PHILIPS

mShield

White Paper

Philips mShield für Krankenhausnetzwerke

Absicherung medizinischer Geräte

Zusammenfassung

Die zunehmende Verbreitung vernetzter medizinischer Geräte, die handelsübliche, integrierte Betriebssysteme verwenden, und die Zunahme an Cyberangriffen auf Gesundheitseinrichtungen machen Krankenhäuser anfälliger für bösartige Angriffe. Zum Schutz vor solchen Angriffen benötigen Krankenhäuser ein mehrschichtiges Sicherheitskonzept mit vielen Barrieren gegen das Eindringen, darunter Patches, Anti-Malware-Lösungen und Firewalls. Philips mShield ist eine Firewall, die für Bildgebungssysteme entwickelt wurde und eine zusätzliche Sicherheitsebene bietet, ohne die Gerätefunktion einzuschränken. Sie schützt Geräte, damit Patienten selbst bei Angriffen auf das Netzwerk weiterhin untersucht werden können.

Einleitung

Krankenhäuser werden zunehmend digital, um Patienten eine bessere Versorgung und Mitarbeitern optimierte Arbeitsabläufe bieten zu können. Persönliche, sensible und vertrauliche Daten werden zwischen den Radiologiesystemen der verschiedenen Abteilungen einer Einrichtung ausgetauscht. Diese Informationen vor Cyberangriffen zu schützen, ist genauso wichtig wie schwierig.

Vorteile von mShield:

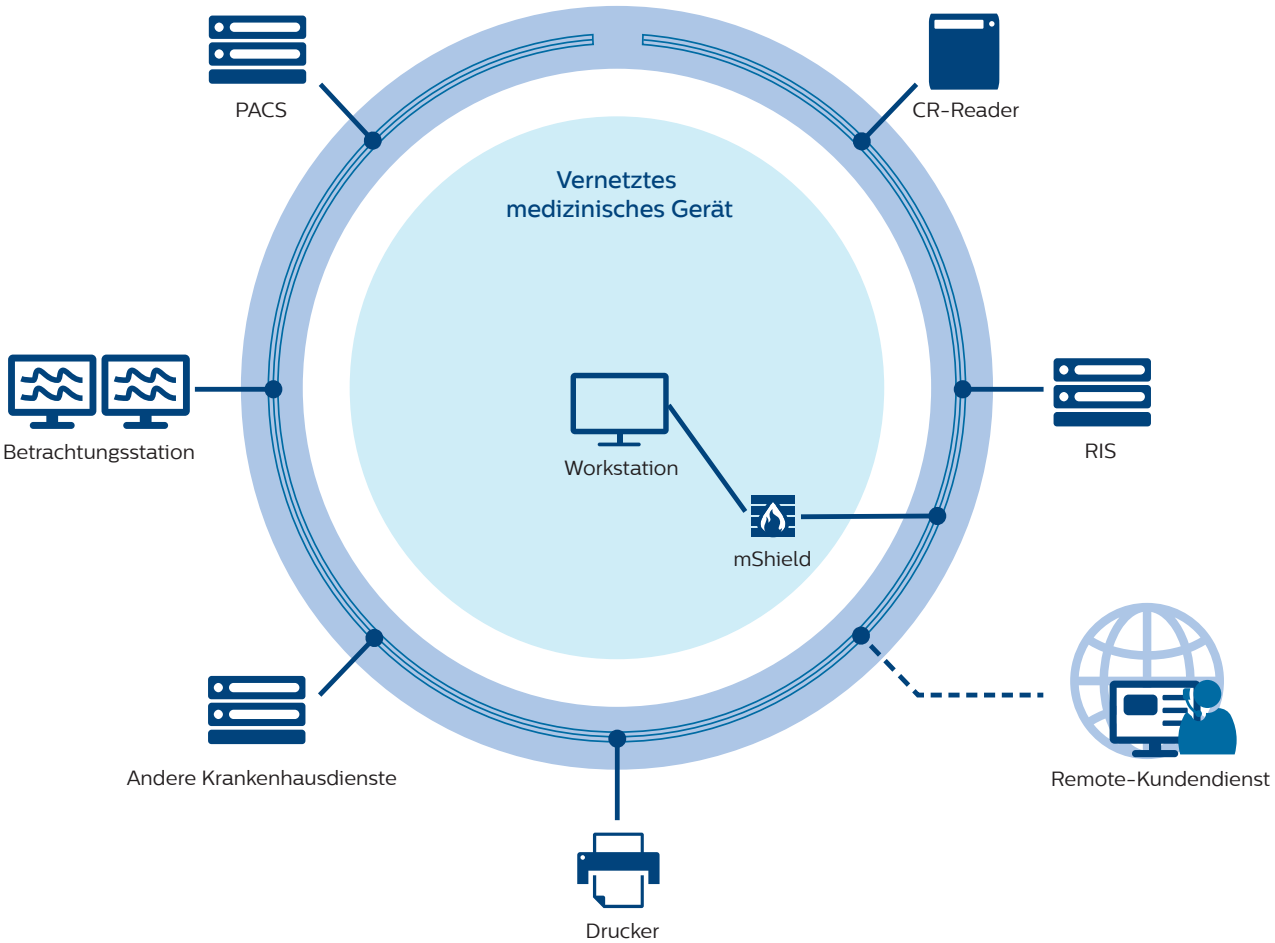
- Verhindert die Replikation von Malware über das Netzwerk
- Gewährleistet die Geräteverfügbarkeit
- Bietet eine zusätzliche Sicherheitsebene

