ADVERTORIAL

Cybersicherheitsmanagement für medizinische Geräte und IoT

Die klinisch validierte Asimily Insight Platform kombiniert die Bestandsaufnahme aller IoMT- und IoT-Geräte mit effizientem Schwachstellenmanagement samt gerätespezifischer Priorisierung und Behebung der Risiken.

ASIMILY: DIE HIGHLIGHTS

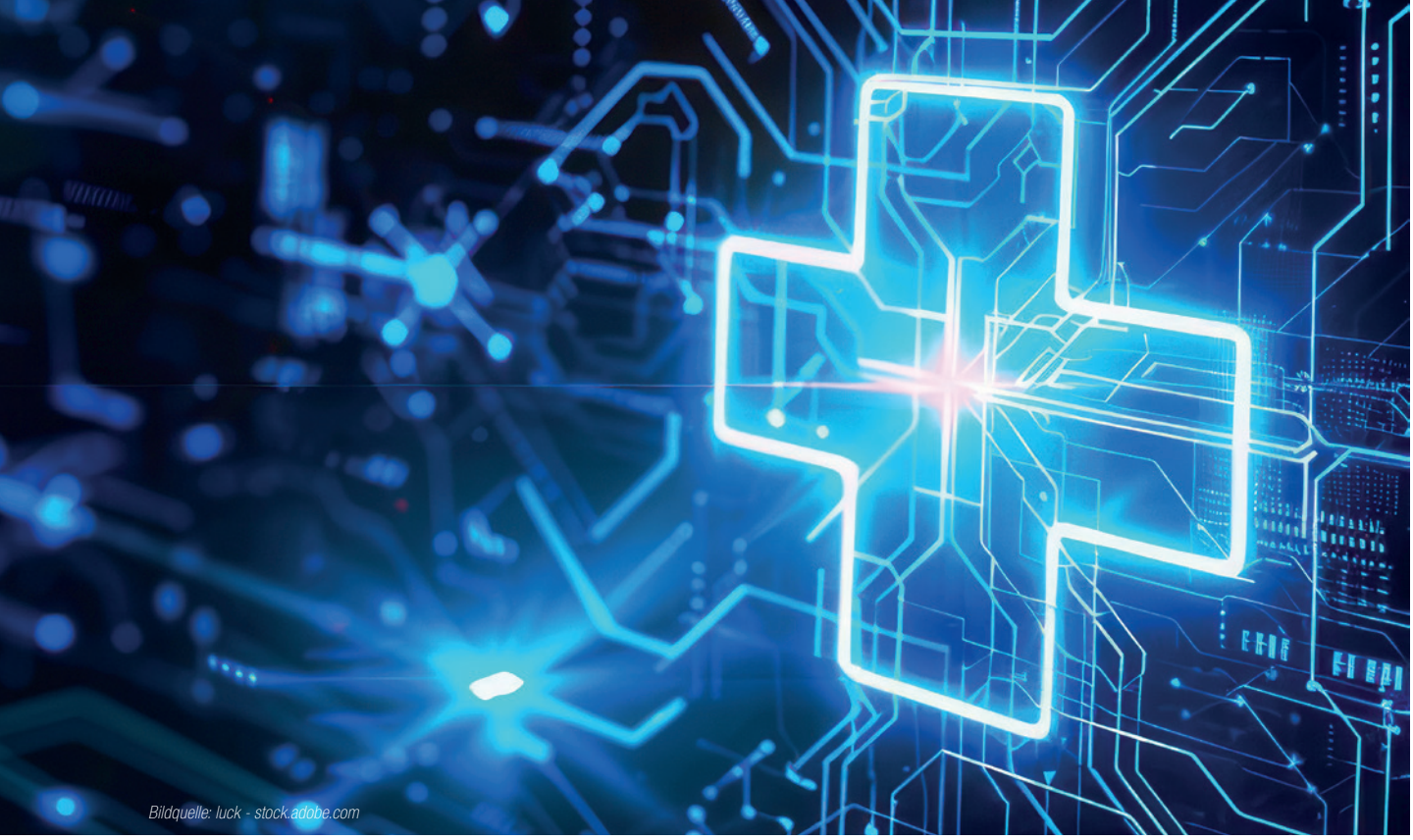
- Umfassende Plattform für IoT-/IoMT-Cybersicherheitsmanagement
- Unterstützt Bestandsaufnahme, Risikominderung, Reaktion auf Vorfälle und Geräteverfügbarkeit
- Identifiziert und priorisiert das Risiko jedes Geräts anhand spezifischer Datenquellen und Gerätekonfigurationen
- Bietet bei Schwachstellen automatisierte Behebung via «Fix»-Button
- Arbeitet mit Schwachstellenscannern wie Tenable und NAC-Systemen wie Palo Alto und Fortinet zusammen
- Als On-Premises-Lösung oder via Cloud einsetzbar
- Agentenlos, das heisst, es ist keine Software-Installation auf den Geräten erforderlich

