# Schwachstellenmanagement im klinischen Netzwerk

Medizintechnik und IT wachsen immer mehr zusammen. Vernetzte Medizingeräte müssen gemäss aktuellen rechtlichen Vorgaben genauso gegen Cyberrisiken geschützt werden wie IT-Systeme. Von Haus aus sind medizinische Geräte jedoch nicht auf Cybersicherheit ausgelegt – die Lösung sind Softwareplattformen wie Medigate und InsightVM.

Vernetzte medizinische Geräte vom Patientenmonitor bis zum Kernspintomografen sind aus dem klinischen Alltag nicht mehr wegzudenken. Wie bei allen mit einem Netzwerk verbundenen Geräten sollte auch bei solchen IoMT-Devices (Internet of Medical Things) auf höchstmögliche Sicherheit geachtet und im Fall von Sicherheitslücken rasch Abhilfe geschaffen werden. In der klassischen IT-Welt kommen dabei sogenannte Vulnerability-Management-Lösungen (VM) ins Spiel. Diese Softwareplattformen scannen alle Geräte im Netzwerk aktiv auf Schwachstellen und bewerten deren Risiko. Durch Empfehlungen an die Administratoren oder durch automatisierte Remediationsprozesse tragen sie zur Stärkung der Sicherheit bei – dies in Kombination mit weiteren Lösungen wie Patch-Management-Systemen und Firewalls.

### Vulnerability-Scans belasten Geräte

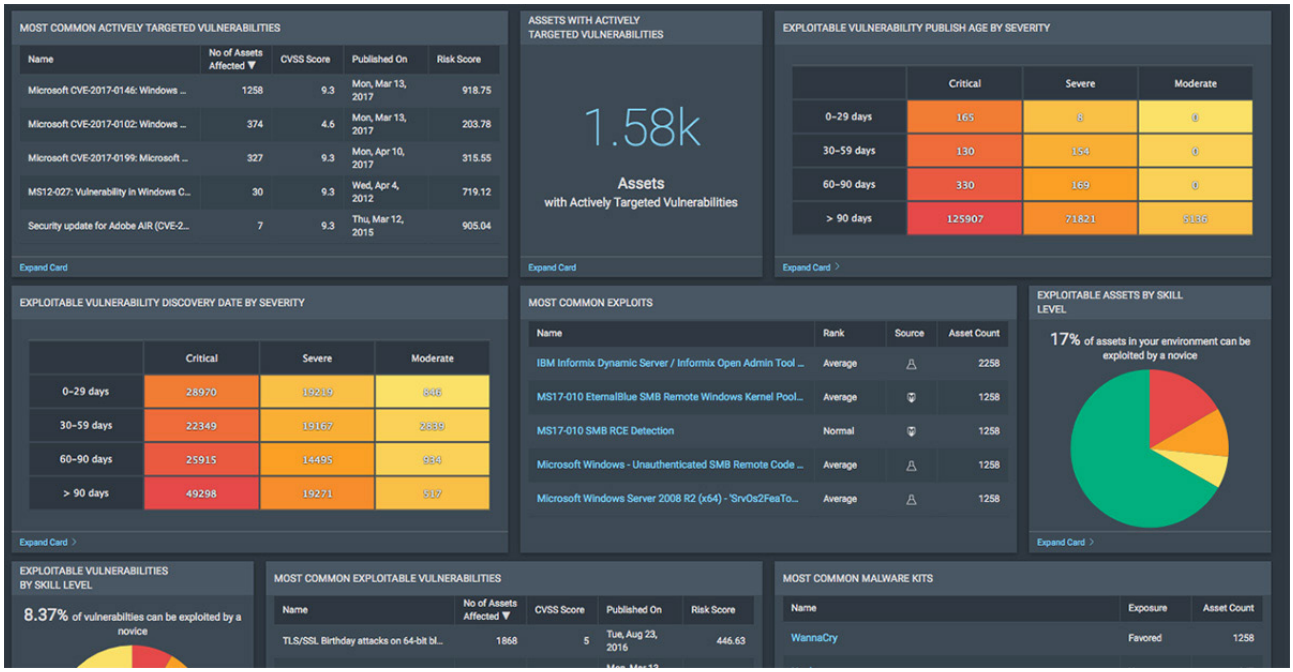
Das aktive Scanning auf Schwachstellen ist ein invasiver Prozess, der die Hardware der gescannten Geräte in unüblicher Weise belastet, zum Beispiel durch vielfache Login-Versuche oder durch gleichzeitige Kommunikation auf mehreren im Normalbetrieb nicht genutzten Ports. Andere Verfahren benötigen die Installation eines Agenten auf den Geräten. Dies ist jedoch bei IoMT-Devices meist nicht möglich: Der Hersteller erlaubt es nicht, oder das Gerät müsste nach dem Aufspielen des Agenten neu zertifiziert werden – ein aufwändiger und zeitraubender Prozess.