Schutz für medizinische Geräte mit mShield

Der Umgang mit Risiken: Empfehlungen und Herausforderungen
Mit einem mehrschichtigen Sicherheitskonzept können sich Krankenhäuser besser gegen viele Bedrohungen ihrer Daten und Systeme verteidigen. Im Einklang mit bewährten Abläufen (Best Practices) sollte das Konzept u.a. folgende Maßnahmen umfassen:

- Regelmäßige Installation wichtiger Sicherheitspatches für das Betriebssystem und Anti-Malware-Lösungen zum Schutz gegen Cyberangriffe und Viren während der gesamten Lebensdauer des Systems
- Härten und Zugriffskontrollen auf Anwendungsebene zur Risikominderung – nur zulässige und erkannte Daten dürfen in das System gelangen
- Hardware-Firewalls, die nur autorisierten Datenverkehr zulassen

Diese Liste unterscheidet sich kaum von den Empfehlungen für andere Branchen. Ein effektiv implementiertes und mehrschichtiges Sicherheitskonzept ist im Fall von medizinischen Geräten jedoch besonders wichtig.



Software-Patches
Software-Patches schließen Sicherheitslücken, die nach der Software-Installation entdeckt werden. Durch regelmäßige Updates können Gesundheitseinrichtungen Schwachstellen in ihrer Software beseitigen, die einen Angriffspunkt für Cyberangriffe auf ihre Systeme und Daten bieten.

Anti-Malware-Lösungen
Anti-Malware-Lösungen sollten als wichtige Schutzmaßnahme Teil eines jeden Endpunkt-Sicherheitskonzepts sein. Eine gängige Anti-Malware-Lösung sind Virenscanner. Virenscanner müssen stets über aktuelle Virendefinitionsdateien mit den neuesten Viren und die aktuellste Scan-Engine verfügen, um wirksam zu sein. Wenn ein medizinisches Gerät nicht mit dem Netzwerk verbunden ist, und sei es nur für kurze Zeit, besteht die Gefahr, ein wichtiges Update zu verpassen.

Eine zweite Anti-Malware-Lösung ist das Whitelisting von Anwendungen. Mit dieser Methode können auf dem System nur Programme ausgeführt werden, die sich auf einer Whitelist befinden, es wird also quasi eine bekannte Softwarekonfiguration eines bestimmten Zeitpunkts festgeschrieben. So wird sogar unterbunden, dass noch nicht bekannte Malware nicht autorisierte Änderungen durchführt (Zero-Day-Exploits). Whitelisting erfordert keine regelmäßigen Updates, um wirksam zu sein.

Hardware-Firewalls
Eine dritte Sicherheitsmaßnahme gegen Angriffe ist die Hardware-Firewall. Eine typische Firewall stellt eine Barriere zwischen internen und externen Netzwerken her und bestimmt anhand von Sicherheitsregeln, ob der Netzwerkverkehr sicher ist. Sie kann das interne Netzwerk auch in Subnetze aufteilen und zwischen diesen Subnetzen Firewall-Filterregeln einsetzen. Diese Sicherheitslösung kann außerdem wichtige Netzwerkknoten isolieren, bis eine potenzielle Bedrohung neutralisiert ist.

