PHILIPS

Azurion

Cybersicherheit

Cybersicherheit in jeder Ebene Ihres interventionellen Arbeitsplatzes

Zum Schutz Ihres interventionellen Arbeitsplatzes wendet Philips die Methoden „Secure by Design“ und „Defense in Depth“ an. In diesem Dokument werden beide Methoden sowie die Lösungen erläutert, die die Arbeitsweise des auf mehreren Ebenen angelegten Systems zur Wahrung der Datenvertraulichkeit und der Systemintegrität ausmachen.

Die Herausforderung

Fortschritte bei der bildgeführten Therapie verlangen eine gleichermaßen ausgereifte Strategie hinsichtlich Cybersicherheit

Es ist vielleicht überraschend, dass die Revolution im Hinblick auf vernetzte Medizinprodukte trotz aller Vorteile noch in den Kinderschuhen steckt. Immer ausgereiftere Produkte und Lösungen erfüllen höhere Anforderungen in punkto Benutzerfreundlichkeit für die Klinikteams und Mitarbeiter. Bahnbrechende Neuerungen, die zur Verbesserung der klinischen Ergebnisse beitragen, sind nun in effizienteren Abläufen integriert und dank reibungsloser Arbeitsabläufe erhalten die Klinikteams direkten Einblick in die relevanten Daten.

Dieses White Paper veranschaulicht, wie sich die weitreichenden Vorteile von vernetzten bildgebenden Geräten in eine hochentwickelte Strategie für Cybersicherheit umsetzen lassen. Wir führen Sie durch diese Strategie und erläutern die Technologien, die die Cybersicherheit Ihres Azurion Systems wahren (siehe Kästchen über Azurion).

Ein zunehmend höherer Entwicklungsstand bedeutet auch, dass Hacker mehr Möglichkeiten zum Eindringen in Ihr System finden, während es für sie hierzu auch immer mehr Anreize gibt. Jüngsten Studien zufolge haben vertrauliche Patientendaten auf dem Schwarzmarkt einen 50 Mal höheren Wert als Finanzdaten.[1] Dies bedeutet, dass Ihr Ziel, eine ausgezeichnete Versorgung bereitzustellen, Kriminellen eine Eintrittsstelle bietet.

Da unser Ziel ein offenes, reibungslos funktionierendes interventionelles Labor ist, das Ärzten und Patienten dient, haben wir Sicherheitslösungen geschaffen, die auch diesen Anforderungen gerecht werden.

Für Philips Image Guided Therapy hat der Schutz von Medizinprodukten und Patientendaten besonders hohe Priorität. Gemeinsam können wir eine sichere Umgebung aufrechterhalten, indem wir wachsam bleiben und die sich ständig verändernden Bedrohungen der Cybersicherheit erkennen. Es ist unser erklärtes Ziel, die spezifischen Bedürfnisse und Anforderungen unserer Kunden zu erfüllen. Unsere Sicherheitspläne berücksichtigen Ihre Mitarbeiter, Prozesse und Technologien mit dem Ziel, die Vertraulichkeit, Integrität und Verfügbarkeit von kritischen Daten zu wahren – unabhängig davon, ob sie sich im Ruhezustand oder in der Übertragung befinden.

Jüngsten Studien zufolge haben ***vertrauliche Patientendaten auf dem Schwarzmarkt einen 50 Mal höheren Wert*** *als Finanzdaten.*

Worum handelt es sich bei der Azurion Plattform für bildgeführte Therapie?

Philips Azurion ist die Plattform für bildgeführte Therapie der jüngsten Generation, mit der Sie Verfahren bei höchster Benutzerfreundlichkeit und mit zahlreichen Integrationsmöglichkeiten einfach und zuverlässig durchführen können, sodass Sie die Leistungsfähigkeit Ihres Labors steigern und Ihren Patienten eine erstklassige Versorgung bieten können.

