PHILIPS

Ultraschall

Sicherheit

Sind Ihre medizinischen Geräte und Patientendaten **geschützt**?

Das Gesundheitswesen sieht sich genauso wie andere Branchen, die auf zunehmend vernetzte Computer-Netzwerke angewiesen sind, immer häufiger mit Sicherheitsverletzungen konfrontiert.

Lisa Gallagher, Senior Director für Datenschutz und Datensicherheit der Healthcare Information and Management Systems Society (HIMSS), schätzt die Anzahl der bisher von Verletzungen der HIPAA-Datenschutzbestimmungen betroffenen Patientendatensätze auf 40 bis 45 Millionen.[1] Obwohl es sich dabei um eine Schätzung handelt, da nicht alle Datenschutzverletzungen gemeldet werden, deutet eine andere Studie auf einen Anstieg der Datenschutzverletzungen bei Gesundheitsdaten um 138% von 2012 bis 2014 hin.[2]

Unabhängig davon, ob diese Verletzungen nun auf Hacker, Malware oder unbefugte Zugriffe zurückzuführen sind, stellen sie eine Bedrohung der Patienten- und Datensicherheit dar. Darüber hinaus können sich Verletzungen der Datensicherheit im Gesundheitswesen auf Schäden in Höhe von mehreren Millionen Dollar belaufen, wobei die Kosten durch Zivilklagen und andere rechtliche Schritte weiter steigen und der Ruf der jeweiligen Einrichtung ebenfalls Schaden nimmt.

Herausforderung für Bildgebungsgeräte

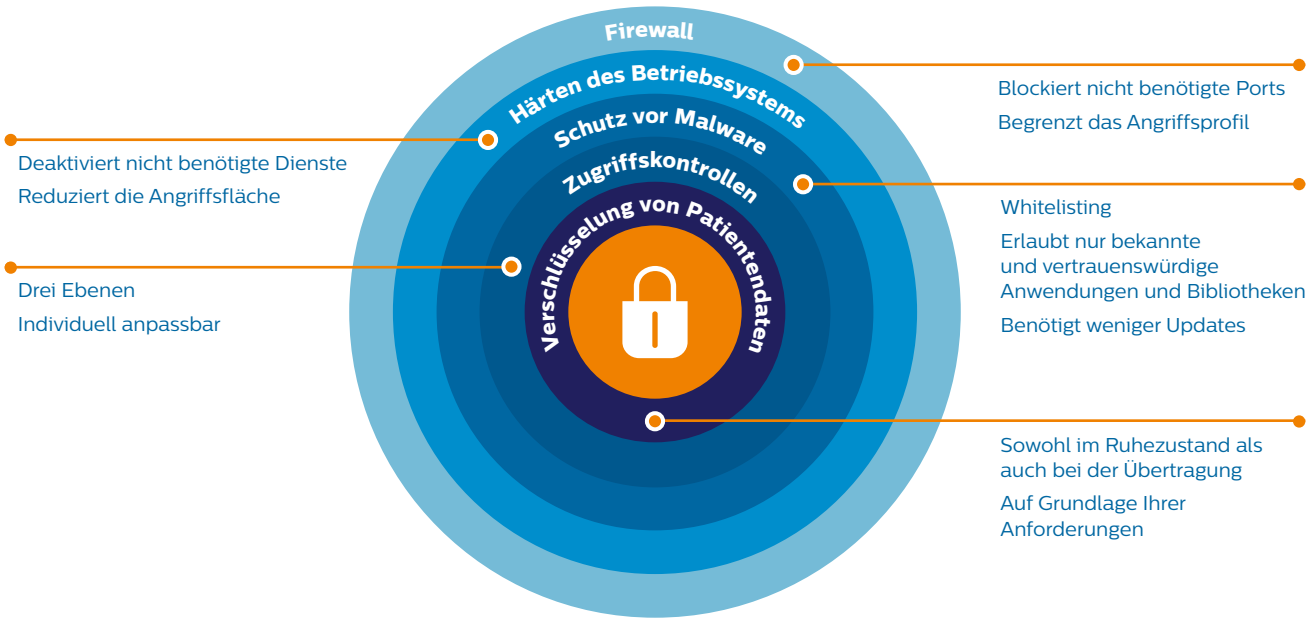
Bildgebungsgeräte sind gegen derartige Angriffe nicht gefeit. Die meisten dieser Geräte wurden in erster Linie für einen größtmöglichen klinischen Nutzen entwickelt. Die Tatsache, dass es sich dabei auch um Computer handelt, die mit einem Netzwerk verbunden und dadurch anfällig für illegale Zugriffe sind, wurde häufig vernachlässigt. Aus diesem Grund dienen Medizinprodukte häufig als Angriffspunkte im Netzwerk von medizinischen Einrichtungen. Zudem wird die Wahrung der Internetsicherheit aufgrund der unzähligen miteinander vernetzten Medizinprodukte zur Herkulesaufgabe. Die HIMSS führt an, dass „Krankenhäuser und ähnliche medizinische Versorgungseinrichtungen üblicherweise 300% bis 400% mehr medizinische Geräte als IT-Geräte besitzen."[3] Deshalb hat die FDA einen Leitfaden für Internetsicherheit bei vernetzten Medizinprodukten herausgegeben.[4]

