PHILIPS

Services and Solutions Delivery

Operative Intelligenz

Ihre Cybersicherheitsstrategie für Medizinprodukte

Executive Briefing

Erkennen der Sicherheitsherausforderungen von Medizinprodukten und wie man ihnen begegnet

„Cybersicherheit steht beim Übergang zur vernetzten Versorgung im Mittelpunkt."

Jeroen Tas, Chief Innovation & Strategy Officer, Philips

Heutzutage sind viele Medizinprodukte wie spezialisierte Computer konstruiert. Fügen Sie den Wunsch von Ärzten hinzu, von einer Vielzahl von Geräten und Orten aus auf Patientendaten zugreifen zu können, und ist es keine Überraschung, dass Medizinprodukte immer mehr Platz im typischen Gesundheits-IT-Netzwerk einnehmen.

Da die Anforderungen zur Gewährung der Patientensicherheit, zur Bereitstellung eines bequemen Zugriffs auf Informationen und Bilder für Ärzte und zur Wahrung der Medizingerätesicherheit zusammenwachsen, stehen IT-Experten und den Wandel vorantreibende Führungskräfte im Gesundheitswesen vor neuen Herausforderungen. Zu diesen Herausforderungen gehören:

- Wie stellen wir die Sicherheit von Medizinprodukten sicher, wenn Behandler auf Patienteninformationen und Bilder auf einer Vielzahl
- Was sind die wahrscheinlichsten Ursachen für Cyberangriffe und die höchsten Risiken für Daten – und wie schützen wir uns davor?
- Wie können wir unsere Ziele zur Senkung der Betriebskosten durch Minimierung von Einzellösungen in unserer Unternehmensarchitektur bei der Anbindung an regulierte Medizinprodukte erreichen?
- Wie können wir unsere Geräte- und Systemanbieter bei der unterschiedlichen Umsetzung bewährter Sicherheitspraktiken durch die Hersteller bewerten und feststellen, wo sie stehen?
- Effektivität und Daten- und Systemsicherheit für unsere vernetzten Medizinprodukte gemäß IEC 80001-1?

Warum ist Sicherheit bei Medizinprodukten eine so große Herausforderung?

Bei Medizinprodukten müssen Sicherheitsupdates, Patches und potenzielle Virensignaturen vom Gerätehersteller ordnungsgemäß bewertet werden, bevor sie sicher verwendet werden können. Dieser Validierungsprozess dauert mindestens 3 Monate ab dem Zeitpunkt der Veröffentlichung des Sicherheitsupdates. Diese Sicherheitsupdates werden auch häufig von Hackern analysiert, um zu sehen, ob Schwachstellen ausgenutzt werden können. Diese Kombination aus langen Verfahrenszeiträumen und intensiver Sichtbarkeit der Sicherheitsupdates für Hacker macht es schwierig, die Sicherheitsmaßnahmen in Echtzeit ausreichend auf dem neuesten Stand zu halten, was die Wahrscheinlichkeit von Sicherheitsvorfällen erhöht. Die Sicherung und der Schutz von Medizinprodukten ist daher eine Aufgabe, der rund um die Uhr nachgegangen werden muss.

So schützen Sie Medizinprodukte und ergreifen Maßnahmen zur Entwicklung einer unternehmensweiten Resilienzstrategie

Um Medizinprodukte zu sichern und zu schützen, empfiehlt der NHS (der britische National Health Service) die folgenden Schritte. Es ist wichtig, dass sie für alle mit dem Netzwerk verbundenen Geräte unabhängig vom Betriebssystem gelten.

Schritt 1:

Identifizieren Sie die Medizinprodukte in der Organisation

Erfassen Sie alle Geräte im Bestand, einschließlich vollständiger Details zusammen mit Betriebssysteminformationen. Diese Prüfung sollte zur Erstellung einer vollständigen Netzwerktopologie führen, die zeigt, wie die betroffenen Geräte mit zugehörigen Geräten und Diensten kommunizieren und wie der Zugriff für die Bereitstellung von Remote-Updates ermöglicht werden kann, wenn dies für das betreffende Gerät angemessen ist. Beispiele für Geräte können MRT-Scanner, tragbare Vitalparametermonitore und Spritzenpumpen sein; sie können sich auf die Richtlinie 93/42/EWG des Europäischen Rates beziehen, die die Definition eines Medizinprodukts festlegt.