Healthcare-Organisationen sind bisher sehr skeptisch, was das Schwachstellenmanagement bei Medizingeräten betrifft. Manche Spitäler prüfen ihr medizinisches Equipment gar nicht erst auf Schwachstellen. Der Grund: Wenn ein aktiver Scan eine Funktionsstörung oder gar den Ausfall eines Geräts bewirkt, das gerade im Einsatz steht, ist die Patientensicherheit unmittelbar und ernsthaft gefährdet. Dass dies im klinischen Alltag nicht vorkommen darf, liegt auf der Hand. Dazu kommt, dass VM-Lösungen meist nicht auf IoMT ausgelegt sind, entsprechende Geräte nicht sauber identifizieren können und Schwachstellen von Medizingerätesystemen gar nicht erst kennen.

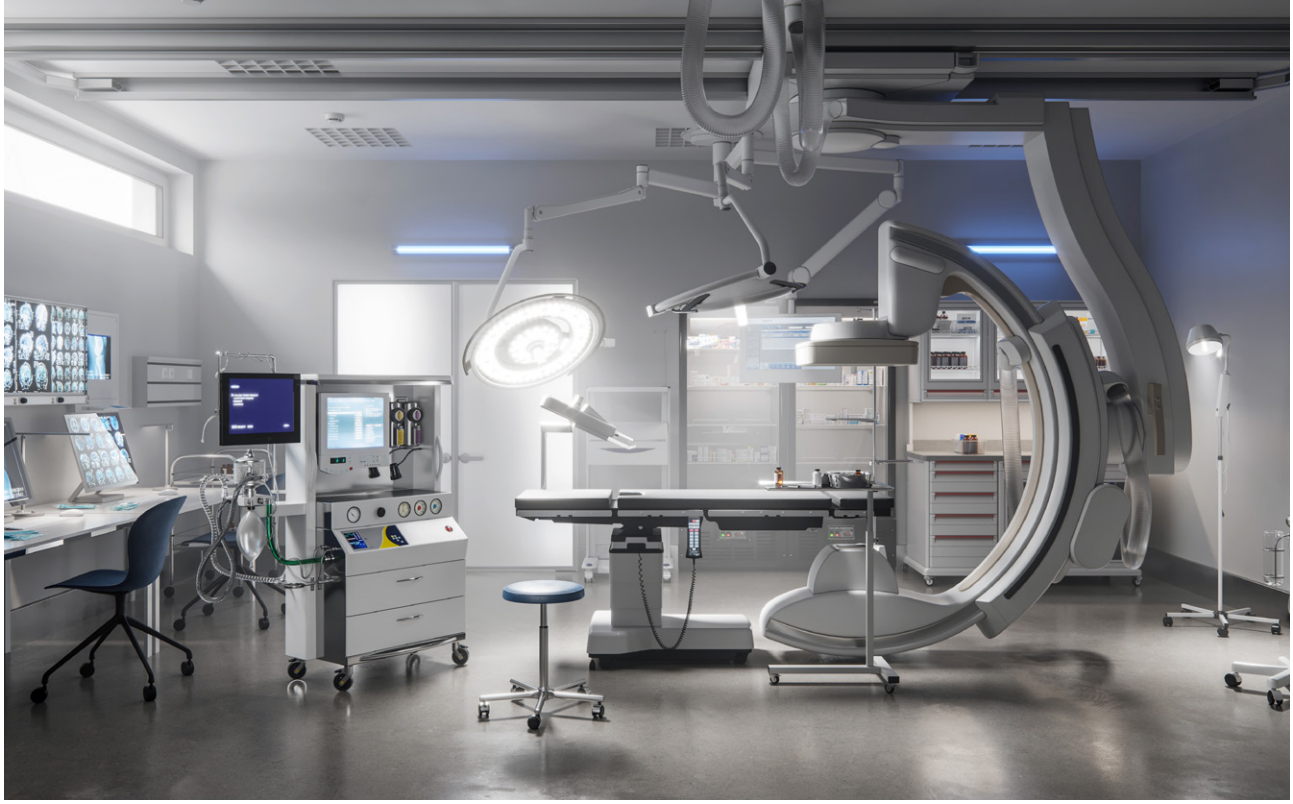
### Schwachstellenmanagement wird zum Muss

Dennoch können Spitäler heute nicht mehr auf Cybersicherheit im medizinischen Gerätepark verzichten. Dies nur schon aus gesetzlichen Gründen. So schreibt etwa das revidierte Schweizer Medizinprodukterecht seit dem 26. Mai 2021 vor, dass Spitäler im Rahmen eines Risikomanagements alle netzwerkfähigen Medizinprodukte durch geeignete Massnahmen vor Cyberrisiken schützen müssen (nMepV Art. 74). In Deutschland gelten vergleichbare Vorschriften, in Österreich sind entsprechende Gesetze in Vorbereitung.