Kein Krankenhaus kommt ohne vernetzte medizinische Geräte aus, vom Patientenmonitor bis zum MRI-System. Vergleichbares gilt für industrielle Umgebungen, kritische Infrastrukturen und das Transportwesen. Sie alle setzen für die Überwachung und Steuerung mehr und mehr auf IoT-Geräte. Es liegt auf der Hand, dass gerade in diesen Branchen die Cybersicherheit einen besonders hohen Stellenwert einnehmen muss – und dies nicht nur für die IT-Systeme, sondern auch für medizinische Geräte (IoMT, Internet of Medical Things) sowie für IoT-Geräte generell.

IT-Vulnerability-Management genügt nicht

Die Nutzung von IoMT- und IoT-Geräten birgt Risiken, die nicht leicht zu bestimmen und zu beheben sind. So lassen sich die Geräte oft gar nicht patchen, oder die Hersteller liefern nur selten Aktualisierungen. Die daraus entstehenden gerätespezifischen Risiken können kritisch oder eher unbedeutend sein. So stellt sich die Frage, welche Risiken mit welcher Dringlichkeit eliminiert werden müssen. Erschwerend kommt hinzu, dass IoMT und IoT zum Grossteil mit spezifischen, oft proprietären Protokollen der jeweiligen Hersteller arbeiten, die in der IT nicht bekannt sind.

Gängige Vulnerability-Management-Lösungen für IT-Umgebungen helfen also nur bedingt. Sie kennen sich mit den Protokollen und Risiken im medizinischen und industriellen Bereich nicht aus und bieten damit keine rasche Möglichkeit, Schwachstellen in diesen Umfeldern nur schon zu erkennen und einzuordnen, geschweige denn



Bildquelle: luck - stock.adobe.com

schnell mit geringem Aufwand für das Personal zu beseitigen oder zu umgehen.

Asimily kann IoMT und IoT

Der US-Hersteller Asimily schliesst diese Lücke und bietet eine umfassende Cybersicherheits-management-Plattform für IoT- und medizinische Geräte an. Die Insight Platform von Asimily sammelt alle verfügbaren Geräteinformationen in Echtzeit und präsentiert die Erkenntnisse auf einem übersichtlichen Dashboard. Als Basis für die Identifizierung von Schwachstellen dient eine riesige Datenbank mit Geräteinformationen, MDS2-Angaben und SBOMs der Hersteller sowie Informationen aus der Anwender-Community.

Zusätzlich berücksichtigt Asimily die Art und die Konfiguration jedes Geräts. So stellen zum Beispiel Geräte, die mit geschützten Gesundheitsinformationen umgehen oder direkt Industrieanlagen steuern, ein massiv grösseres Risiko dar als viele andere. Die CVSS-Bewertung, die Vulnerability-Management-Lösungen generell verwenden, kennt solche Unterschiede nicht. Asimily hat mit seiner Datenbasis, die unter anderem über 1000 medizinische Geräte abdeckt, eindeutig die Nase vorn.

Und weil Asimily Sicherheitsprobleme, die mit hoher Wahrscheinlichkeit auftreten oder eine hohe Tragweite aufweisen, priorisiert behandelt, reduziert sich der Aufwand für die Behebung deutlich – Unwichtiges kann man links liegen lassen. In der Praxis lässt sich mit Asimily eine Reduktion des manuellen Aufwands für Vulnerability-Management-Analysten um bis zu 90 Prozent erreichen.

Die Lösung von Asimily erlaubt es überdies, viele Schwachstellen quasi auf Knopfdruck zu beheben – mit einem Klick auf den «Fix»-Button. Die Plattform arbeitet dafür mit NAC- und anderen Security-Systemen zusammen und kann so zum Beispiel risikobehaftete Ports schliessen, falls möglich Patches aufspielen oder eine (Mikro-) Segmentierung des fraglichen Geräts vornehmen.

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58 | 5430 Wettingen | 056 437 60 60
info@boll.ch | www.boll.ch