Die Denkweise

Secure by Design – Sicherer Entwicklungslebenszyklus (Secure Development Lifecycle, SDLC) von Philips

Branchentrends haben gezeigt, dass sich Cyberangriffe auf die Anwendungsebene von Produkten verlagern und eine erhebliche Bedrohung für Kunden- und Patientendaten über das Internet der Dinge (IoT) darstellen. Laut der vom Internet Storm Center erfassten Daten geschehen über 70% der Netzwerkangriffe auf der Anwendungsebene.

Wir stärken die Cyberresilienz unserer Produkte und Dienstleistungen durch Anwenden von Funktionen, Komponenten und Techniken, einschließlich Praktiken, gemäß ISO-Normen (siehe Kästchen). Dies ist eine praktische und wohl erprobte Maßnahme zur Einbindung von Sicherheit und Datenschutz in den Software-Entwicklungsprozess.

Durch Nutzen dieser Methodologie werden Anforderungen und Kontrollen in jeder Phase des sicheren Entwicklungslebenszyklus behandelt, darunter auch die Verwendung von Sicherheitsrisikobewertungen der Produkte, Prozesse der Datenschutzfolgenabschätzung (DSFA), statische Codeanalysen, Analysen von Software-Materiallisten anderer Anbieter, ethische Penetrationstests und fortlaufende Schulungen zur Produktsicherheit in der gesamten Philips Organisation. Während Tools und Prozesse für Philips SDLC von entscheidender Bedeutung sind, stellt „Secure by Design“ eine Denkweise dar, die ein ganzheitliches Konzept von Anfang bis Ende erfordert. Es beginnt bei der Architektur und dem allgemein gehaltenen Design und reicht bis hin zu Codierung, Tests und Unterstützung nach Markteinführung.

Für den interventionellen Arbeitsplatz insbesondere umfasst dies 20 verschiedene Bereiche, u.a.: Autorisierung, Auditprüfungen, Notfallzugriff, Datenintegrität und -authentizität, Vertraulichkeit der Speicherung (Verschlüsselung im Ruhezustand) sowie Vertraulichkeit/Integrität der Übertragung (Verschlüsselung bei Übertragung). Diese Bereiche entsprechen anerkannten Sicherheitsframeworks und -standards weltweit.

Sicherheitsstandards einschließlich, aber nicht beschränkt auf:

