SCHUTZ MEDIZINISCHER GERÄTE

ÜBERBLICK

Branche

Gesundheitswesen

Anwendungsbereich

Schutz medizinischer Geräte in Einrichtungen des Gesundheitswesens vor Cyberangriffen

Medizinische Geräte

Da die Cybersicherheit für die Hersteller medizinischer Geräte oft nur eine untergeordnete Rolle spielt, ist die Anfälligkeit medizinischer Geräte für Cyberangriffe inzwischen ein bekanntes Problem.

Vorteile für die Einrichtung

- Minderung der Risiken für die Patienten, die mit den Geräten behandelt werden
- Schutz vor Malware und anderen schädlichen Inhalten in Netzwerken medizinischer Geräte
- Verbesserung der Compliance mit der EU-DSGVO, HIPAA und anderen geltenden Datenschutzbestimmungen

Vorteile für den Betrieb

- Verbesserung der Transparenz des Datenverkehrs zu und von medizinischen Geräten im Netzwerk
- Vereinfachte Wartung von Segmenten in medizinischen Netzwerken durch einfachere Sicherheitsstrategien
- Reduzierung der Netzwerklatenz und der Ausfallzeiten, insbesondere bei zeitkritischen medizinischen Anwendungen

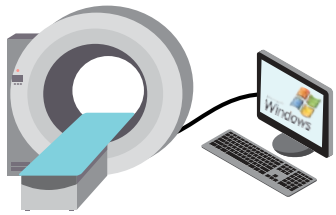
Vorteile für die Sicherheit

- Reduzierung des Risikos erfolgreicher Cyberangriffe und des Diebstahls elektronisch geschützter Gesundheitsdaten
- Verhinderung von Angriffen auf weitere Systeme von infizierten medizinischen Geräten aus (in den meisten Fällen Ransomware oder Ausschleusung elektronisch geschützter Gesundheitsdaten aus dem Netzwerk)

Herausforderung

Bezüglich der Cybersicherheit sind medizinische Geräte meist die anfälligsten Netzwerkkomponenten einer Einrichtung des Gesundheitswesens. Trotzdem werden sie aus verschiedenen Gründen oft nur unzureichend geschützt:

1. **Fehlende Kooperation seitens der Hersteller**



   Die Einrichtungen stoßen häufig auf Ablehnung, wenn sie die Hersteller medizinischer Geräte um Unterstützung bei der Sicherung dieser Geräte bitten. Oft wird die Einhaltung von Vorgaben der US-amerikanischen FDA oder anderer Regulierungsbehörden als Grund dafür genannt, dass Geräte nicht aktualisiert werden können. Dabei hat die FDA wiederholt Leitlinien für die Umsetzung grundlegender Sicherheitsmaßnahmen veröffentlicht, beispielsweise für das Patching und die Nutzung von Tools zur Endpunktsicherung.[1]

2. **Nutzung veralteter Betriebssysteme**

   Häufig stellen Hersteller medizinischer Geräte diese zusammen mit Windows-basierten PCs bereit, die die Daten überwachen und erfassen. Aufgrund der hohen Aktualisierungskosten werden mitunter noch immer Betriebssysteme wie Windows® XP oder gar Windows 95 genutzt, die schon lange nicht mehr unterstützt werden. Eine neue MRT-Anlage kann beispielsweise drei Millionen US-Dollar kosten.[2]

   Auf allen Betriebssystemen von Microsoft® sollten monatlich aktuelle Patches eingespielt werden, um neu entdeckte Schwachstellen zu beseitigen, bevor sie für Cyberangriffe ausgenutzt werden. Für nicht mehr unterstützte Betriebssysteme werden jedoch keine Patches mehr veröffentlicht. Ein nicht gepatchter Windows-PC, der mit einem medizinischen Gerät verbunden ist, kann zum Einfallstor für verschiedene Arten von Cyberangriffen werden. Wenn durch einen solchen Angriff Malware auf ein medizinisches Gerät gelangt, kann diese die mit dem Gerät behandelten Patienten gefährden oder elektronisch geschützte vertrauliche Patientendaten aus dem Netzwerk ausschleusen.

3. **Geräteverwaltung per Fernzugriff mit nicht standardgerechten Verfahren**

   In Krankenhäusern werden teilweise Tausende von Geräten eingesetzt, die von Hunderten unterschiedlicher Hersteller stammen können. Wenn jeder Hersteller auf einem eigenen Verfahren zur Fernverwaltung seiner Geräte besteht, kann dies zu unnötigen Risiken für das Krankenhaus führen.

4. **Fehlende Bewertung medizinischer Geräte vor dem Einsatz**

   Angesichts der inkonsistenten Sicherheit von medizinischen Geräten sind Einrichtungen des Gesundheitswesens letztendlich selbst dafür verantwortlich, die Sicherheit jedes einzelnen Geräts zu prüfen, bevor sie es an ihr Netzwerk anschließen. Wenn eine Einrichtung bzw. der verantwortliche Mitarbeiter ein Gerät vor dem Kauf nicht angemessen bewertet, kommt es zu vermeidbaren Risiken.

   In diesem Dokument geht es um die Bewältigung dieser vier gängigen Herausforderungen in Einrichtungen des Gesundheitswesens.

1. https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm
2. http://www.time.com/money/2995166/why-does-mri-cost-so-much/

Geschäftliche Einflussfaktoren

Medienberichte über Sicherheitslücken haben das öffentliche Bewusstsein für die Gefahren geschärft, die durch ungeschützte oder nicht gepatchte medizinische Geräte in Einrichtungen des Gesundheitswesens entstehen.

