PHILIPS

Ultraschall

Sicherheit

Schützen Sie Ihre medizinischen Geräte vor Verletzungen des Patientendatenschutzes?

Wie jede Branche, die sich auf zunehmend miteinander verbundene Computer-Netzwerke stützt, sieht sich das Gesundheitswesen einer steigenden Anzahl von Sicherheitsverletzungen gegenüber.

Lisa Gallagher, Leiterin des Bereichs für Datenschutz und Datensicherheit bei der Healthcare Information and Management Systems Society (HIMSS), schätzt, dass rund 40 bis 45 Millionen Patientenakten HIPAA-Datenschutzverletzungen zum Opfer gefallen sind.[1] Obwohl es sich bei dieser Zahl um eine Schätzung handelt, da nicht alle Verletzungen gemeldet werden, geht aus einer anderen Studie hervor, dass die Zahl an Datenschutzverletzungen bei Patientenakten zwischen 2012 und 2014 um 138 Prozent gestiegen ist.[2]

Ganz gleich, ob es sich bei diesen Datenschutzverletzungen um Angriffe durch Hacker oder Malware oder um nicht autorisierte Zugriffe handelt – sie stellen eine Bedrohung für die Patientensicherheit und den Datenschutz dar. Außerdem können die Kosten von Datenschutzverletzungen im Gesundheitswesen mehrere Millionen US-Dollar betragen, verursacht u.a. durch Zivilklagen und andere Gerichtsverfahren, ganz zu schweigen von der Rufschädigung für die betroffene Einrichtung.

Eine Herausforderung für Bildgebungssysteme

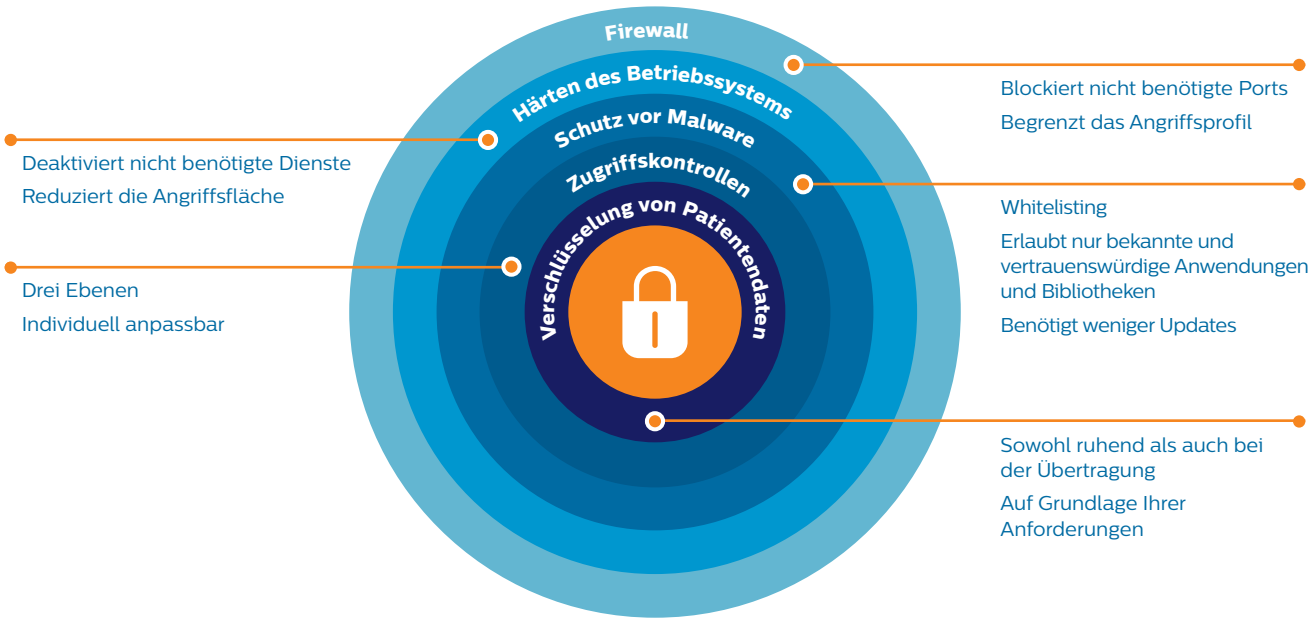
Bildgebungssysteme sind nicht immun gegen diese Angriffe. Die meisten Bildgebungssysteme werden unter dem Gesichtspunkt des klinischen Nutzens entwickelt, unter Vernachlässigung der Tatsache, dass es sich auch um vernetzte Computersysteme handelt, die zu unlauteren Zwecken missbraucht werden können. Dadurch sind medizinische Geräte anfällig und können Angreifern als Eintrittspunkt zum gesamten Versorgungssystem dienen. Darüber hinaus macht die bloße Anzahl der vernetzten medizinischen Geräten die Aufrechterhaltung der Internetsicherheit zu einer überwältigenden Aufgabe. Die HIMSS berichtet, dass „Krankenhäuser und ähnliche medizinische Versorgungseinrichtungen in der Regel 300% bis 400% mehr medizinische Geräte als IT-Geräte besitzen.“[3] Deshalb hat die FDA Richtlinien zur Internetsicherheit für vernetzte medizinische Geräte herausgegeben.[4]

