Inventar, Management und Sicherheit für vernetzte medizinische Geräte

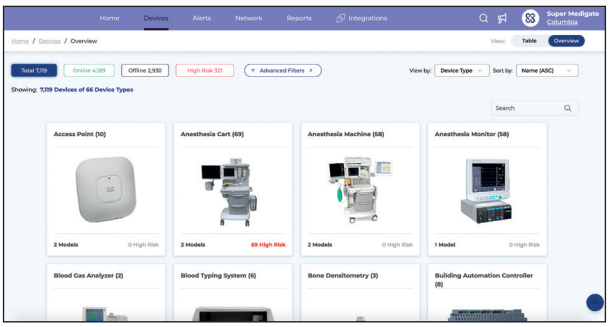
Viele Healthcare-Organisationen verfügen nicht über ein komplettes Inventar der vernetzten medizinischen Geräte – ein Risiko für die Sicherheit und ein Hindernis für eine ganzheitliche Verwaltung. Die Lösung von Medigate identifiziert alle IoMT-Devices, stellt anomale Vorgänge fest und liefert verwertbare Erkenntnisse für das Management.

Medizinische Geräte vom Perfusor über den Patientenmonitor bis zum MRT sind heutzutage immer öfter vernetzt – sei es, um ihre Funktion zu überwachen oder die gewonnenen Daten zentral zu analysieren. Eine Studie von Frontier Communications postuliert denn auch, dass schon 2020 gegen 40 Prozent der gesamten IoT-Technologie auf das Gesundheitswesen entfallen. Und 60 Prozent der Healthcare-Institutionen nutzen demnach bereits die Möglichkeiten von IoT – oder besser gesagt IoMT: Internet of Medical Things.

Dem gegenüber steht die Tatsache, dass in vielen Spitälern die komplette Übersicht über das Inventar der klinischen IoT-Geräte fehlt, ganz zu schweigen vom Wissen über deren Standorte, Nutzung und technische Verwundbarkeiten. Das sind schlechte Voraussetzungen für ein ganzheitliches Management und für die Sicherheit der Medizintechnik. Denn Hacker haben es zunehmend auf die Netzwerke des Gesundheitswesens abgesehen. Immer wieder geraten Kliniken in die Fänge von Ransomware-Erpressern, wobei auch IoMT-Geräte eine empfindliche Schwachstelle bilden. Ein weiterer Grund für die Attraktivität von Healthcare-Organisationen für Cyberkriminelle: Patientendaten gehören zu den gefragtesten Datendiebesgütern – man spricht von «Patient Health Information (PHI) Theft».

Das junge, auf IoMT spezialisierte Unternehmen Medigate bringt mit seiner Lösung Licht ins Dunkel der vorhandenen Healthcare-Technologie. Medigate liefert ein komplettes Inventar aller vernetzten Geräte, identifiziert anomale Vorgänge, hilft bei der Durchsetzung von Sicherheitsrichtlinien und liefert wertvolle Erkenntnisse für das Management der Medizintechnik – bis hin zum Nutzungsgrad etwa von Computertomografen, was wiederum als Basis für Beschaffungsentscheide dienen kann.

Technisch funktioniert die Medigate-Plattform wie folgt: Eine Sensor-Appliance untersucht den Netzwerkverkehr, im Allgemeinen über gespiegelte Switch-Ports, filtert die für IoMT relevanten Informationen aus dem Datenstrom und leitet sie zur Analyse an die Medigate-Cloud oder optional an einen Analyse-Server vor Ort weiter. Dabei kommt das enorme Know-how von Medigate über die Details medizinischer Geräte bis hin zu proprietären Protokollen und Firmware-Versionen zum Einsatz. Die so gewonnenen Erkenntnisse liefert die Lösung auf einer übersichtlichen Web-Konsole in Text und Grafik an die Anwender aus.



Medigate ermöglicht automatisiert eine stringente Sicherheitsstrategie für den oft schlecht geschützten und nur selten mit Updates versorgten medizintechnischen Gerätepark.

So ist auf einen Blick zu erkennen, wie viele Geräte insgesamt erkannt wurden und wie viele im Moment online sind. Per Drill-Down kommt man zu detaillierten Informationen über jedes einzelne Gerät. Die Konsole präsentiert darüber hinaus Informationen zu allfälligen Schwachstellen der Devices sowie weitere Informationen wie den genauen Gerätetyp, die installierte Software-Version, die Betriebsdauer, den Standort, die Aktivitäten und die Auslastung des jeweiligen Geräts. Medigate informiert zudem nicht nur über die Herkunft des medizinischen Datenverkehrs, sondern auch über dessen Ziel und warnt bei Anomalien. So lässt sich unmittelbar erkennen, wenn zum Beispiel Patientendaten auf einen nicht dafür zugelassenen Speicher abgelegt werden.

Medigate ist als offene Plattform konzipiert, die sich auf die vorhandenen medizinischen Geräte versteht und mit Cybersecurity-Lösungen und Directories zusammenarbeitet. So bietet die Plattform enge Integration mit den Firewalls verschiedener Hersteller wie Palo Alto Networks, Check Point oder Fortinet, mit Network-Access-Control-Plattformen, Vulnerability-Management- und SIEM-Lösungen. Und die Einbindung von Directory-Services wie AD oder LDAP ermöglicht, den Datenverkehr bis auf die Ebene des angemeldeten Nutzers zu analysieren.

Medigate: die Highlights

- Erstellt komplettes, exaktes Inventar aller medizinischen Geräte
- Erkennt Anomalien in der Gerätenutzung und im Datenverkehr
- Unterstützt die Durchsetzung der Sicherheitsrichtlinien
- Verhindert zusammen mit Firewall-Lösungen illegitimen Datenabfluss
- Liefert direkt verwertbare Erkenntnisse über Auslastung der Geräte und weitere Management-Informationen

BOLL Engineering AG
Jurastrasse 58, 5430 Wettingen
Tel. 056 437 60 60
info@boll.ch, www.boll.ch