- 2013 – Dick Cheney, der ehemalige Vizepräsident der USA, gibt Änderungen seines Herzschrittmachers in Auftrag, um Angriffe zu verhindern.[3]
- 2015 – Die FDA bestätigt, dass es möglich sei, über das Netzwerk eines Krankenhauses per Fernzugriff auf das Symbiq Infusion System zuzugreifen.[4]
- 2015 – Die FDA und Hospira® veröffentlichen ein Dokument, das Sicherheitslücken in bestimmten LifeCare-Infusionspumpen von Hospira beschreibt.[5]
- 2016 – Das Unternehmen Johnson & Johnson® warnt seine Kunden, dass eine seiner Insulinpumpen anfällig für Cyberattacken sei.[6]
- 2016 – MedSec™ Holdings und der Hedge-Fonds Muddy Waters weisen in einer kontroversen Veröffentlichung auf mehrere kritische Sicherheitslücken in Geräten von St. Jude Medical® hin, nachdem Sie Leerkäufe von Aktien von St. Jude getätigt hatten.[7]
- 2017 – Die FDA und ein weiteres im Bereich Sicherheitsforschung aktives Unternehmen bestätigen die Existenz der Sicherheitslücke mit einem Patch und einem Sicherheitshinweis.[8]

Da Hersteller ihre Geräte traditionell kaum oder gar nicht durch integrierte Sicherheitsmaßnahmen schützen, werden in Zukunft höchstwahrscheinlich ähnliche Meldungen über weitere Schwachstellen folgen, die die Sicherheit und Effizienz verschiedener medizinischer Geräte gefährden.

Gefahren	Bedrohung	Schwachstellen
• Patientensicherheit • Patientendaten • Betriebsausfall und Umsatzverlust • Patientenvertrauen • Guter Ruf	• Malware • Nicht autorisierte Manipulation der Therapie • Lateraler Angriff • Hacktivismus • Cyberkriegsführung	• Lange Nutzungsdauer • Kein sicherheitsgerechtes Designziel • Fehlender Endpunktschutz vor Malware • Mangelhaftes Patching • Stark reglementierte, nicht anpassbare Systeme

Abbildung 1: Überblick über gefährdete Bereiche, Bedrohungen und Risikofaktoren bei medizinischen Geräten

In den USA legt die Lebensmittel- und Arzneimittel-Überwachungsbehörde FDA die Regeln und Vorschriften für medizinische Geräte fest. 2014 hat die FDA eine Richtlinie herausgegeben, in der sie Herstellern medizinischer Geräte und Einrichtungen des Gesundheitswesens empfiehlt, geeignete Maßnahmen zu ergreifen, damit ein Cyberangriff nicht zum Ausfall medizinischer Geräte führen kann.[9] Die Richtlinie enthält jedoch weder einen Rahmenplan noch spezifische Empfehlungen zur Minimierung dieser Gefahr. Bislang muss also jede Einrichtung des Gesundheitswesens selbst entscheiden, wie sie ihre Geräte angemessen schützen sollte.

Herkömmliche Ansätze

Da es kaum konkrete Richtlinien zur Sicherheit von medizinischen Geräten gibt, versuchen einzelne Einrichtungen im Gesundheitswesen in Eigenregie, ihre Systeme so gut wie möglich zu schützen. Dazu nutzen sie meist ältere Sicherheitstechnologien, die die Geräte nicht angemessen schützen und nicht skalierbar genug sind, um vom Netzwerk- oder Sicherheitsteam betreut zu werden. (Mit diesem Problem haben viele IT-Verantwortliche im Gesundheitswesen zu kämpfen.)

Herkömmlicher Ansatz Nr. 1: Flaches Netzwerk

Einige Einrichtungen des Gesundheitswesens – insbesondere kleinere Kliniken – haben möglicherweise weder das Kapital noch das Personal zur Verwaltung eines komplexen, segmentierten Netzwerks. Daher schließen sie medizinische Geräte einfach an dasselbe Netzwerk an wie alle anderen Geräte. Eine solche flache Netzwerkarchitektur ist in zweierlei Hinsicht problematisch: 1) Die medizinischen Geräte sind nicht vor Problemen im restlichen Netzwerk geschützt und 2) das restliche Netzwerk ist nicht vor Problemen geschützt, die von den medizinischen Geräten ausgehen. Wie bereits oben erwähnt, sind medizinische Geräte häufig mit Windows-basierten PCs verbunden, auf denen nicht unbedingt die neuesten Endpunktschutzmaßnahmen installiert werden können. Wenn das Netzwerk und die Endpunkte nicht ausreichend geschützt sind, ist dieser Ansatz für Einrichtungen des Gesundheitswesens mit dem größten Risiko verbunden.

Keine Segmentierung:
- Medizinische Geräte und Endbenutzer-PCs im gleichen Netzwerk

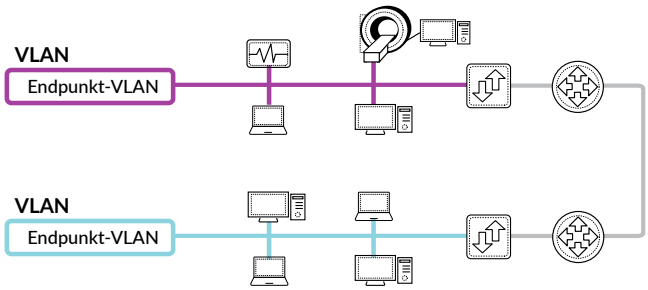
Vorteile:
- Einfache Wartung

Nachteile:
- Keine Vorkehrungen für die Netzwerksicherheit
- Hohes Risiko, dass ein infiziertes Gerät Malware an andere überträgt

3. https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/
4. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm
5. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm446809.htm
6. http://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L
7. https://threatpost.com/st-jude-patches-additional-cardiac-device/123596/
8. https://ics-cert.us-cert.gov/advisories/ICSMA-17-009-01A
9. https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

Herkömmlicher Ansatz Nr. 2: Segmentiertes Netzwerk, das nur auf switchbasierten VLANS und ACLs basiert (keine Firewall)

Häufig werden medizinische Geräte in Netzwerken im Gesundheitswesen in einem eigenen VLAN für medizinische Geräte zusammengefasst. Für die Geräte werden dann ACLs (Zugriffssteuerungslisten) auf Netzwerkebene 3 definiert, um den Verkehr zwischen den Endpunkten und dem VLAN zu regulieren. Dieser Ansatz nutzt keine internen Firewalls und bietet keinen angemessenen Schutz, da die medizinischen Geräte nach wie vor über das Netzwerk angegriffen werden können. Außerdem ist die Skalierung bei diesem Ansatz problematisch.



