MAXIMALE SICHERHEIT FÜR IHR KRANKENHAUS

UNSERE BEWÄHRTE SVA SECURITY-METHODIK FÜR IHRE IoMT-UMGEBUNG



Das Internet of Medical Things (IoMT) wird für die Gesundheitsversorgung zunehmend wichtiger. Das heißt auch, dass die Anzahl vernetzter Geräte bei den Leistungserbringern wächst. Umgebungen umfassen bspw. die Hardware und Software, die zur Überwachung und Steuerung lebenswichtiger medizinischer Geräte und Prozesse verwendet werden. Von MRT- und CT-Scannern bis hin zu Infusionspumpen und Herzmonitoren – die Sicherheit dieser Systeme ist von höchster Bedeutung.

Hauptgründe für die Sicherung der IoMT-Umgebung:

1. **Schutz sensibler Patientendaten:** Medizingeräte sammeln und verarbeiten sensible Gesundheitsdaten. Ein Cyberangriff kann zu Datenschutzverletzungen führen, die die Privatsphäre der Patientinnen und Patienten sowie die Reputation des Krankenhauses gefährden.
2. **Sicherstellung der Patientenversorgung:** Viele Systeme müssen rund um die Uhr verfügbar sein, um eine kontinuierliche Patientenversorgung zu gewährleisten. Ein Angriff kann lebenswichtige Geräte außer Betrieb setzen und die Patientengesundheit gefährden.
3. **Veraltete Medizingeräte:** Viele medizinische Geräte laufen auf älteren Betriebssystemen, die anfällig für Sicherheitslücken sind. Diese Schwachstellen müssen identifiziert und behoben werden, um die Sicherheit zu gewährleisten.
4. **Netzwerksicherheit:** Medizingeräte sind oft mit dem Krankenhausnetzwerk verbunden. Ein kompromittiertes Gerät kann als Einstiegspunkt für Angreifer dienen, um auf andere Systeme zuzugreifen und größeren Schaden anzurichten.
5. **Regulatorische Anforderungen:** Krankenhäuser unterliegen strengen regulatorischen Anforderungen und Compliance-Vorschriften. Eine sichere IoMT-Umgebung hilft dabei, diese Vorschriften einzuhalten und hohe Geldstrafen zu vermeiden.

DARUM SVA

Mit branchenübergreifender Expertise und Herstellerunabhängigkeit entwickelt SVA integrierte Sicherheitslösungen, maßgeschneidert für Ihre IoMT-Umgebung. Durch die enge Zusammenarbeit zwischen den Bereichen Cyber Security, Healthcare und anderen SVA-Fachbereichen maximieren wir die Sicherheit Ihrer IoMT-Systeme und gewährleisten gleichzeitig eine hohe Betriebskontinuität.

Bereit für zukunftssichere IoMT-Security? Kontaktieren Sie uns, um mehr über unsere Healthcare Security Services zu erfahren und wie wir Ihre Betriebstechnologie schützen können. Unsere Experten stehen bereit, um mit Ihnen zusammenzuarbeiten, um eine resiliente und sichere Umgebung für die Patientenversorgung zu schaffen – die Grundlage für die weiterführende Digitalisierung.

UNSER IoMT-SECURITY PORTFOLIO

1. **Operational Technology (OT) Security Assessment:** Wir analysieren bestehende und fehlende technische sowie organisatorische Sicherheitsmaßnahmen in Ihren OT- bzw. IoMT-Systemen und identifizieren Risiken. Wir zeigen Maßnahmen auf, um die Cyber-Resilienz in Ihren Umgebungen schrittweise und nachhaltig zu steigern. Eine kombinierte Nutzung mit einer OT/IoMT Asset-Visibility Lösung (siehe Punkt 2) wird empfohlen.