Auch aus technischen Gründen ist es nötig, sich mit der Sicherheit von IoMT-Geräten zu beschäftigen. Dazu ist es aber zuerst notwendig, den aktuellen Status aller vernetzten Medizingeräte zu kennen. Denn erst wenn man die vollständige Visibilität besitzt, können Massnahmen für




***Schafft einen fundierten Überblick: Dashboard mit Risikobewertung.***



den Schutz der vernetzten Medizingeräte ergriffen werden. Diese Visibilität fehlt heute oft. Zwar werden die IoMT-Geräte üblicherweise in einer zentralen Software geführt, die Gerätedaten werden aber typischerweise manuell eingepflegt und einige Angaben wie Schwachstellen nicht erkannt beziehungsweise nicht festgehalten, wodurch die Aktualität leidet.

Gefragt ist somit eine Lösung, die zunächst ein komplettes Inventar aller vernetzten Geräte liefert, mit Angaben bis hin zu Details wie Gerätetyp, Modell, Firmware- und Applikationsversion, Seriennummer, Standort, Netzwerksegment, Auslastung und zuständiger Abteilung. Zweitens sollte die Lösung IoMT-Geräte ohne aktives Scanning überprüfen können. Drittens dürfen die klassischen Vulnerability-Management-Funktionen nicht fehlen. Und viertens soll die Lösung die Kommunikation der Geräte analysieren und bei Verdachtsmomenten und Anomalien Alarm auslösen.

**Inventar, Analyse und Risikobewertung für IoMT-Geräte**

Mit Medigate bietet der gleichnamige Hersteller eine auf IoMT spezialisierte Plattform an, die als Erstes automatisch ein komplettes Inventar aller vernetzten Geräte erstellt. Dabei kommt ein passives Verfahren zum Einsatz, das die Geräte nicht tangiert: Eine Sensor-Appliance untersucht den Netzwerkverkehr anhand gespiegelter Switch-Ports, filtert die IoMT-relevanten Informationen per Deep Packet Inspection aus dem Datenstrom und leitet sie zur Analyse. Dabei werden nur Gerätemetadaten und keine Patientendaten übertragen. Nachdem Medigate die Gerätedaten analysiert hat, werden diese durch die eigene Datenbank mit detaillierten Angaben angereichert. Medigate führt über 2 Millionen Geräte in seiner Datenbank, versteht über 100 proprietäre Medizintechnikprotokolle und kann so genaue Informationen über den vorhandenen Gerätepark liefern.

Medigate stellt die inventarisierten Geräte und damit verbundene bekannte Schwachstellen auf einer übersichtlichen Weboberfläche dar, die Einblicke bis ins Detail verschafft. Durch die Analyse des Netzwerkverkehrs ist die Plattform zudem in der Lage, Anomalien wie unerwünschte Verbindungen und Logins oder Kommunikation mit dem Internet in Echtzeit zu erkennen, Warnmeldungen auszugeben und in Zusammenarbeit mit anderen Sicherheitslösungen wie Firewalls gefährliche Kommunikation zu unterbinden. Die Lösung unterstützt damit auch die Definition und die Einhaltung von Sicherheitsregeln.

**Das erfolgreiche Duo: Medigate und InsightVM**

Über Integrationen arbeitet Medigate bidirektional mit anderen Plattformen zusammen. Besonders gelungen ist die Kombination mit der VM-Plattform InsightVM von Rapid7. Damit beim Vulnerability-Scan nur IT-Geräte aktiv durch Rapid7 gescannt werden, übermittelt Medigate die IoMT-Geräteangaben an InsightVM und teilt InsightVM so mit, welche Medizingeräte von den aktiven Scanaufträgen ausgeschlossen werden müssen. Darüber hinaus informiert Medigate InsightVM über IoMT-Schwachstellen (Clinical CVEs), die aus der Forschung von Medigate und von den Geräteherstellern her bekannt sind.

Umgekehrt bezieht Medigate von Rapid7 Schwachstelleninformationen zu allen erkannten Geräten (auch Nicht-IoMT). Medigate kann damit für jedes erkannte vernetzte Gerät einen Risikoscore berechnen, der auch allgemeine Verwundbarkeiten bezüglich Betriebssystem, Netzwerk-Connectivity, verschiedener technischer Eigenschaften und weiterer Parameter berücksichtigt, und diesen direkt in der eigenen Oberfläche präsentieren. Ein weiterer Vorteil der Integration ist, dass alle Schwachstellen in einem Dashboard sichtbar sind (entweder via Medigate oder via InsightVM) und somit zentral erfasst, beobachtet und bearbeitet werden können.

Kurz gesagt: Die bidirektionale Integration der detaillierten Gerätevisibilität von Medigate mit den Vulnerability-Scanning-Features von InsightVM schafft eine bisher unerreichte Fähigkeit, mit den Schwachstellen aller vernetzten Geräte (IoMT, IoT und IT) umzugehen, die Risiken im gesamten Spital zu bewerten und zu managen sowie je nach Priorität der Sicherheitsprobleme die passenden Massnahmen zu ergreifen.

BOLL
IT Security Distribution

**BOLL Engineering AG**

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60

info@boll.ch
www.boll.ch