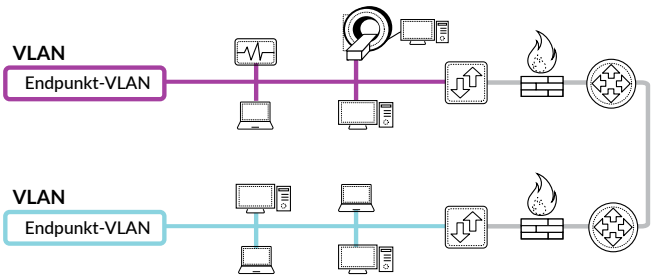
Switchbasierte ACLs:
- Nutzung von VLANs zum Isolieren medizinischer Geräte
- Steuerung des Datenverkehrs mithilfe IP- und portbasierter ACLs auf Switches

Vorteile:
- Einfache Isolierung medizinischer Geräte

Nachteile:
- IP- und portbasierte ACLs
- Administration in größeren Umgebungen nur bedingt skalierbar
- Kein Schutz gegen aktive Bedrohungen wie etwa Malware

Herkömmlicher Ansatz Nr. 3: Segmentiertes Netzwerk, das auf VLANS, ACLs im Switch und herkömmlichen Firewalls basiert

Dieser Ansatz ist mit Ansatz Nr. 2 vergleichbar, nutzt aber zusätzlich herkömmliche Firewalls, um den Datenverkehr zwischen den VLANs auf Ebene 3 einzuschränken. Dadurch ist dieser Ansatz etwas sicherer, aber er basiert immer noch auf port- und IP-basierten Regeln und hat die damit verbundenen Nachteile.



Switchbasierte ACLs mit herkömmlichen Firewalls:
- Nutzung von VLANs zum Isolieren medizinischer Geräte
- Steuerung des Datenverkehrs mithilfe IP- und portbasierter ACLs auf Switches

Vorteile:
- Bessere Isolierung medizinischer Geräte

Nachteile:
- Dieselben IP- und portbasierten ACLs wie bei Ansatz Nr. 2
- Administration in größeren Umgebungen nur bedingt skalierbar
- Kein Schutz gegen aktive Bedrohungen wie etwa Malware

Viele medizinische Geräte werden als „unantastbar" betrachtet, entweder weil der Anbieter den Endpunktschutz beschränkt oder weil es physisch nicht möglich ist, Sicherheitsvorkehrungen auf dem Gerät zu implementieren. Die einzige Möglichkeit zum Schutz solcher Geräte ist die Einschränkung des Netzwerkzugriffs. Alle herkömmlichen Ansätze zur netzwerkbasierten Zugriffskontrolle haben gemein, dass sie vier wichtige Anforderungen an den Schutz medizinischer Geräte nicht erfüllen:

1. Ausgereifte netzwerkbasierte Gefahrenabwehr
2. Einfache Verwaltung
3. Skalierbarkeit zur Unterstützung einer steigenden Anzahl an medizinischen Geräten
4. Konsistenter Ansatz für den Fernzugriff durch den Anbieter

Der Ansatz von Palo Alto Networks

Die Next-Generation Security Platform von Palo Alto Networks® bietet ein für das Gesundheitswesen angemessenes Sicherheitsniveau für medizinische Geräte. Diese Plattform verhindert durch eine ausgefeilte netzwerkbasierte Gefahrenabwehr und zonenbasierte Segmentierung, dass Bedrohungen aus anderen Netzwerksegmenten medizinische Geräte erreichen (und umgekehrt). Die Architektur der Plattform erleichtert zudem die Administration und die Skalierung zur Unterstützung einer beliebig großen Anzahl an medizinischen Geräten.

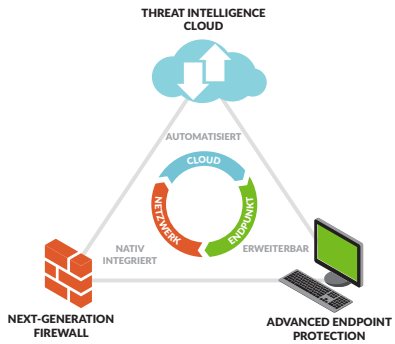


Abbildung 2: Next-Generation Security Platform von Palo Alto Networks

- **Steuerung des gesamten Datenverkehrs auf der Anwendungsebene** (Ebene 7 des OSI-Modells). Die Plattform nutzt eine innovative Technologie namens App-ID™, um Datenpakete zuverlässig zu identifizieren und der richtigen Anwendung zuzuordnen. App-ID funktioniert unabhängig vom genutzten Port und Protokoll und kann nicht durch Verschleierungstaktiken wie Port-Hopping oder Verschlüsselung umgangen werden. In hochsensiblen oder spezialisierten Zonen des Netzwerks wie beispielsweise dem CDE bietet dieser Ansatz den bestmöglichen Schutz, denn er bietet Sicherheitsadministratoren die Option, nicht identifizierbaren Datenverkehr generell zu untersagen und nur Datenpakete weiterzuleiten, die eindeutig einer legitimen Anwendung zugeordnet werden können.