- IEC 80001
- ISO 27001
- ISO 27034
- ISO 27002
- ISO 27018
- NIST SP 800-53

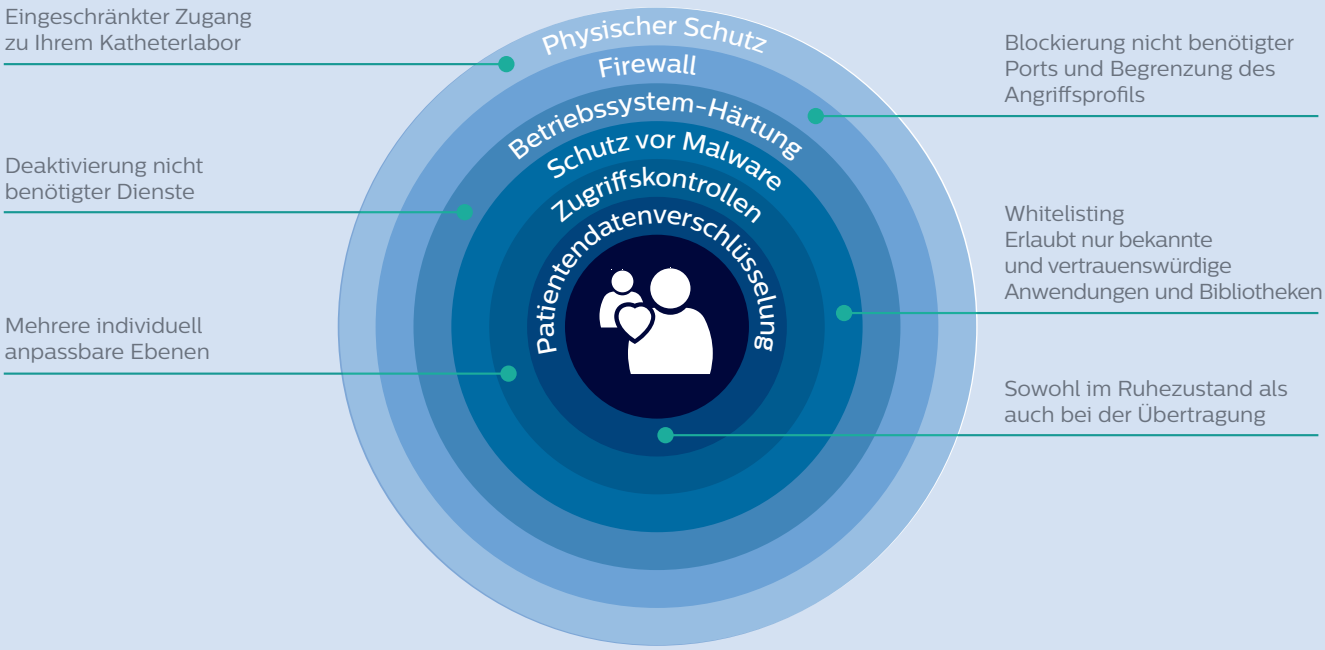
Die Strategie

Defense in Depth

Ihr Krankenhaus ist sicherlich mit dem Schweizer-Käse-Modell bezüglich der Patientensicherheit vertraut, wobei kumulative Maßnahmen eine Bedrohung des Lebens des Patienten verhindern. Die Strategie „Defense in Depth“ ist genau die gleiche Strategie: Auch wenn eine Maßnahme fehlschlägt, wehren mehrere andere Maßnahmen den Angriff ab. Als Folge werden Angriffe abgewehrt, die sich möglicherweise aus verschiedenartigen Vektoren ergeben.

Das unten stehende Diagramm zeigt, dass eine mehrschichtige Verteidigung schwieriger zu durchbrechen ist als eine einzelne Barriere. Diese Strategie bildet die Grundlage für bewährte Abläufe (Best Practices) im Bereich der Sicherheit von medizinischen Geräten. Die Maßnahmen können beispielsweise Sicherheitsrichtlinien, Prozessvorgaben, Zugriffskontrollen, technische Maßnahmen, Schulungen und Risikobewertungen umfassen.

Viele dieser Kontrollmaßnahmen sind standardmäßig integriert. Bei anderen Maßnahmen arbeiten wir eng mit Ihnen zusammen, um den Schutz Ihrer Patientendaten zu optimieren.



Ebenen im Einklang

Jede Ebene der Strategie „Defense in Depth“ stellt einen wirksamen Baustein an sich dar. Ihr Zusammenspiel trägt indes zur Optimierung der Cybersicherheit Ihres Krankenhauses bei. Alle Ebenen wirken zusammen, um den Gefährdungsgrad einzuschränken. Dazu gehören:

- **Physischer Schutz**
- **Firewall**
- **Betriebssystem-Härtung**
- **Schutz vor Malware**
- **Zugriffskontrollen**
- **Patientendatenverschlüsselung**

Jede dieser Maßnahmen spielt eine wichtige Rolle dabei, Hacker-Angriffe abzuwehren, das System vor Malware zu schützen und unbefugten Zugriff zu verhindern. Wir erläutern jede einzelne Maßnahme und beleuchten den jeweiligen besonderen Stellenwert, den sie in Bezug auf die Cybersicherheit Ihres interventionellen Arbeitsplatzes einnimmt.