Eine spezielle Firewall für Medizinprodukte von Philips: mShield
Aufgrund der speziellen Gegebenheiten bei medizinischen Geräten sind Bildgebungssysteme selbst mit einem hervorragenden Endpunkt-Sicherheitskonzept angreifbar. Daher hat Philips mShield entwickelt, um Krankenhäuser in ihren Sicherheitsbestrebungen zu unterstützen und gleichzeitig die wichtige Versorgungsfunktion seiner medizinischen Geräte zu sichern. mShield ist eine dedizierte Firewall, die Bedrohungen für Bildgebungssysteme wirksam blockiert und die Systeme schützt, ohne ihre Nutzung einzuschränken.

mShield umfasst Hardware- und Softwarekomponenten und basiert auf dem sicherheitsorientierten Betriebssystem OpenBSD[1]. Es ermöglicht die Isolierung und den Schutz von Netzwerken und minimiert die Exponierung von Verbindungspunkten („Angriffsfläche“) zwischen den medizinischen Geräten und dem Krankenhausnetzwerk. mShield sollte auf jedem einzelnen Gerät installiert sein, obgleich es auch möglich ist, ein mShield für mehrere vernetzte Geräte zu verwenden.

Aufgrund seiner Spezifität kann mShield den relevanten Datenverkehr anhand von strengen Regeln auf Gültigkeit prüfen und diesen ausschließlich auf autorisierte Geräte und bestimmte Dienste beschränken. Röntgengeräte nutzen beispielsweise für gewöhnlich DICOM als Hauptkommunikationsprotokoll und nur wenige andere, unterstützende Protokolle. Dank einer Richtlinie, die Pakete standardmäßig ablehnt („default-deny“), und einigen wenigen Firewall-Ausnahmen kann mShield die Modalität wirksam vom Netzwerk entkoppeln und ihre Struktur verstecken, während gleichzeitig die Konnektivität für medizinische Applikationen oder Fernwartung erhalten bleibt.

mShield verhindert die Replikation von Malware über das Netzwerk, stellt die Geräteverfügbarkeit sicher und bietet eine zusätzliche Sicherheitsebene sowie Schutz, wenn das integrierte Betriebssystem des medizinischen Geräts vom Hersteller des Betriebssystems nicht länger unterstützt wird.

Verhindert die Replikation von Malware über das Netzwerk

mShield blockiert nahezu alle typischen netzwerkbasierten Replikationspfade für Viren und Würmer und verhindert so Infektionen. Dieser Ansatz beugt dem größten Problem von Virenscannern vor, die von regelmäßigen und zeitnahen Updates abhängig sind und erst reagieren können, wenn das Virus mit dem System interagiert.

Zwar können medizinische Geräte dennoch durch ein von mShield zugelassenes Netzwerkprotokoll gefährdet werden, das Infektionsrisiko ist jedoch nur gering. Der Grund dafür ist, dass sich Krankenhausumgebungen in verschiedenen Punkten voneinander unterscheiden und medizinische Netzwerke häufig hochspezifisch angepasst werden, wodurch Massen-Malware sich nur schwer überall verbreiten kann. Außerdem richtet mShield zwischen bestimmten Knoten in einem Krankenhausnetzwerk vertrauenswürdige Verbindungen ein und forciert diese, was das Risiko einer massenhaften Ausbreitung von Malware weiter reduziert.

Infektionen sind auch auf Wegen möglich, die mShield umgehen, z.B. Wechselmedien. Das Risiko hierfür hängt von der Verwendungshäufigkeit, den auf den medizinischen Geräten implementierten Sicherheitsvorkehrungen und den Sicherheitsrichtlinien des Krankenhauses ab. Wenn medizinische Geräte jedoch auf einem solchen Weg infiziert werden, verhindert mShield, dass sich das Virus auf anderen Geräten im Netzwerk repliziert, da mShield sowohl eingehende als auch ausgehende Datenpakete prüft.