ANWENDUNGSBEREICH: *Schutz medizinischer Geräte*

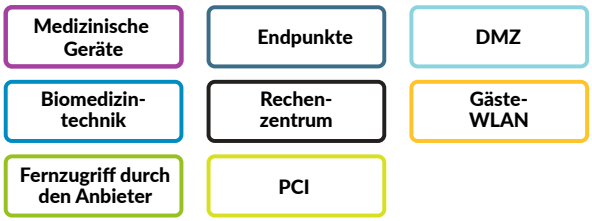
- **Minimale Zugriffsrechte** im gesamten Netzwerk: Zusammen mit App-ID versetzen unsere Technologien User-ID™ und Content-ID™ Unternehmen in die Lage, den Zugriff auf das CDE anhand einer Reihe spezifischer Attribute genau zu kontrollieren. Zu diesen Attributen zählen die jeweilige Anwendung sowie die verwendeten Funktionen, die tatsächliche Identität einzelner Benutzer und Gruppen und die Daten, auf die zugegriffen wird (wie etwa Kreditkarten- oder Sozialversicherungsnummern). Das Ergebnis ist die definierte Implementierung einer Zugriffskontrolle nach dem Konzept der Erteilung minimaler (d.h. nur unbedingt erforderlicher) Zugriffsrechte. Die Administratoren definieren klare Sicherheitsregeln und lassen nur den unbedingt erforderlichen Datenverkehr zu. Alle anderen Datenübertragungen werden automatisch blockiert.
- **Ausgefeilte Gefahrenabwehr.** Eine Kombination aus Antiviren-/Anti-Malware-, Intrusion Prevention- und Advanced Threat Prevention Technologien (Content-ID und der Bedrohungsanalysedienst WildFire™) filtern bekannte und unbekannte Bedrohungen aus dem gesamten Datenverkehr heraus.
- **Flexible Datenfilterung.** Die Administratoren können Datenverkehr von und zu legitimen Anwendungen zulassen, unerwünschte Datentransferfunktionen und Dateitypen dennoch sperren sowie die Übertragung sensibler Daten wie Kreditkartennummern oder spezifische Datenmuster in Anwendungsinhalten oder Anhängen kontrollieren.

Sicherheitsfunktion	Produkt
• Layer-7-Firewall (physisch oder virtuell) • Whitelisting von Anwendungen • URL-Filterung • Intrusion Protection System einschließlich Anti-Exploit-Lösung • Intrusion Detection System • Netzwerkbasierte polymorphe Anti-Malware-Lösung • Polymorpher Schutz vor Command-and-Control-Datenverkehr • Schutz vor Diebstahl von Anmeldedaten	• Next-Generation Firewall • URL Filtering subscription • Threat Prevention subscription
• Malware-Analyseumgebung (Sandbox) mit automatischer Signaturerstellung für Feedback-basierten Schutz vor neuen Bedrohungen an den Sicherheitspunkten	• WildFire-Subscription oder -Appliance
• Geräte- und Richtlinienverwaltung und Bedrohungstransparenz	• Panorama™ für das Management der Netzwerksicherheit
• Endpunktbasierte Anti-Exploit-Lösung (signaturlos) • Endpunktbasierte Anti-Malware-Lösung (signaturlos)	• Traps™ advanced endpoint protection
• Bedrohungsdatenanalyse, -suche und -abwehr • Automatisierte Einspeisung und Nutzung von Bedrohungsdaten	• Kontextbezogener Bedrohungsdatenservice AutoFocus™ • MineMeld™ zum Sammeln, Nutzen und Teilen von Bedrohungsdaten, eigenständig oder als Teil von AutoFocus
• SaaS-Anwendungstransparenz, Schutz des geistigen Eigentums und Gefahrenabwehr	• SaaS-Sicherheitsdienst Aperture™
• Ununterbrochen verfügbares Client-VPN für Endpunkte stellt sicher, dass der gesamte Datenverkehr von einem Endpunkt eine Next-Generation Firewall passieren muss.	• Netzwerksicherheit für Endpunkte durch GlobalProtect™

Abbildung 3: Wichtige Sicherheitsfunktionen auf der Next-Generation Security Platform

Der Ansatz von Palo Alto Networks zum Schutz von medizinischen Geräten basiert im Wesentlichen auf der Next-Generation Firewall von Palo Alto Networks, die wiederum auf die erweiterten Sicherheitsfunktionen der anderen oben beschriebenen Produkte zugreift. Die Next-Generation Firewall wird in Einrichtungen des Gesundheitswesens zur Definition von Zonen (Netzwerksegmentierung) genutzt. Beispiele für derartige Zonen in einem Krankenhaus finden Sie in Abbildung 4.

Abbildung 4: Beispiele für Sicherheitszonen zur Netzwerksegmentierung in einem Krankenhaus



In Krankenhäusern werden häufig weitere Sicherheitszonen definiert, um die Sicherheitsinfrastruktur durch zusätzliche Isolierung zu verbessern.

1. Zusätzliche Zonen im Segment mit den medizinischen Geräten schränken den Zugriff durch den Anbieter und andere kritische Funktionen wie die Patientenüberwachung ein
2. Zusätzliche Zonen im PCI-Segment grenzen endpunktbasierte Geräte von rechenzentrumsbasierten Geräten ab
3. Zusätzliche Zonen im Endpunktsegment isolieren Abteilungen (beispielsweise die Finanzabteilung und die Krankenpflege) voneinander
4. Dedizierte Zonen für IP-Telefone und/oder Badging-Systeme

Das folgende Diagramm zeigt beispielhaft eine logische Architektur, in der die Next-Generation Firewall Isolierungszonen zwischen Geräten erzwingt, die an ein Krankenhausnetzwerk angeschlossen sind. Jeder Datenverkehr zwischen zwei Zonen muss eine Next-Generation Firewall passieren und wird dort auf Bedrohungen untersucht. Nur Datenverkehr, der von den Sicherheitsrichtlinien ausdrücklich zugelassen ist, kann die Firewall passieren. Eine Zone ist eine Gruppierung von physischen oder virtuellen Schnittstellen, die einem Netzwerksegment entspricht, an Ihre Firewall angeschlossen ist und von ihr kontrolliert wird. Die Zoneneinteilung kann auf vielen Faktoren basieren, die am häufigsten genutzte Trennungsbasis sind jedoch VLANs. Wie in Abbildung 5 dargestellt gibt es normalerweise ein VLAN je Zone.