Für Philips Ultrasound hat der Schutz von medizinischen Geräten und der Patientendaten besonders hohe Priorität. Gemeinsam können wir eine sichere Umgebung aufrechterhalten, indem wir wachsam bleiben und die sich ständig verändernden Bedrohungen der Internetsicherheit erkennen. Es ist unser erklärtes Ziel, die spezifischen Bedürfnisse und Anforderungen unserer Kunden zu erfüllen.

Mit der richtigen **Strategie beginnen**

Die Defense-in-Depth-Strategie basiert auf der Idee, dass eine mehrschichtige Verteidigung schwerer zu durchbrechen ist als eine einzelne Barriere und bildet die Grundlage für bewährte Abläufe (Best Practices) im Bereich der Sicherheit von medizinischen Geräten. Geeignete Maßnahmen sind beispielsweise Sicherheitsrichtlinien, Prozessvorgaben, Zugriffskontrollen, technische und organisatorische Maßnahmen, Schulungen und Risikobewertungen.

Defense-in-Depth-Strategie



Sicherheit von CX50 und Sparq Produkten*
Philips Ultrasound hat das Prinzip der „Defense-in-Depth-Strategie“ auf die CX50 und Sparq Ultraschallsysteme angewendet und eine mehrschichtige Sicherheitsstrategie implementiert, die fünf Aspekte umfasst:

- Firewall
- Härten des Betriebssystems
- Schutz vor Malware
- Zugriffskontrollen
- Verschlüsselung von Patientendaten

Jede dieser Maßnahmen spielt eine wichtige Rolle dabei, Hacker abzuwehren, das System vor Malware zu schützen und den unbefugten Zugriff zu verhindern.

Firewall blockiert nicht benötigte Ports
Strenge Firewall-Richtlinien, die alle unnötigen Ports blockieren, unterbinden die Kommunikation mit unbefugten Computern. Das Angriffspotential wird so reduziert.

* Gilt für die Softwareversionen CX50 4.0 und Sparq 2.0 oder höher.

Härten des Betriebssystem deaktiviert nicht benötigte Dienste

Ähnlich wie bei Firewalls werden beim Härten des Betriebssystems alle nicht erforderlichen Services und Funktionen, die im Betriebssystem enthalten sind, identifiziert und solche deaktiviert, die für Ultraschallsysteme nicht erforderlich sind. Durch das Härten des Betriebssystems wird das Angriffspotential reduziert, indem Services beseitigt werden, die mit der Zeit angreifbar werden können. Philips befolgt die von der Defense Information Systems Agency (DISA) herausgegebenen Standard Technical Implementation Guides (STIGs).