Gewährleistet die Verfügbarkeit medizinischer Geräte

mShield dient als einziger Zugangspunkt für sämtliche Netzwerkkommunikation vom oder zum geschützten medizinischen Gerät. So kann mShield die Auswirkungen eines Angriffs auf das jeweilige medizinische Gerät absorbieren. Selbst wenn mShield infolgedessen abstürzt, bleibt das Gerät weiterhin funktionsfähig.

Dies macht viele Arten von Angriffen (sowie zufällige Netzwerkanomalien, die das Gerät beeinträchtigen könnten) unmöglich oder wesentlich schwieriger. Das Gerät arbeitet weiter, als ob es vom Netzwerk getrennt wäre, und stellt zur Übertragung von Bildern oder anderen Daten erneut eine Verbindung her, sobald das Netzwerk verfügbar ist.

Eine zusätzliche Sicherheitsebene

mShield blockiert Exploits über das Netzwerk und gewährleistet so eine kontinuierlich hohe Netzwerksicherheit. In der Vergangenheit konnte mShield beispielsweise bereits Malware wie den SASSER-Wurm und die WannaCry-Ransomware erfolgreich blockieren.

Sicherheit für nicht unterstützte Software anderer Anbieter

Vom Hersteller nicht mehr erhältliche und nicht mehr unterstützte Software stellt für Krankenhäuser ebenfalls eine Herausforderung dar. Durch ein Upgrade auf das aktuellste Betriebssystem können Sie die weitere Unterstützung und die Bereitstellung aktueller Sicherheitspatches für Ihr System sicherstellen. Wenn dies aus finanziellen oder technischen Gründen jedoch nicht möglich ist, bietet mShield zumindest eine weitere Sicherheitsebene.

„Ich würde das Gesundheitswesen in Bezug auf die Internetsicherheit immer noch als sehr fragil bezeichnen. Daher müssen wir genau hier ansetzen und sicherstellen, dass Geräte mit Patches und Updates aktualisiert werden können, sie einem Exploit, Angriff oder einer Verletzung der Datensicherheit standhalten können und trotzdem weiterhin sicher und ordnungsgemäß funktionieren. Wir müssen an einen Punkt gelangen, an dem das Krankenhaus selbst, die Hersteller sowie das Gesundheitswesen im Allgemeinen derartige Ereignisse überstehen können, ohne die medizinische Versorgung unterbrechen zu müssen.“[2]

– Dr. Susanne Schwartz, geschäftsführende Direktorin, Office of Strategic Partnerships and Technology Innovation, FDA Center for Devices and Radiological Health.

Nachtrag

Funktionsweise von mShield: technische Beschreibung, Installation und Konfiguration
Philips mShield verwendet Layer-2-Filter sowie ARP-Filter (Address Resolution Protocol) und Layer-3-Filter (SPI, Stateful Packet Inspection) in Kombination mit einem Stealth-Modus (auch Bridging-Modus). Ein Experte erklärt die Funktionsweise wie folgt: „Eine Firewall ist wie eine Tür, von der alle wissen und die alle passieren möchten. Eine Paketfilter-Bridge kann man sich eher wie einen Geheimagenten vorstellen, der im Hintergrund Bedrohungen beseitigt und keinen Gegenangriffen ausgesetzt ist. OpenBSD PF-Bridges können die Sicherheit jeder Netzwerkarchitektur maßgeblich erhöhen.“[3] Die Filterregeln sind an die Kommunikationsanforderungen von medizinischen Geräten von Philips angepasst.

Das mShield Design entspricht den Empfehlungen internationaler Branchenkonsortien wie NEMA, COCIR und JIRA. Sie empfehlen die Verwendung von Firewalls als „wirksame und flexible Tools“ und als Teil einer umfassenden Strategie zur Wahrung der Datensicherheit medizinischer Informationssysteme.[4]

mShield wurde speziell als Systemschutz-Tool auf Geräteebene entwickelt und bietet dadurch viele Vorteile gegenüber breit ausgelegten Sicherheitsvorkehrungen. Als Sicherheitslösung ist mShield mit Host-Firewall-Software-Produkten vergleichbar, punktet jedoch insbesondere hinsichtlich Flexibilität, Wartung und Datensicherheit.