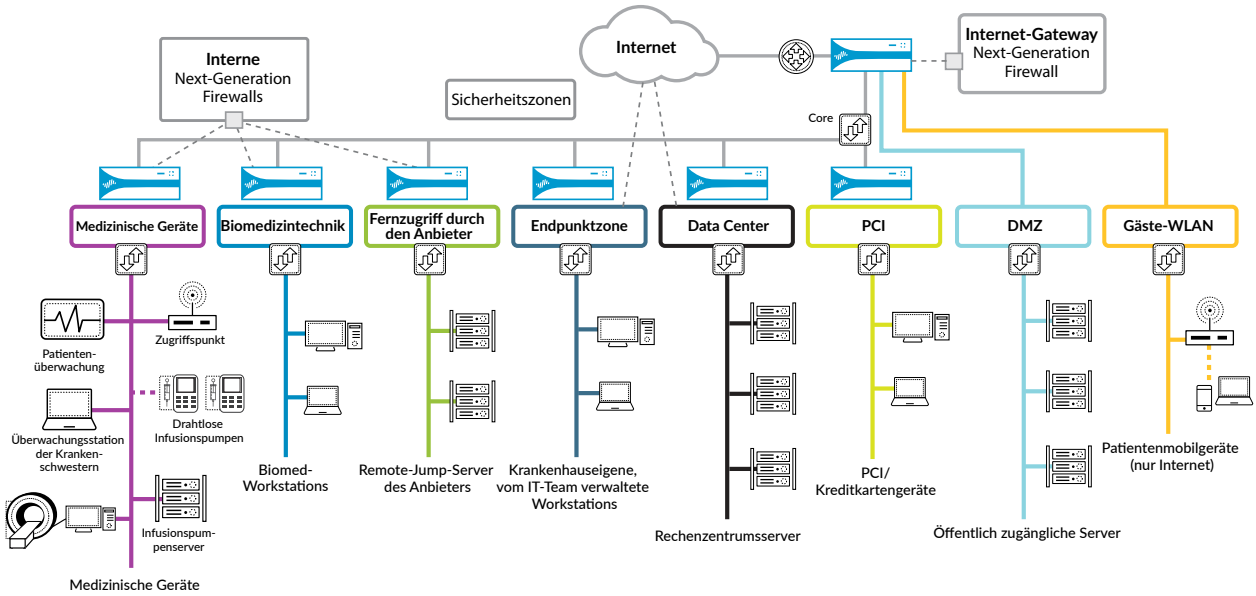


Abbildung 5: Diagramm einer Architektur mit Sicherheitszonen für medizinische Geräte

Die drei Zonen mit medizinischen Geräten sind als 1) Medizinische Geräte, 2) Biomedizintechnik und 3) Fernzugriff durch den Anbieter ausgewiesen.

- Die Zone „Medizinische Geräte“ umfasst alle drahtgebundenen und drahtlosen medizinischen Geräte.
- Die Zone „Biomedizintechnik“ umfasst alle Workstations, die von den Mitarbeitern zur Unterstützung medizinischer Geräte genutzt werden. Diese Zone kann auch PCs umfassen, die von Krankenhausmitarbeitern zur Analyse von Daten aus medizinischen Geräten genutzt werden.
- Die Zone „Fernzugriff durch den Anbieter“ soll die Jump-Server umfassen, über die die Hersteller oder Anbieter auf einzelne medizinische Geräte zugreifen können, um sie per Fernzugriff zu verwalten.

Die Sicherheitsstrategien, mit denen definiert wird, welche Datenflüsse in den einzelnen Zonen zulässig sind, basieren auf einem Zero-Trust-Modell. Standardmäßig wird jedweder Datenverkehr zwischen den Zonen blockiert. Nur der Datenverkehr für die ausdrücklich zugelassenen Anwendungen (mit App-ID) und Benutzer (mit User-ID) kann die Firewall passieren.

Normaler Datenverkehr zwischen den Zonen

Die folgende Tabelle zeigt einige Datenströme, die bei der Definition der Zonen und der entsprechenden Sicherheitsrichtlinien in der Next-Generation Firewall berücksichtigt werden sollten. Dank der dynamischen Adressgruppen in PAN-OS® können Geräte in PAN-OS problemlos gruppiert und anhand verschiedener Kriterien (wie zum Beispiel IP-Adressbereiche) automatisch angepasst werden, wenn Geräte hinzugefügt, verlagert oder entfernt werden.

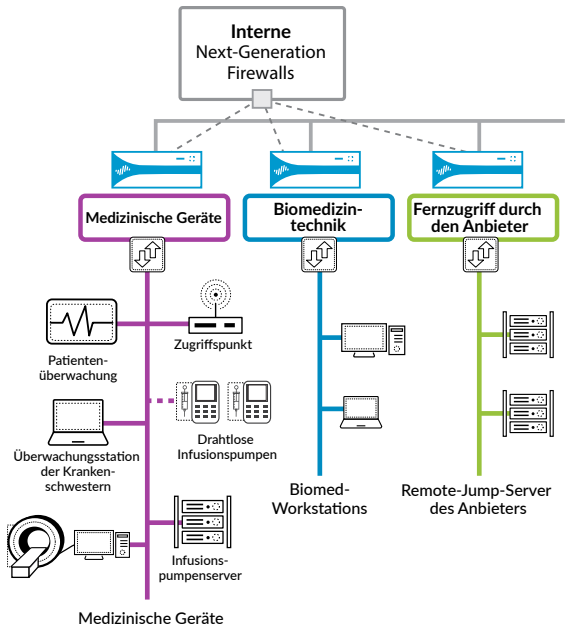


Abbildung 6: Überblick über Sicherheitszonen für medizinische Geräte

Beispiele für die Notwendigkeit von Datenflüssen	Sicherheitsrichtlinien auf der Sicherheitsplattform für den Datenverkehr zwischen Zonen

Ein medizinisches Gerät soll Daten an ein elektronisches Patientendatensystem übertragen, das sie in die entsprechende Patientenakte einträgt.	• Konfigurieren Sie zwei dynamische Adressgruppen:
	  · Eine Gruppe enthält die zugelassenen medizinischen Geräte.
	  · Die andere enthält die Server für elektronische Patientendatensysteme in der Rechenzentrumszone.
	• Erstellen Sie eine Sicherheitsrichtlinie, die bestimmte App-IDs in beiden dynamischen Adressgruppen zulässt.