Malware-Schutz per Whitelisting bietet Schutz mit geringem Wartungsaufwand

Die klassische Methode zum Schutz vor Malware, die Virenschutz-Software, erfordert regelmäßige Updates, um neuen Viren und Malware, die täglich in Umlauf gebracht werden, gewachsen zu sein. Krankenhäuser laufen Gefahr, angegriffen zu werden, bevor die Virenschutz-Software neue Malware identifiziert und bekämpft hat.

Um dieses Risiko zu senken, hat Philips die McAfee Application Control Lösung implementiert. Diese Lösung, die auch als Whitelisting bekannt ist, schützt Ihre CX50 und Sparq Systeme vor Malware, indem sie nur bekannten und vertrauenswürdigen Anwendungen und Bibliotheken die Ausführung gestattet. Da Whitelisting im Gegensatz zu Virenschutz-Software keine fortlaufenden Aktualisierungen benötigt, sind weniger Wartungsmaßnahmen und Updates erforderlich.

Auf Ihren Bedarf abgestimmte Zugriffskontrollen

Schätzungsweise 22% der Sicherheitsverletzungen seit 2009 sind auf unbefugte Zugriffe zurückzuführen.[2] Zur besseren Kontrolle des Zugriffs auf die Daten Ihrer Ultraschallsysteme bieten CX50 und Sparq die Wahl zwischen drei verschiedenen Zugriffskontrollstufen:

- **Keine Einschränkungen (Vorgabestufe):** Ein klinischer Anwender kann Untersuchungen durchführen und auf frühere und auf dem System gespeicherte Untersuchungen zugreifen, ohne sich anzumelden.
- **Nur Patientendaten werden gesperrt:** Jeder Anwender muss gültige Anmeldedaten eingeben, um auf frühere Untersuchungen zuzugreifen. Notfalluntersuchungen können jedoch ohne Anmeldung vorgenommen werden.
- **Sperrung des gesamten Systems:** Jeder Anwender muss sich erfolgreich anmelden, bevor er eine Untersuchung vornimmt oder auf Patientendaten zugreift.

Verschlüsselung von gespeicherten und übertragenen Patientendaten

Alle Patientendaten, die auf den Festplattenlaufwerken des CX50 und Sparq gespeichert sind, können gemäß den individuellen Anforderungen Ihrer Einrichtung verschlüsselt werden. Darüber hinaus können Sie zur Verschlüsselung von Patientendaten während der Übertragung DICOM mit TLS zur Knotenauthentifizierung ohne Verschlüsselung, DICOM mit Verwendung der TLS-Verschlüsselung oder eine Kombination aus beidem wählen. (Dies erfordert die entsprechende Funktionalität auf Ihrem PACS-System.)

Benutzerverwaltung vereinfacht Kontenpflege

Die CX50 und Sparq Systeme bieten Ihnen die Möglichkeit, mehrere Konten für klinische Anwender und die Krankenhausverwaltung einzurichten. Bei beiden Systemen haben Mitarbeiter der Krankenhausverwaltung die Möglichkeit, Kennwortrichtlinien in Übereinstimmung mit lokalen Datenschutzanforderungen und -richtlinien festzulegen. CX50 und Sparq Systeme lassen sich in Ihre LDAP-Umgebung (Lightweight Directory Access Protocol) einbinden, so dass Anwender und Gruppen mittels Standard-Netzwerkkonten (z.B. Active Directory) authentifiziert werden können.

Audit Logging liefert Daten zur Analyse

Philips Ultrasound hat die Audit Logging Funktionen der CX50 und Sparq Systeme erweitert. Benutzer können das System so konfigurieren, dass die Protokolle zur Aufbewahrung, zum Abrufen und zur weiteren Analyse an einen lokalen Systemprotokoll-Server (Syslog-Server) gesendet werden. Zur Unterstützung der forensischen Analyse können Sie die Einheitlichkeit der Zeitstempel sicherstellen, indem Sie die Zeit auf den Ultraschallsystemen mit Ihrem Netzwerk-Zeitserver synchronisieren.