Funktioniert wie ein Ethernet-Switch
Für gewöhnlich verfügen Firewalls über zwei oder mehr Schnittstellen, wobei jede Schnittstelle für ein bestimmtes Subnetz konfiguriert ist. Zusätzlich zur Prüfung und Filterung von Datenpaketen verwaltet die Firewall auch das Routing zwischen diesen Subnetzen. Jeder Computer in einem Subnetz muss die Firewall (des Routers) anhand ihrer IP-Adresse (und MAC-Adresse*) erkennen, um alle für ein anderes Subnetz bestimmten Pakete übermitteln zu können.
* Die MAC-Adresse (Medium Access Controller) hat das Format aa:bb:cc:dd:ee:ff (bei jedem durch Doppelpunkte getrennten Teil handelt es sich um einen Hexadezimalwert im Bereich von 00 bis ff). Die MAC-Adresse ist eine eindeutige Kennung für eine Netzwerkkarte.

Anders als diese gängigen Firewalls ist mShield jedoch kein Router, sondern verhält sich ähnlich wie ein Ethernet-Switch: mShield teilt das Netzwerk nicht in Subnetze. In vielen Fällen ist dies ein Vorteil hinsichtlich Wartung und Administration, beispielsweise auch bei Nachrüstungen. Die geschützten medizinischen Geräte müssen dann nicht neu konfiguriert und es muss ihnen kein dediziertes Subnetz zugewiesen werden.

Unsichtbar
mShield ist im Netzwerk nicht direkt sichtbar, weder anhand einer IP- noch anhand einer MAC-Adresse. Dies verringert seine Angriffsfläche und ermöglicht den wartungsfreien Betrieb über einen langen Zeitraum.

Robust
Das mShield Betriebssystem, OpenBSD, ist als besonders sicheres Netzwerkbetriebssystem bekannt. Für mShield wurde dieses allgemeine Betriebssystem in Größe und Funktionsumfang auf das mögliche Minimum reduziert. So verfügt es beispielsweise nur über die absolut notwendigen Kernel-Treiber und System-Tools und lässt standardmäßig keine interaktiven Benutzeranmeldungen zu. Außerdem wird mShield ausschließlich über den Speicher (RAM-Disk) ausgeführt. Schreibzugriff auf das integrierte Flash-Laufwerk ist nur für Konfiguration und Software-Updates möglich, was in einer stark verbesserten Systemverfügbarkeit und Robustheit resultiert. Dank dieser Architektur bleibt die Integrität der internen Software von mShield auch bei Stromausfällen und Neustarts erhalten, sodass mShield stets zuverlässig in sauberem, funktionsfähigem Zustand startet.

Verwaltung des Netzwerkverkehrs
Netzwerkpakete werden auf verschiedenen Ebenen des TCP/IP-Protokollstacks gefiltert. Standardmäßig blockiert mShield alle Pakete, die nicht IPv4 oder ARP entsprechen. Die IP-Adressen aller geschützten Hosts sind in der mShield Konfiguration gespeichert, was das Filtern auf Basis von IP-Adressen erleichtert. Ein speziell entwickelter ARP-Filter verhindert außerdem ARP-Spoofing (absichtlich oder unbeabsichtigt, z.B. durch eine doppelte IP-Adresse) für die konfigurierten Adressen.

TCP-Kommunikation wird nur mit einem gültigen Satz TCP-Flags übertragen. Alle ungültigen Pakete werden unabhängig von ihrem Ursprung verworfen (z.B. Pakete mit gleichzeitigem SYN- und FIN-Flag). UDP- und ICMP-Pakete werden ebenfalls zustandsabhängig gefiltert.

Die Anzahl an Quellknoten, die eine Kommunikation initiieren (TCP, UDP oder ICMP), wird, soweit sinnvoll, überwacht und begrenzt. Der Einsatz einer maximalen Paketrate verhindert, dass das geschützte medizinische Gerät von Denial-of-Service-Zuständen beeinträchtigt wird. Das bedeutet: Wenn eine Modalität mit mShield geschützt ist und ein Denial-of-Service-Zustand eintritt, wird schlimmstenfalls die Netzwerkverbindung unterbrochen, wenn mShield selbst überlastet ist; die Modalität ist jedoch weiterhin für lokale klinische Arbeitsabläufe verfügbar. Patienten können also weiterhin untersucht werden. Die Datenübertragung findet dann statt, wenn Netzwerk und System sicher sind.

