BROSCHÜRE

Schutz von medizinischen Netzwerken und Geräten

Cybersicherheit für Einrichtungen des Gesundheitswesens

Digitalisierung und Vernetzung der Medizin stellen neue Herausforderungen dar

Mit der Digitalisierung im Gesundheitswesen und der Anbindung zahlreicher medizinischer Geräte an klinische Netzwerke ist die Angriffsoberfläche für Cyberattacken im Krankenhaus stark gewachsen. Organisationen im Gesundheitswesen verspüren einen starken Handlungsdruck, für Einblick in jede Geräteverbindung zu sorgen und wirksame Maßnahmen zu ergreifen, um den Betrieb und die Patientenversorgung vor den damit verbundenen potenziellen Risiken zu schützen. Denn diese Systeme sind für Angreifer ein äußerst attraktives Ziel. Die Angriffe drohen die Geräte in ihrer Funktionsweise zu stören und damit das Wohl und das Leben von Patienten zu gefährden. Weiter werden Patientenakten und Finanzdaten gestohlen, Lösegelder erpresst und das geistige Eigentum sowie der Ruf des Krankenhauses gefährdet. Nicht zuletzt drohen bei einem erfolgreichen Angriff auf ein Krankenhaus bedeutende Ertragsausfälle und Folgekosten.

Um ihre Informationen und Ressourcen zu schützen, müssen Gesundheitsorganisationen die Bedrohungen, die in Beziehung mit diesen IoMT-Geräten (Internet of Medical Things, IoMT) bestehen, identifizieren und wirksam eindämmen können. Medizinische Geräte sind in der Regel empfindlicher, verwenden unterschiedliche Protokolle und Betriebssysteme und können sogar mit einzelnen Patienten verbunden werden, was bedeutet, dass herkömmliche Erkennungs- und Abwehrmaßnahmen unwirksam oder störend wirken. Es erfordert einiges klinisches Fachwissen, um die verschiedenen Geräte zu identifizieren und ihre Rolle im klinischen Arbeitsablauf zu verstehen und sichere Zugriffsrichtlinien und Abhilfemaßnahmen festzulegen. Hinzu kommt die Tatsache, dass die Budgets für IT-Sicherheit einem bedeutenden Spardruck ausgesetzt sind. Deshalb wird der Gefahr, die von den medizinischen Geräten für die Sicherheit ausgeht, vielerorts nicht mit den notwendigen Mitteln entgegengetreten.

Herausforderungen auf einen Blick

- Die Anzahl der medizinischen Endgeräte nimmt zu und damit vergrößert sich die Angriffsfläche
- Hochsensible Daten im Gesundheitswesen sind für Angreifer besonders lukrativ
- Medizinische IoT-Geräte haben spezifische Eigenschaften
- Fundiertes Know-how für klinische Netzwerke ist gefragt
- Strenge Zugriffsrichtlinien sowie Richtlinien für Datenaustausch

Fortinet und Medigate helfen beim Schutz von IoMT-Geräten

Als Fortinet Fabric-Ready Partner ist die Medigate-Lösung in verschiedene Fortinet-Lösungen integrierbar und wird damit zum Bestandteil der Fortinet Security Fabric. Die daraus resultierende Partnerschaft zwischen Medigate und Fortinet bringt das klinische und Cybersicherheits-Fachwissen zusammen, das Gesundheitsorganisationen benötigen, um Sicherheitsrisiken und Ereignisse, die IoMT-Geräte in ihr Netzwerk einbringen, effektiv zu verstehen, zu verwalten und zu verhindern.

Medigate und Fortinet liefern somit eine hochmoderne IoMT-Security-Lösung, die sich mit den Sicherheitsrisiken befasst, denen die angeschlossenen Geräte im klinischen Netzwerk ausgesetzt sind. Die Medigate Device Security and Asset Management Plattform lässt sich z.B. in die Fortinet Next Generation Firewall FortiGate und die Netzwerkzungangskontrolllösung FortiNAC integrieren. Dadurch wird Krankenhäusern das fundierte klinische Fachwissen zur Verfügung gestellt, dass sie zur genauen Identifizierung und Analyse ihrer medizinischen IoMT-Geräte benötigen. Die Medigate-Plattform überwacht das Netzwerk kontinuierlich, um ein detailliertes Echtzeit-Inventar aller angeschlossenen Geräte zu erstellen. Die Plattform bildet auch die gesamte interne und externe Kommunikation dieser Geräte ab, um proaktiv verdächtige Aktivitäten zu erkennen, die von den erwarteten klinischen Arbeitsabläufen und dem beabsichtigten Herstellerverhalten abweichen. Medigate speist diese Informationen über die Fortinet Security-Fabric-Ready-APIs in FortiNAC ein, womit sich auch in einem nicht segmentierbaren flachen Layer-2-Netz die Zugriffe granular überwachen und kontrollieren lassen. Darüber hinaus bietet die Integration in FortiGate die Möglichkeit eine Netzwerksegmentierung zu erstellen, sowie über Applikation Control, Whitelisting und zusätzlich über IDS/IPS-Signaturen Angriffe auf Schwachstellen zu erkennen und abzuwehren. Die gemeinschaftliche Lösung ermöglicht eine automatisierte Erstellung und präzise Durchsetzung der in klinischen Umgebungen benötigten Anforderungen, z.B. Absicherung personenbezogener Daten, mittels NAC- und Firewall-Richtlinien umzusetzen, sowie risikobehaftete Kommunikation und die Verbreitung von Angriffen zu verhindern.

Vorteile auf einen Blick

- Sofortige Maßnahmen gegen verdächtige Geräte ergreifen, um die Risiken zu minimieren
- Dynamisches Erstellen und Durchsetzen von Richtlinien zur Blockierung böswilliger Kommunikation in Echtzeit
- Mikrosegmentierung einrichten, um die Ausbreitung von Angriffen zu verhindern und die Sicherheitshaltung des Krankenhauses zu stärken
- Umfassenden Überblick und Verwaltungsmöglichkeiten über die angeschlossenen medizinischen Geräte erhalten

Kontakt:

Fortinet
Feldbergstraße 35 - D-60323 Frankfurt
Riedmühlestrasse 8 - CH-8305 Dietlikon
Wienerbergstraße 11, Twin Towers, Turm A / 9. OG A-100 Wien
www.fortinet.com/de

December 8, 2021 4:32 PM
Sheldon:Fortinet:2021-12-1372902-Cybersecurity-for-Healthcare:2021-12-CS_IOT_Medical_Partners_AU-A4-DE
1372902-0-0-DE