Optionale Sicherheitsfunktionen

- Firewall-Richtlinie zur Blockierung nicht benötigter Ports

Betriebssystem-Härtung

- Betriebssystem-Einstellungen gemäß den DISA STIGS
- Deaktivierung nicht benötigter Dienste
- Deaktivierung der Autorun-Funktion für Wechselmedien

Schutz vor dem Export auf Datenträger

- Bietet die Möglichkeit, den Export von Patientendaten auf Wechselmedien zu deaktivieren

Zugriffsstufe

- Keine Einschränkungen – Benutzer können Untersuchungen durchführen und auf alle früheren Untersuchungen und MWL-Daten (Modality Work List) zugreifen
- Nur Patientendaten sind gesperrt – Benutzer können Untersuchungen ohne Anmeldung durchführen, müssen sich jedoch anmelden, bevor sie auf frühere Untersuchungen oder MWL-Daten zugreifen können
- Gesamtes System ist gesperrt – Benutzer und Administratoren müssen sich vor jedem Zugriff auf das System anmelden

Richtlinie zur Benutzerverwaltung

- Benutzerverwaltung lokal
  - Lokale Benutzerverwaltung
  - Unterstützung mehrerer eindeutiger Benutzerkonten
  - Unterstützung mehrerer eindeutiger Administratorkonten
- Remote-Benutzerverwaltung
  - Unterstützt Active Directory-Authentifizierung mittels LDAP (System ist möglicherweise nicht mit Domäne verbunden)
  - Unterstützung einzelner Konten oder AD-Gruppen für Benutzer und Administratoren
  - Verwendung von LDAP oder sicherem LDAP möglich
  - Kunde kann das System für die Durchführung einer authentifizierten Bindung konfigurieren

Kennwortrichtlinien

- Möglichkeit, Kennwortrichtlinien für lokale Konten festzulegen
  - Kennwortverlauf (1 bis 8)
  - Mindest-Kennwortlänge (6 bis 14 Zeichen)
  - Maximale Kennwortlänge (6 bis 63 Zeichen)
  - Mindest-Kennwortalter (0 bis 998 Tage)
  - Maximales Kennwortalter (1 bis 999 Tage)
  - Kennwortkomplexität
- Richtlinien für Kontosperrung
  - Grenzwert für Kontosperrung (1 bis 999 Minuten)
  - Dauer der Kontosperrung (1 bis 999 Minuten)
  - Zurücksetzen des Zählers für Kontosperrungen (Minuten)
- Automatische Abmeldung – Benutzer wird nach dem angegebenen Inaktivitätszeitraum automatisch abgemeldet
  - Deaktiviert, 5, 10, 20, 30 oder 60 Minuten*
- Festplattenverschlüsselung
  - 128 Bit
  - 128 Bit mit Diffuser
  - 256 Bit
  - 256 Bit mit Diffuser
- Anmeldebanner/Banner mit rechtlichen Hinweisen
  - Konfigurierbares Anmeldebanner/Banner mit rechtlichen Hinweisen
  - Konfigurierbarer Titel für Anmeldebanner/Banner mit rechtlichen Hinweisen
- Export von Prozessprotokollen
  - Export von Prozessprotokollen mittels syslog möglich
  - Verfügbare Protokolle: UDP oder TLS

Schutz

- Optionaler Schutz vor Malware mit der White-Listing-Lösung von McAfee Application Control

Sicherheit für Behörden

- Konfigurierbare Option zur Bereitstellung aktueller Sicherheitsfunktionen mit kompletter Härtung des Systems zum Schutz der Patientendaten; durch die Option entfällt die Möglichkeit zur Einrichtung und Konfiguration von VPNFunktionalitäten

* Aktive Untersuchung wird unterbrochen.

1. Gallagher L. Presentation. 2012 Boston Privacy and Security Forum.
2. McCann E. HIPAA data breaches climb 138 percent. Healthcare IT News. 6. Februar 2014.
3. Medical Device Security. Healthcare Information and Management Systems Society. http://www.himss.org/resourcelibrary/TopicList.aspx?MetaDataID=1581
4. Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software. U.S. Food and Drug Administration. http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm

www.philips.de/healthcare

Gedruckt in den Niederlanden.
4522 991 58723 * SEP 2020