Hardware
Die mShield Hardware wurde mit besonderem Blick auf Sicherheit und Geschäftskontinuität gewählt und entspricht allen länderspezifischen Vorschriften wie CE, UL und CSA. Es handelt sich um eine langlebige Hardware ohne störanfällige mechanische Speichermedien und unzweckmäßige Leistungsmerkmale wie Tastatur oder Video. Die hochwertige Hardware ist für erhöhte Betriebstemperaturen von bis zu 55 °C zertifiziert. Die mShield Hardware eignet sich sowohl für Upgrades älterer medizinischer Geräte als auch für die Integration mit neuen medizinischen Geräten.

Installation und Konfiguration
Zur ordnungsgemäßen Installation und Konfiguration von mShield muss dem Servicetechniker die Netzwerkkonfiguration des medizinischen Geräts, all seiner Komponenten und der Peer-Hosts, mit denen das Gerät kommuniziert, bekannt sein. Die Nutzung vorgegebener Templates (pro System) vereinfacht die ordnungsgemäße Einrichtung von mShield und die Anpassung an veränderte Netzwerkparameter ohne Beeinträchtigung der Netzwerkinteroperabilität.

Servicetechniker verwenden ein kompatibles Philips Service Tool, das alle notwendigen Informationen (einschließlich Versionsinformationen) für die Konfiguration von mShield enthält, Upgrades und die Fehlersuche vereinfacht und Protokolldateien extrahieren kann.

Software-Updates können lokal über die Service Tools oder indirekt über eine Fernverbindung mit dem geschützten medizinischen Gerät durchgeführt werden, je nachdem, ob das Gerät Remote Software Distribution unterstützt, und abhängig von den verfügbaren Funktionen.
Das F&E-Team von Philips beobachtet aktiv potenzielle sowie auftretende Kernel- und Anwendungsfehler und verwendet ein erstklassiges Qualitätssystem zur schnellen Beurteilung und Bereitstellung von Fehlerbereinigungen nach Bedarf.

Konfigurationselemente
Bei der Konfiguration ist es Hauptaufgabe der lokalen Servicetechniker, alle verbundenen Geräte nach Typ und Netzwerkparametern (z.B. IP-Adresse) zu ermitteln. Außerdem müssen die Kommunikationsbeziehungen zwischen Hosts im Netzwerk gemäß der individuellen Situation vor Ort identifiziert und konfiguriert werden, z.B. in Bezug auf die folgenden Elemente:
- NTP (Zeitsynchronisierung)
- Syslog (zentrale Protokollierung/Prozessprotokoll)
- DICOM- oder „Secure DICOM“-basierte PACS- und RIS-Systeme, Drucker, PCR-Reader und andere Geräte
- Philips Remote Services (PRS)

Protokollierung
Die in mShield integrierte syslog-Funktion schreibt alle Protokolldateien in den Speicher (RAM). Die Protokolldateien können vor einer Unterbrechung der Stromversorgung oder dem Neustarten exportiert werden, damit sie nicht verloren gehen. Die Protokolldateien in mShield sind nicht permanent, damit das System jederzeit abgeschaltet werden kann, ohne die Integrität des integrierten Flash-Laufwerks zu gefährden.

Literaturverweise

1 Siehe http://openbsd.org/ sowie die zugehörige BSD-Lizenz unter http://openbsd.org/policy.html
2 „Medical Device Security: The FDA's View.“ Careers Info Security. 9. Juli 2019. https://www.careersinfosecurity.com/medical-device-security-fdas-view-a-12748, aufgerufen am 5. November 2019.
3 Quelle: George Rosamond „Building a more secure network“: http://www.sans.org/rr/whitepapers/modeling/1415.php
4 Quelle: „Defending Medical Information Systems Against Malicious Software“, Dez. 2003, von NEMA (National Electrical Manufacturers Association-USA), COCIR (European Coordination Committee of the Radiological Electrometrical Industry) und JIRA (Japan Industries Association of Radiological Systems): www.nema.org/prod/med/upload/medical-defending.pdf

4522 991 57053 * SEP 2020

So erreichen Sie uns:
Bitte besuchen Sie uns unter www.philips.de/healthcare
healthcare@philips.com