu ermöglichen.

Stormshield
E-Mail: dach@stormshield.eu
www.stormshield.com/de/loesungen/