Philips Ultrasound ist sich bewusst, wie wichtig es ist, dass Ihre Medizinprodukte und Patientendaten geschützt sind. Gemeinsam können wir eine sichere Arbeitsumgebung schaffen, indem wir wachsam bleiben und die sich laufend verändernden Gefahren im Hinblick auf die Internetsicherheit im Auge behalten. Unser Streben ist es, die Bedürfnisse und Anforderungen unserer Kunden zu erfüllen.

Mit der **richtigen Strategie** beginnen

Die Defense-in-Depth-Strategie basiert auf dem Konzept, dass eine mehrschichtige Verteidigung schwieriger zu durchbrechen ist als eine einzelne Schutzmaßnahme. Diese Strategie bildet die Grundlage für bewährte Abläufe (Best Practices) im Bereich der Sicherheit von Medizinprodukten. Die Maßnahmen können beispielsweise Sicherheitsrichtlinien, Prozessvorgaben, Zugriffskontrollen, technische Maßnahmen, Schulungen und Risikobewertungen umfassen.

Defense-in-Depth-Strategie



Sicherheit von EPIQ und Affiniti Produkten

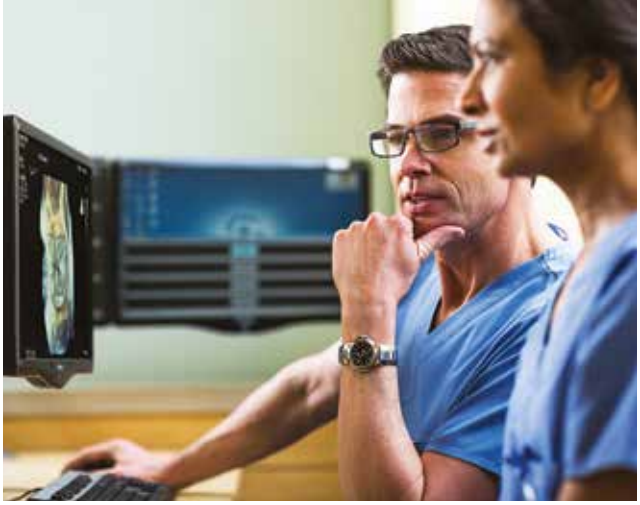
Philips Ultrasound hat das „Defense-in-Depth"-Prinzip auf die EPIQ und Affiniti Ultraschallsysteme angewendet und eine mehrschichtige Sicherheitsstrategie implementiert, die die folgenden fünf Aspekte umfasst:

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

Jeder dieser Aspekte spielt eine wichtige Rolle dabei, Hacker zu behindern, das System vor Malware zu schützen und unbefugte Zugriffe zu verhindern.

Die Firewall blockiert nicht benötigte Ports

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



Bei der Härtung des Betriebssystems werden nicht benötigte Dienste deaktiviert

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

Whitelisting bietet Malware-Schutz bei geringem Wartungsaufwand

Die klassischen Sicherheitsmaßnahmen wie Malware-Schutz und Virenschutzsoftware müssen regelmäßig aktualisiert werden, damit sie in Bezug auf neue Viren und Malware, die tagtäglich in Umlauf gebracht werden, stets auf dem neuesten Stand sind. Krankenhäuser sind gerade vor der Aktualisierung der Virenschutzsoftware der Gefahr eines Malware-Angriffs ausgesetzt.