Physischer Schutz

Angriffe können durch entsprechende Software- und Hardwaremaßnahmen ganz entscheidend eingedämmt werden. Diese Ebene sorgt dafür, dass menschliches Verhalten, die Prozesse im Krankenhaus und die Logistik Ihre Systeme in punkto Sicherheit angriffssicher machen. Wir arbeiten eng mit Ihnen zusammen und schauen uns die physischen Aspekte an, zum Beispiel ob Labore geeignet platziert sind, Mitarbeiterprotokolle vorhanden sind und ein allgemeines Bewusstsein vorherrscht, um die Sicherheit für Ihre gesamten interventionelle Arbeitsplätze zu verbessern.

Firewall blockiert nicht benötigte Ports

Strenge Firewall-Richtlinien schränken den Datenverkehr vom und zum Katheterlabor ein, indem alle unnötigen Ports blockiert werden und die Kommunikation mit unbefugten Computern unterbunden wird. Das Angriffspotential für Hacker wird so reduziert.

Härten des Betriebssystems 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 Katheterlaborsysteme 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).

Betriebssystem-Patching

Was heute als sicher gilt, ist morgen schon nicht mehr sicher. Betriebssystem-Patching sorgt dafür, dass die neuesten Patches sorgfältig validiert sowie zeitgerecht und regelmäßig zur Verfügung gestellt werden. Ihr interventioneller Arbeitsplatz verfügt somit stets über die neueste Sicherheitsstufe.

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 Whitelisting-Lösung in seine Systeme integriert. Diese Lösung schützt Ihr Azurion System per Whitelisting vor Malware, d.h., sie lässt ausschließlich bekannte und vertrauenswürdige Anwendungen und Bibliotheken zu. Da die Whitelisting-Lösung nicht wie klassische Virenschutzsoftware fortlaufend aktualisiert werden muss, profitieren Sie von einem geringeren Wartungs- und Aktualisierungsaufwand.

Auf Ihren Bedarf abgestimmte Zugriffskontrollen

Schätzungen zufolge sind 22% der Sicherheitsverletzungen seit 2020 auf unbefugte Zugriffe zurückzuführen.[2] Damit Sie den Zugriff auf die in Ihren Bildgebungssystemen gespeicherten Daten kontrollieren können, bietet Azurion zwei verschiedene Ebenen der Zugriffskontrolle:

- Authentifizierter Zugriff: Alle Benutzer müssen sich erfolgreich anmelden, bevor sie einen Scan durchführen oder auf Patientendaten zugreifen können.
- Direkter Zugriff: Ein klinischer Benutzer kann Untersuchungen durchführen und auf frühere und auf dem System gespeicherte Untersuchungen zugreifen, ohne sich anzumelden.

Azurion bietet Ihnen die Möglichkeit, mehrere Konten für Benutzer und Krankenhausverwaltung einzurichten. Bei beiden Systemen haben Mitarbeiter der Krankenhausverwaltung die Möglichkeit, Kennwortrichtlinien in Übereinstimmung mit lokalen Sicherheitsanforderungen und -richtlinien festzulegen.

Verschlüsselung von gespeicherten und übertragenen Patientendaten

Alle Patientendaten, die auf den Festplattenlaufwerken des Azurion Systems gespeichert sind, werden bei den meisten Azurion Systemen standardmäßig verschlüsselt (je nach lokalen Bestimmungen). Darüber hinaus können Sie zur Verschlüsselung von Patientendaten während der Übertragung entweder DICOM mit TLS zur Knotenauthentifizierung ohne Verschlüsselung, DICOM mit Verwendung der TLS-Verschlüsselung oder eine Kombination aus beidem wählen. (Dies setzt die entsprechende Funktionalität auf Ihrem PACS-System voraus.)

Sicherheitskernfunktionen
Im Folgenden finden Sie eine Auflistung der technischen Funktionen, die in unseren Interventionslaboren integriert sind und die mit jeder neuen Version stetig weiterentwickelt werden.