Medizinische Geräte sollen Daten an PCs in der Zone „Biomedizintechnik“ übertragen, wo diese von technischen Mitarbeitern und Ärzten analysiert werden.	• Konfigurieren Sie zwei dynamische Adressgruppen:
	  · Eine Gruppe enthält die zugelassenen medizinischen Geräte.
	  · Die andere enthält PCs für die Biomedizintechnik in der Zone „Biomedizintechnik“.
	• Erstellen Sie eine Sicherheitsrichtlinie, die bestimmte App-IDs in beiden dynamischen Adressgruppen zulässt.

Der Hersteller von medizinischen Geräten soll eine Gruppe von medizinischen Geräten per Fernzugriff verwalten.	Fordern Sie vom Hersteller, dass er mit dem GlobalProtect-Client zusammenarbeitet • Konfigurieren Sie eine Sicherheitsrichtlinie, die Herstellern anhand der Sicherheitsgruppe im Unternehmensverzeichnis Zugriff auf bestimmte Jump-Server in der Zone „Fernzugriff durch den Anbieter“ gewährt. • Konfigurieren Sie eine dynamische Adressgruppe für eine Gruppe von medizinischen Geräten. • Konfigurieren Sie eine Richtlinie, die bestimmten App-IDs (z.B. RDP) in der Zone „Fernzugriff durch den Anbieter“ Zugang zu den dynamischen Adressgruppen der Geräte erlaubt.
Drahtlose Geräte sollen mit einem Server verbunden werden (z.B. drahtlose Infusionspumpen mit einem Infusionspumpenserver), damit sie auf Medikamentenbibliotheken zugreifen und Diagnose- und Therapiestatistiken melden können.	• Es ist keine Sicherheitsrichtlinie erforderlich, da der Datenverkehr keine Zonengrenze überquert und daher keine Next-Generation Firewall passieren muss.

Abbildung 6: Beispiele für Anforderungen an den Datenfluss und die jeweils möglichen Sicherheitsrichtlinien auf der Sicherheitsplattform

Wie in den vorherigen Abschnitten beschrieben, lässt die Next-Generation Firewall Datenverkehr zwischen Zonen unter Berücksichtigung einer Kombination aus App-ID, User-ID und dynamischen Adressgruppen zu. Dies ermöglicht das Erstellen von Sicherheitsrichtlinien, die leicht verständlich sind und einfach verwaltet werden können. Kunden fragen jedoch häufig, wie der Datenverkehr innerhalb einer Zone am Zugriffs-Switch (Layer 2) beschränkt werden kann, also näher am Gerät als die Firewall. Solche Layer-2-Kontrollen sind erforderlich, um strengere Richtlinien durchzusetzen, beispielsweise wenn medizinische Geräte am selben Switch und im selben VLAN nicht miteinander kommunizieren dürfen. Der nächste Abschnitt stellt verschiedene Optionen für die Erfüllung derartiger Anforderungen in Krankenhäusern vor.

Optionen zur Kontrolle des Datenverkehrs auf Ebene 2

In der folgenden Tabelle sind Optionen aufgelistet, mit denen der Datenverkehr am Zugriffs-Switch (also auf Layer 2) eingeschränkt werden kann. Dabei handelt es sich typischerweise um Datenverkehr, der von der Next-Generation Firewall kommt.

Option 1 – Einrichtung eines VLANs für die verschiedenen Arten von medizinischen Geräten Der meistgenutzte Ansatz für die Netzwerksegmentierung in Krankenhäusern ist die Einrichtung eines speziellen VLANs (und einer entsprechenden Zone) für jeden Gerätetyp. So gibt es beispielsweise ein VLAN für Infusionspumpen und ein anderes für Kernspintomografen. Alle Datenströme von einem VLAN zum anderen werden zwecks Layer-3-Prüfung zur Next-Generation Firewall hin gebündelt gesendet. Krankenhäuser mittlerer Größe haben typischerweise 20 bis 30 VLANs und Zonen für medizinische Geräte verschiedener Art.	**Vorteile:** • Einfachste Lösung für eine angemessene Segmentierung mit minimalem Administrationsaufwand. **Nachteile:** • Der Datenverkehr innerhalb der VLANs, also der Verkehr zwischen medizinischen Geräten der gleichen Art, wird nicht kontrolliert, da er keine Next-Generation Firewall passiert. • Die VLAN-Zuweisung eines Geräts in einem drahtgebundenen Netzwerk wird nicht automatisch aktualisiert. Wenn ein Gerät verlagert wird, muss die Port-VLAN-Zuweisung am Switch manuell geändert werden.
Meistgenutzter Ansatz	
Option 2 – ACLs auf dem Zugriffs-Switch Bei dieser Option wird der Datenverkehr nicht durch VLANs, sondern durch ACLs auf den Zugriffs-Switches kontrolliert.	**Vorteile:** • Feinkörnigere Zugriffskontrolle für jedes einzelne Gerät. **Nachteile:** • Die Anzahl der ACLs steigt oft schnell an, sodass die Administration nach kurzer Zeit sehr aufwendig wird. Dieser explosionsartige Anstieg der ACLs ist besonders in großen Krankenhausnetzwerken zu beobachten. • Es gibt keinerlei Sicherheitsvorkehrungen zur Verhinderung der Ausbreitung von Malware zwischen den medizinischen Geräten in einem VLAN.
Option 3 – Einsatz einer kleinformatigen Next-Generation Firewall an jedem Zugriffs-Switch Jeder Zugriffs-Switch wird mit einer passenden Next-Generation Firewall ausgestattet, die die Zugriffsrichtlinien durchsetzt.	**Vorteile:** • Die Sicherheitsfunktionen der nächsten Generation verhindern die Übertragung von Malware und anderen Bedrohungen von einem medizinischen Gerät zum anderen. **Nachteile:** • Wenn die Anzahl der mit medizinischen Geräten verbundenen Zugriffs-Switches zu groß wird, ist diese Option möglicherweise zu teuer.

Option 4 – Einsatz von ForeScout zur Automatisierung der VLAN-Zuweisungen auf der Zugriffs-Switch-Ebene und zur Integration mit der Next-Generation Firewall

ForeScout® arbeitet mit vorgelagerten Next-Generation Firewalls zusammen, um infizierte Geräte automatisch in einem eigens eingerichteten Segment zu isolieren.

