Medizintechnik:
Per Retrofit in die sichere Digitalisierung

Einer der weltweit größten Hersteller für diagnostische Ultraschallgeräte und Kernspintomographen setzt schon seit vielen Jahren auf Fernwartung. Damit der digitale Zugang keine Angriffsfläche für Cyberattacken bietet, schützt das Unternehmen seine sensible Medizintechnik mit der Endian 4i Edge Software. Dadurch gelang es, die bereits vorhandenen Gateways mit Hochfrequenzschutz zu einer leistungsstarken Security-Appliance aufzurüsten.

„Medizintechnik wurde lange Zeit für den Einsatz in geschlossenen Systemen konzipiert. Durch die Digitalisierung und die damit einhergehende Verbindung zum Internet, werden diese Geräte zur potentiellen Zielscheibe für Cyberangriffe", erklärt Endian CEO Raphael Vallazza. „Die ENDIAN SECURE DIGITAL PLATFORM bietet die Möglichkeit, Medizintechnik durch einen schnellen und einfachen Retrofit zu vernetzen und abzusichern, ohne dass nachträgliche Zulassungsverfahren notwendig werden."

Medizintechnik: Sonderfall bei der Digitalisierung

Das Vorschalten eines IoT-Security-Gateways vor ein medizintechnisches Gerät ist in der Regel eine gute Lösung, um bestehende Medizintechnik mit allen notwendigen Konnektivitäts- und Sicherheitskomponenten für eine sichere Digitalisierung nachzurüsten. Bei Kernspintomographen und Ultraschallgeräten ist der Einsatz von IoT-Security-Gateways allerdings nicht unproblematisch, denn bei diesen Geräten entstehen im Einsatz hochfrequente Strahlungen, die den Betrieb der IoT-Security-Gateways stören können. Für die Einrichtung der Konnektivität in der typisch heterogenen IT-Umgebung eines Krankenhauses nutzte der Medizintechnikhersteller

"Medizintechnik wurde lange Zeit für den Einsatz in geschlossenen Systemen konzipiert. Durch die Digitalisierung und die damit einhergehende Verbindung zum Internet, werden diese Geräte zur potentiellen Zielscheibe für Cyberangriffe."

Raphael Vallazza,
Endian CEO

Das **Endian Switchboard** ist das Herzstück der ENDIAN SECURE DIGITAL PLATFORM. Als zentrales Steuerungselement ermöglicht es einen sicheren Fernzugriff auf die Geräte vor Ort, Datenerfassung, Edge Computing und ein leistungsstarkes Management von Benutzer- und Gerätebe-rechtigungen.

deshalb spezielle Gateways des Produzenten SECO, die gegen die Hochfrequenzen geschützt sind und allen medizinischen Regularien entsprechen.

IoT-Security Gateway Software für umfassende IT-Sicherheit

Um diese Gateways weiterhin einsetzen zu können entschied sich der Hersteller für eine einzigartige Lösung von Endian. Der Südtiroler Hersteller bietet eine integrierte Cybersecurity-Plattform, die die digitale Welt (IT) und die physische Welt (OT) miteinander verbindet. Für die Anbindung physischer Geräte kommen die Endian 4i Edge Gateways zum Einsatz und davon gibt es auch eine Software Variante, das sogenannte Endian 4i Edge Software..

Das Endian 4i Edge Software verwandelt jeden Industrie-PC und jedes IoT-Gateway (x86 oder ARM-Technologie) in Endians leistungsstarke Lösung für Konnektivität und Cybersecurity, um medizinische Geräte abzusichern. Mehrere, fein aufeinander abgestimmte Sicherheitsfunktionen sorgen dann für einen umfassenden Schutz: Deep Packet Inspection (DPI) analysiert die Datenpakete, die über das Netzwerk verschickt werden. Im Gegensatz zu normalen Analysemethoden, die sich rein auf die Metadaten beschränken, geht DPI bis in die Anwenderebene und ist in der Lage, über 300 IT- und OT-Protokolle zu erkennen, ebenso wie 2.000 Applikationen. Ein Virtual Private Network (VPN) sorgt für einen sicheren Fernzugriff, indem es die Daten bei der Übertragung verschlüsselt, so dass sie weder ausgelesen noch manipuliert werden können. Sollte ein Angreifer die Firewall überwunden haben, erkennt das Intrusion Detection System (IDS) den Angriff und das Intrusion Prevention System (IPS) kann ihn unterbinden.