- Firewall-Richtlinie zur Blockierung nicht benötigter Ports
- Betriebssystem-Härtung
  – Betriebssystemeinstellungen gemäß den DISA STIGS
  – Deaktivierung nicht benötigter Dienstleistungen
  – Deaktivierung der Autorun-Funktion für Wechselmedien
- Schutz vor dem Export auf Datenträger
  – Bietet die Möglichkeit, den Export von Patientendaten auf Wechselmedien zu deaktivieren
- Schutz vor Malware mithilfe von Whitelisting-Lösungen
- Zugriffsstufe
  – Keine Einschränkungen
  – Nur Patientendaten sind gesperrt – Benutzer können Untersuchungen ohne Anmeldung durchführen, müssen sich jedoch erfolgreich anmelden, damit sie auf frühere Untersuchungen zugreifen können
  – Gesamtes System ist gesperrt
  – Benutzer und Administratoren müssen sich vor jedem Zugriff auf das System erfolgreich anmelden
- Richtlinie zur Benutzerverwaltung
  – Lokale Benutzerverwaltung
  – Unterstützung von eindeutig zugeordneten Benutzerkonten
  – Unterstützung von eindeutig zugeordneten Administratorkonten
  – Verwaltung der Funktionen für Fernzugriff
- Kennwortrichtlinien – bietet die Möglichkeit, Kennwortrichtlinien für lokale Konten festzulegen
- Verschlüsselung von Festplattenlaufwerken – AES-128 und AES-256
- Export von Audit-Logs – Audit-Logs können mit syslog exportiert werden – verfügbare Protokolle: UDP oder TLS

Dienstleistungen, die Ihre Cybersicherheit wahren

Das Ausschlaggebende jeder Strategie zur Cybersicherheit besteht darin, sicherzustellen, dass Ihre Hardware und Betriebssysteme auf dem neuesten Stand sind. Wir stellen Hardware- und Software-Upgrades über unseren Technology Maximizer Vertrag bereit und führen einmalige Betriebssystem-Upgrades durch. Diese bieten unverzügliche Sicherheitsvorteile und andauernden Schutz durch Software- und Hardware-Upgrade-Vereinbarungen. Darüber hinaus haben sie den weiteren Vorteil, die klinischen Ergebnisse und die Sicherheit Ihres Krankenhauses zu verbessern.

Weitere Informationen unter:
www.philips.com/technology-maximizer

Unser Engagement

Kontinuierliche Entwicklung der Cybersicherheit

Um der Verpflichtung nachzukommen, die Sicherheit unserer Produkte zu verbessern, hat sich Philips verschrieben, das bestehende Produktsortiment fortlaufend zu überprüfen und weiterzuentwickeln, um den Anforderungen unserer auf Sicherheit bedachten Kunden optimal gerecht zu werden. Wir setzen alles daran, die Produkte der Zukunft auf der Basis fundamentaler Sicherheitsprinzipien zu konzipieren.

Wir werden auch weiterhin eng mit Anbietern, IT-Unternehmen und Kunden zusammenarbeiten, um flexible Lösungen für aktuelle Probleme zu finden, während wir bereits an neuen Produkten mit integrierter Sicherheit arbeiten.

Wenn Sie weitere Informationen erhalten möchten, senden Sie eine E-Mail an: productsecurity@philips.com

1 Laut Cybersecurity Ventures haben personenbezogene Gesundheitsdaten auf dem Schwarzmarkt einen 50 Mal höheren Wert als Finanzdaten. Gestohlene Patientenakten erzielen mehr als 50 US-Dollar pro Akte (10 bis 20 Mal höher als Kreditkartendaten). https://www.forbes.com/sites/insights-intelai/2019/02/11/confronting-one-of-healthcares-biggest-challenges-cyber-risk/

2 Im Jahr 2020 machte die Verwendung gestohlener Zugangsdaten 22% der Datenschutzverletzungen aus. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

4522 991 63583 * DEC 2020

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