Um dieses Risiko zu senken, hat Philips die Lösung McAfee Application Control in seine Systeme integriert. Diese Lösung schützt Ihre EPIQ und Affiniti Systeme per Whitelisting vor Malware, d.h., sie lässt ausschließlich bekannte und vertrauenswürdige Anwendungen und Bibliotheken zu. Da die Whitelisting-Lösung nicht wie klassische Virenschutzsoftware laufend aktualisiert werden muss, profitieren Sie von einem geringeren Wartungs- und Aktualisierungsaufwand.

Zugriffskontrollen lassen sich auf Ihre Bedürfnisse zuschneiden

Schätzungen zu Folge sind 22% der Sicherheitsverletzungen seit 2009 auf unbefugte Zugriffe zurückzuführen.[2] Damit Sie den Zugriff auf die auf Ihren Ultraschallsystemen gespeicherten Daten kontrollieren können, bieten EPIQ und Affiniti drei verschiedene Ebenen der Zugriffskontrolle:

- **Keine Einschränkungen (Standardvorgabe):** Klinische Mitarbeiter können ohne Anmeldung Untersuchungen durchführen und auf alle vorherigen auf dem System gespeicherten Untersuchungen zugreifen.
- **Nur Patientendaten sind gesperrt:** Alle Benutzer müssen sich anmelden, bevor sie auf gespeicherte Untersuchungen zugreifen können. Notfalluntersuchungen können jedoch auch ohne Anmeldung durchgeführt werden.
- **Gesamtes System ist gesperrt:** Alle Benutzer müssen sich erfolgreich anmelden, bevor sie einen Scan durchzuführen oder auf Patientendaten zugreifen können.

Verschlüsselung von Patientendaten sowohl im Ruhezustand als auch bei der Übertragung

Alle Patientendaten, die auf den Festplattenlaufwerken der EPIQ und Affiniti Systeme 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.)

Die Benutzerverwaltung vereinfacht die Kontenpflege

EPIQ und Affiniti Systeme bieten Ihnen die Möglichkeit, mehrere Konten für Anwender und Krankenhausverwaltung einzurichten. Bei beiden Systemen haben Mitarbeiter der Krankenhausverwaltung die Möglichkeit, Kennwortrichtlinien in Übereinstimmung mit lokalen Sicherheitsanforderungen und -richtlinien festzulegen. EPIQ und Affiniti Systeme lassen sich in Ihre LDAP-Umgebung einbinden, so dass Anwender und Gruppen mittels Standard-Netzwerkkonten (d.h. Active Directory) authentifiziert werden können.

Audit Logging liefert Daten zur Analyse

Philips Ultrasound hat die Audit-Logging-Fähigkeiten der EPIQ und Affiniti Systeme erweitert. Benutzer können das System so konfigurieren, dass die Protokolle an einen lokalen Systemprotokoll-Server (Syslog-Server) zur Aufbewahrung, Abrufbarkeit und weiteren Analyse gesendet werden. Zur Unterstützung der forensischen Analyse können Benutzer die Einheitlichkeit der Zeitstempel sicherstellen, indem sie die Zeit auf den Ultraschallsystemen mit ihrem Netzwerk-Zeitserver synchronisieren.

Sicherheitsoptionen

Grundausstattung

- 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

Safeguard (zusätzlich erhältliche Option)

- Schutz vor Malware mit der Whitelisting-Lösung McAfee Application Control

Security Plus (zusätzlich erhältliche Option)

- Zugriffsstufe
  - Keine Einschränkungen – Benutzer können Untersuchungen durchführen und auf alle früheren Untersuchungen und MWL-Daten 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 werden nach dem festgelegten 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

* Aktive Untersuchungen werden angehalten.

1. Gallagher L. Präsentation. 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.com/healthcare

Gedruckt in den Niederlanden.
4522 991 16003 * SEP 2020