Mehr Sicherheit durch granulares Rechtemanagement

Eine granulare Verwaltung von Zugriffsrechten stellt ein zusätzliches Sicherheitslevel dar. Das Endian Switchboard, als zentrales Management-Tool der ENDIAN SECURE DIGITAL PLATFORM, bietet die Möglichkeit, Nutzer oder Nutzergruppen mit unterschiedlichen Rechten auszustatten. So lässt sich beispielsweise festlegen, wer auf welche Geräte zugreifen darf, welche Aktionen dort ausgeführt werden dürfen und welche Daten einsehbar sind. Jeder Zugriff wird dabei dokumentiert, so dass jederzeit transparent ist, wer wann auf welchem Gerät war und welche Maßnahmen dort durchgeführt wurden.

Aktuellster Schutz trotz veraltetem Betriebssystem

Über das Endian Switchboard lassen sich zudem die neuesten Sicherheitsupdates auf alle IoT-Gateways aufspielen. Das war für den Medizintechnikhersteller besonders wichtig, denn die Ultraschallgeräte und Kernspintomographen, für die ein Fernzugang hergestellt werden sollte, basierten auf dem Betriebssystem Windows XP. Da Microsoft die Updates für dieses Betriebssystem bereits 2014 eingestellt hat, ist sein Einsatz aus Perspektive der IT-Sicherheit heute zu riskant. „In der Industrie und auch in der Medizintechnik sind Maschinen oft zehn Jahre oder länger in Betrieb", erklärt Raphael Vallazza. „Damit ist es durchaus üblich, medizintechnische Geräte mit älteren Betriebssystemen noch im Einsatz zu sehen. Indem die Gateways über das Switchboard aktualisiert werden, sind alle Geräte geschützt. Auch im Hinblick auf die NIS2-Richtline, die bis Ende 2024 in nationales Recht überführt wird, ist das ein zentraler Aspekt."

Endian 4i Edge Software: Sie verwandelt jedes IoT-Gateway (x86) oder Industrie-PC in ein Endian 4i Edge Gateway. Dabei handelt es sich um eine leistungsstarke Cybersecurity-Lösung für die Industrie, die auf dem gehärteten Betriebssystem EndianOS basiert. Sie bietet die Möglichkeit, industrielle Anlagen, wie SPS, HMI, RTU und andere SCADA-Systeme abzusichern und zu verbinden.

Keine Gefahr durch mobile Datenträger

Die Ultraschallgeräte und Kernspintomographen waren noch einem weiteren IT-Sicherheitsrisiko ausgesetzt: Ärzte und Krankenhauspersonal nutzen regelmäßig USB-Sticks, um Aufnahmen der Untersuchungen zu speichern. Über diese externen Speichermedien kann jedoch auch Schadsoftware auf die Maschinen gelangen und sich sogar über das Netzwerk ausbreiten, wenn die Geräte mit der IT vernetzt sind.

Um dem entgegenzuwirken wurde festgelegt, dass die USB-Sticks nicht mehr direkt am Ultraschallgerät oder Kernspin eingesteckt werden sollten, sondern im IoT-Gateway, das auch über den erforderlichen USB-Port verfügt. Damit die Geräte vor Schadsoftware geschützt sind, wurde eine Anti-Virensoftware auf dem IoT-Gateway installiert. Sobald ein USB-Stick zum Einsatz kommt, wird das Medium erst mal auf mögliche Viren oder Trojaner überprüft und schädliche Programme blockiert.

Dass sich alle Bestandsanlagen per Retrofit so schnell und sicher vernetzen ließen, ohne neue Hardware anschaffen zu müssen, hat den Hersteller der diagnostischen Ultraschallgeräte und Kernspintomographen überzeugt. Alle Geräte der neueren Generation werden zukünftig mit der ENDIAN SECURE DIGITAL PLATFORM ausgeliefert.

Endian SRL

Hypatiastraße 2
I-39100 Bozen (BZ) Italy

Tel: +39 0471 631 763
E-mail: info@endian.com