ForeScout CounterACT® wird direkt mit den Zugriffs-Switches verbunden und erledigt NAC-ähnliche Aufgaben. CounterACT überwacht, verwaltet und koordiniert die mit dem Netzwerk verbundenen medizinischen Geräte.

Dynamische Netzwerksegmentierung
Durch die gemeinsame Nutzung von ForeScout und Palo Alto Networks können Krankenhäuser ihr Netzwerk dynamisch segmentieren und die Sicherheitsmaßnahmen zwischen den Produkten automatisieren.

Wenn ein medizinisches Gerät an das Netzwerk angeschlossen wird, erkennt CounterACT die Art des Gerätes und kommuniziert mit der Next-Generation Firewall, um die dynamischen Adressgruppen automatisch mit Tags für die Netzwerksegmentierung zu aktualisieren.

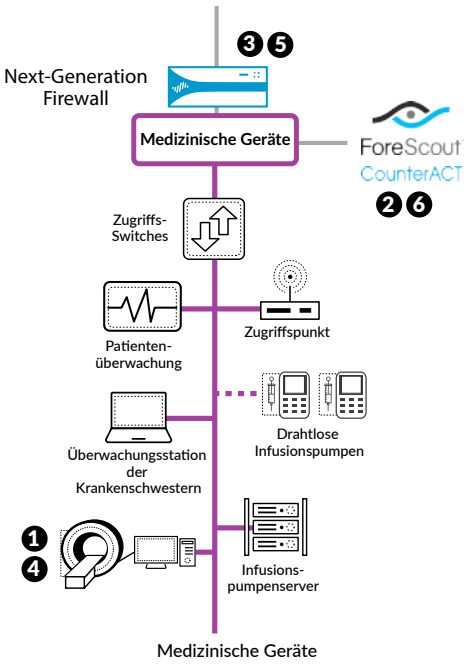
Automatische Isolierung infizierter Geräte
Wenn die Next-Generation Firewall beziehungsweise WildFire erkennt, dass ein medizinisches Gerät infiltriert wurde, wird CounterACT benachrichtigt. CounterACT kann so konfiguriert werden, dass es das infizierte Gerät automatisch isoliert, um die Ausbreitung der Malware zu verhindern.

Vorteile:

- Höchstes Maß an Automatisierung und Gefahrenabwehr.
- VLAN-Zuweisungen „folgen" den Geräten, wenn sie an neue Ports im Netzwerk angeschlossen werden.
- Hervorragende Gefahrenabwehr: Die Sicherheitsfunktionen der nächsten Generation verhindern, dass sich Bedrohungen wie etwa Malware von einem medizinischen Gerät zum anderen ausbreiten können.
- Deutlich geringerer Administrationsaufwand: CounterACT klassifiziert neue medizinische Geräte automatisch und weist sie der richtigen VLAN-Zone und Next-Generation Firewall zu. So kann eine rasant steigende Anzahl von ACLs problemlos verwaltet werden.

Nachteile:

- Wenn die Anzahl der mit medizinischen Geräten verbundenen Zugriffs-Switches zu groß wird, ist diese Option möglicherweise zu teuer.



Szenario 1: Automatische Netzwerksegmentierung für verschiedene Arten von medizinischen Geräten

1. Verschiedene Arten von medizinischen Geräten sind an das Netzwerk angeschlossen.
2. ForeScout CounterACT erkennt, klassifiziert und kategorisiert medizinische Geräte automatisch aufgrund ihrer Identität, Funktion und anderer Kriterien.
3. Anschließend fügt ForeScout Extended Module das medizinische Gerät in eine dynamische Adressgruppe einer Next-Generation Firewall von Palo Alto Networks ein. Dabei leitet es neben Tags auch andere Informationen weiter, beispielsweise zur Funktion und zur Kompatibilität.
4. Die Next-Generation Firewall nutzt diese Daten von ForeScout und vordefinierte Richtlinien, um die richtigen Zugriffsrechte zu definieren. Nicht vertrauenswürdige Geräte werden komplett blockiert. Für medizinische Geräte werden nur die unbedingt erforderlichen Zugriffsrechte gewährt.

Szenario 2: Automatische Netzwerkisolierung medizinischer Geräte

5. Eine Next-Generation Firewall erkennt, dass ein medizinisches Gerät mit Malware infiziert wurde und benachrichtigt CounterACT.
6. ForeScout CounterACT isoliert das medizinische Gerät im Netzwerk, um die Ausbreitung der Malware zu verhindern.

Abbildung 7: Integration von Palo Alto Networks Next-Generation Firewall mit ForeScout CounterACT

Praxisbeispiel aus einem Krankenhaus

Das Fisher-Titus Medical Center bietet über 70.000 Einwohnern in North Central Ohio eine umfassende, hochmoderne Gesundheitsversorgung. Die Klinik umfasst ein Akutkrankenhaus mit 99 Betten, eine Pflegeeinrichtung mit 69 Betten, eine Einrichtung für betreutes Wohnen mit 48 Einheiten, ein Gesundheitszentrum sowie ambulante Dienste. Das Fisher-Titus Medical Center ist ein gemeinnütziges kommunales Krankenhaus. Es nutzt Technologie in verschiedenen Bereichen, um die Krankenversorgung zu verbessern und die Administration zu straffen. Potenzielle Schwachstellen in den medizinischen Geräten, das steigende Risiko von Cyberangriffen und das Wachstum der Einrichtung führten dazu, dass die Klinik sich für die Next-Generation Sicherheitsplattform von Palo Alto Networks entschied, als der Support für ihre Firewalls von Juniper Networks® endete.

Die Klinik hat mehrere VLANs und Zonen für verschiedene Arten von medizinischen Geräten und Standorten definiert. Spezifische Richtlinien in der Next-Generation Firewall legen nun genau fest, welche medizinischen Geräte miteinander kommunizieren dürfen. Mit einer sorgfältig gewählten Mischung aus geeigneten VLANs und Zonen konnte die Klinik den Wartungsaufwand für die ACLs minimieren und einen zuverlässigen Prozess für die Implementierung neuer medizinischer Geräte in ihrem Netzwerk entwickeln.