2. **IoMT Asset Visibilität:** Wir schaffen umfassende Sichtbarkeit von Assets durch fortschrittliche Lösungen von spezialisierten Herstellern im Bereich OT & IoMT. Dadurch ermöglichen wir eine vollständige Inventarisierung und Überwachung aller Geräte, Systeme und Schwachstellen im Netzwerk der angeschlossenen Geräte. Zudem visualisieren wir die Netzwerkverbindungen zwischen den Systemen, externen Dienstleistern und dem Internet.

3. **Security Monitoring:** Wir entwickeln und implementieren Systeme zur Angriffserkennung für OT- und IoMT-Umgebungen. Mit fortschrittlichen Industrial Cyber Security Solutions erkennen wir Cyberangriffe, Malware und Anomalien in gerätespezifischen Protokollen.

4. **IT-/OT-Netzwerksegmentierung:** Die richtige Netzwerksegmentierung von IoMT-Geräten ist essenziell, um betriebskritische Systeme sowie die Patientensicherheit zu schützen und die Ausbreitung von Angriffen einzuschränken. Unsere Segmentierungskonzepte basieren auf bewährten Modellen wie den Vorgaben der ISA/IEC 62443 und der Purdue-Referenzarchitektur, die wir mit unseren Praxiserfahrungen ergänzen. Nach Analyse des Ist-Zustands legen wir effektive Schutzzonen und sichere Netzwerksegmente fest und setzen Sie gemeinsam mit Ihnen um.

5. **Unterstützung im Bereich OT-Governance:** Wir bieten Beratung und Unterstützung bei der Einhaltung von Standards und Gesetzen wie IT-SiG 2.0, EU-NIS2 oder ISA/IEC 62443. Zudem helfen wir Ihnen, die Anforderungen von Cyberversicherungen zu erfüllen.

6. **IT-/OT-SOC (Security Operations Center):** Wir bieten Echtzeitüberwachung von IT- und OT-Systemen, um Angriffsindikatoren und Bedrohungen frühzeitig zu erkennen.

7. **Beratung zu Sicherheitsarchitektur:** Wir bieten Beratung zur Konzeption und Implementierung von technischen Sicherheitslösungen für die Sicherheitsarchitektur. Basierend auf unseren Praxiserfahrungen und Standards wie ISA/IEC 62443 umfasst dies System-Hardening, Anti-Malware-Lösungen, sichere Fernzugriffe und weitere Maßnahmen zur Risikominderung.

8. **Schwachstellen- und Risk-Management:** Ein proaktives Schwachstellenmanagement ist entscheidend, um potenzielle Sicherheitslücken frühzeitig zu erkennen und zu beheben. Unser Team unterstützt Sie mit zielgerichteter Beratung zum Aufbau eines effektiven und effizienten Schwachstellen- und Risikomanagements. Wir konzentrieren uns darauf, relevante Schwachstellen präzise zu identifizieren und durch geeignete Maßnahmen effektiv zu beheben, um Ihre IoMT-Umgebung effektiv zu schützen.

SIE MÖCHTEN MEHR ERFAHREN?
Wir freuen uns auf Ihre Kontaktaufnahme!

SVA gehört zu den führenden IT-Dienstleistern Deutschlands und beschäftigt mehr als 3.200 Mitarbeiter an 27 Standorten. Das unternehmerische Ziel von SVA ist es, hochwertige IT-Produkte der jeweiligen Hersteller mit dem Projekt-Know-how, dem Service-Spektrum und der Flexibilität von SVA zu verknüpfen, um so optimale Lösungen für die Kunden zu erzielen.

DIE FACHLICHEN FOKUSBEREICHE VON SVA SIND:

- Agile IT & Software Development
- Big Data & AI
- Business Continuity
- Cyber Security
- Datacenter Infrastructure
- Digital Process Solutions
- End-User Computing
- Mainframe
- SAP

KONTAKT

Geschäftsbereich Healthcare
Healthcare@sva.de

SVA System Vertrieb Alexander GmbH
Borsigstraße 26
65205 Wiesbaden
www.sva.de