FISHER TITUS MEDICAL CENTER
Simply Smarter Care

„Unsere alten Firewalls haben nur den Datenverkehr für bestimmte Dienste und Ports blockiert. Es ließ sich nicht genau erkennen, welche Anwendungen die medizinischen Geräte ausführten, deshalb konnte Malware unbemerkt eingeschleust werden."

– Dylan Border
Lead Project Engineer

Zum vollständigen Kundenbericht

Das Sicherheitsteam hat einen detaillierten Überblick sowohl über den bekannten legitimen Datenverkehr als auch über den als schädlich oder verdächtig erkannten Verkehr, der mit neuen Richtlinien schnell und problemlos gehandhabt werden kann. Außerdem kann das Team mit Funktionen wie etwa App-ID und User-ID aufgrund der Rollen der verschiedenen Benutzer festlegen, welche Nutzer auf welche Anwendungen und Systeme zugreifen dürfen.

Die Implementierung im Überblick

Produkte:

- Next-Generation Firewall von Palo Alto Networks
- Subscriptions: URL-Filtering, Threat Prevention, WildFire (optional)

Vorgehensweise:

Plan für den schrittweisen Einsatz: Wie jede große Technologie-Bereitstellung sollte auch die Implementierung einer Next-Generation Firewall schrittweise mit zunehmender Abdeckung und Kontrolle erfolgen. In Einrichtungen des Gesundheitswesens, die auf mehrere Standorte verteilt sind, werden Next-Generation Firewalls häufig an einem Standort nach dem anderen eingeführt. Dabei bietet es sich an, mit den weniger kritischen Netzwerksegmenten zu beginnen.

Definition von VLANs, Zonen und Umfang der einzelnen Phasen: Beim Einsatz einer Next-Generation Firewall ist der Schutz von medizinischen Geräten typischerweise nur einer von vielen Anwendungsbereichen. In einem Krankenhaus werden außerdem viele andere Geräte genutzt, die ebenfalls den richtigen Netzwerksegmenten zugeordnet werden müssen. Erstellen Sie zunächst eine grobe Übersicht der im Netzwerk eingesetzten Gerätekategorien und legen Sie für jede Kategorie eine Zone fest (siehe Abbildung 4). Sobald Sie wissen, wie viele Zonen Sie benötigen, erstellen Sie die für die Genehmigung durch die Entscheidungsträger erforderliche Dokumentation. Sie werden vermutlich Genehmigungen für 1) die VLAN-/Zonenarchitektur in der vorliegenden Form, 2) die schrittweise Änderung der Architektur und 3) den endgültigen Zustand einholen müssen.

Besprechen Sie die Vor- und Nachteile der verschiedenen, im Abschnitt „Optionen zur Kontrolle des Datenverkehrs auf Layer 2“ skizzierten Möglichkeiten mit Ihren Netzwerk- und Sicherheitsarchitekten, und wägen Sie sorgfältig ab, ob das Risiko von VLAN-internem Datenverkehr bzw. Verkehr zwischen medizinischen Geräten minimiert werden soll.

Die Umstellung von einer flachen zu einer stark segmentierten Netzwerkarchitektur erfordert eine sorgfältige Planung, Änderungsmanagement und ausreichend Zeit, denn das Scheitern eines solchen Projekts kann schnell zu negativen Schlagzeilen führen. Der Aufwand lohnt sich jedoch – insbesondere, wenn die Vorteile der Automatisierung der Plattform spürbar werden.

Vorteile der Nutzung von Palo Alto Networks zum Schutz medizinischer Geräte

Vorteile für das Geschäft

- Minderung der Risiken für die Patienten, die mit den Geräten behandelt werden
- Schutz vor Malware und anderen schädlichen Inhalten in Netzwerken medizinischer Geräte
- Verbesserung der Compliance mit der EU-DSGVO, HIPAA und anderen geltenden Datenschutzbestimmungen

Vorteile für den Betrieb

- Verbesserung der Transparenz des Datenverkehrs zu und von medizinischen Geräten im Netzwerk
- Vereinfachte Wartung von Segmenten in medizinischen Netzwerken durch einfachere Sicherheitsstrategien
- Reduzierung der Netzwerklatenz und der Ausfallzeiten, insbesondere bei zeitkritischen medizinischen Anwendungen

Vorteile für die Sicherheit

- Reduzierung des Risikos erfolgreicher Cyberangriffe und des Diebstahls elektronisch geschützter Gesundheitsdaten
- Verhinderung von Angriffen auf weitere Systeme von infizierten medizinischen Geräten aus (in den meisten Fällen Ransomware oder Ausschleusung elektronisch geschützter Gesundheitsdaten aus dem Netzwerk)

Fazit

Hacker werden Krankenhäuser und andere Einrichtungen des Gesundheitswesens auch weiterhin angreifen, um Patientendaten zu stehlen oder Ransomware einzuschleusen. Medizinische Geräte sind aus mehreren Gründen besonders anfällig für Cyberangriffe. Eine umfassende Sicherheitsstrategie für Unternehmen im Gesundheitswesen erfordert spezielle Maßnahmen zur Erkennung und Abwehr von Angriffen auf medizinische Geräte. Die Next-Generation Sicherheitsplattform von Palo Alto Networks bietet einen äußerst effektiven Ansatz. Die wichtigsten Sicherheitsfunktionen sind in die Plattform integriert. Die flexible Segmentierung basiert auf App-ID für die Anwendungserkennung und User-ID für die Benutzererkennung. Der umfassende Ansatz für die Segmentierung unterstützt die ständig steigende Anzahl und Vielfalt medizinischer Geräte sowie das ausgedehnte Internet der medizinischen Dinge. So können Einrichtungen im Gesundheitswesen viele der Bedrohungen minimieren, denen ihre Geräte ausgesetzt sind, und gleichzeitig die hohen medizinischen Standards wahren, die ihre Patienten erwarten.

Theatinerstr. 23
80333 München, Deutschland
Telefon: 0800-7239771
Sales: 0800-7239771
Support: +31 20 808 4600
www.paloaltonetworks.de