Schritt 2:

Entwickeln und wenden Sie einen Schadensbegrenzungsplan an

Erstellen Sie einen effektiven Begrenzungsplan, der die folgenden Ansätze kombiniert:
Reduzieren Sie die Gefährdung, indem Sie verhindern, dass die Geräte auf nicht vertrauenswürdige Inhalte zugreifen (was es bösartigen Inhalten effektiv erschwert, das Gerät zu erreichen und auszunutzen).
Reduzieren Sie die Auswirkungen einer Kompromittierung, indem Sie den Zugriff auf sensible Daten oder Dienste von anfälligen Geräten verhindern (so wird der Schaden selbst bei einer Kompromittierung der Geräte minimiert).

Schritt 3:

Reduzieren Sie die Wahrscheinlichkeit einer Datenschutzverletzung

- Verhindern Sie den Zugriff von nicht vertrauenswürdigen Diensten
- Verhindern Sie den Zugriff auf Wechsel-medien oder schränken Sie ihn ein
- Schränken Sie den Netzwerkzugriff ein Entfernen Sie unnötige Dienste Schränken Sie den Fernzugriff ein
- Entfernen Sie den Zugriff auf Dienste (Zugriffsebenen einschränken)
- Richten Sie Zonen und Unterbrechungen in Netzwerken ein
- Richten Sie eine effektive und proaktive Schutzüberwachung ein
- Stellen Sie eine ordnungsgemäße Anti-Malware- und Angriffserkennung sicher

Schritt 4:

Verwenden Sie eine Benutzerverwaltung

Verwalten Sie Benutzerkonten während des gesamten Lebenszyklus sorgfältig; zum Beispiel durch das Löschen von Konten, wenn Mitarbeiter ausscheiden oder den Arbeitsplatz wechseln. Erstellen Sie ein Verfahren zur Reaktion auf Vorfälle.

Schritt 5:

Arbeiten Sie mit Dritten zusammen und verstehen Sie Zusammenhänge richtig

Berücksichtigen Sie die Sicherheit von Drittorganisationen und priorisieren Sie bei der Auftragsvergabe Support und Sicherheit. Wie schnell sollten Sie beispielsweise im Falle eines Sicherheitsvorfalls Support-Techniker vor Ort haben, um Gegenmaßnahmen zu ergreifen? Wie schnell sollte ein Patch nach der Veröffentlichung und dem Test auf ein Medizinprodukt angewendet werden, das dieser betrifft? Wenn Sie diese Angaben in Verträge aufnehmen, können Sie Ihre eigenen Sicherheitsanforderungen leichter im Auge behalten.

Schritt 6:

Überprüfen Sie regelmäßig Ihren Bestand an Medizinprodukten

Warum sollten Sie mit Philips zusammenarbeiten, um eine hochmoderne Cybersicherheitsstrategie zu definieren und zu implementieren?

Die Sicherheitsprogramme der Hersteller sind entscheidend, um sicherzustellen, dass Sicherheit und Datenschutz von Anfang an im Mittelpunkt stehen. Vor kurzem hat die FDA eine Empfehlung herausgegeben, dass Hersteller von Medizinprodukten und Gesundheitseinrichtungen Sicherheitsvorkehrungen treffen sollten, um das Risiko von Cyberangriffen zu verringern, was die Notwendigkeit gut konzipierter Programme weiter unterstreicht. Sicherheitsprogramme müssen einige grundlegende Elemente enthalten, um erfolgreich zu sein:

Philips fördert die konsequente Anwendung von Strategien zur proaktiven Bewältigung von Risiken und Bedrohungen, einschließlich der im Bereich der Cybersicherheit oft als „die drei Todsünden" bezeichneten:

Sicherheit von Anfang an

Passwortrisiko:
das Risiko eines fehlenden starken Identitäts- und Berechtigungsmanagements, z. B. Multifaktor-Authentifizierung

Verschlüsselungsrisiko:
das Risiko eines Mangels an starker Ende-zu-Ende-Datenverschlüsselung – von der Quelle, an der die Daten erzeugt werden, über das Netzwerk bis zur Speicherung in einem Rechenzentrum – und/oder wirksame Lösungen zur Verhinderung von Datenverlust

Patch-Management-Risiko:
das Risiko eines fehlenden effektiven Patch-Managements, das beispielsweise in alten Betriebssystemen Schwachstellen schafft

Geprägt durch die Leitprinzipien von „Security by Design“

Die ganzheitliche Strategie von Philips basiert auf den Leitprinzipien von „Security by Design“. Wir vereinen die Leistungsfähigkeit unserer Mitarbeiter, Prozesse und Technologien, um die Vertraulichkeit, Integrität und Verfügbarkeit kritischer klinischer und personenbezogener Daten über den gesamten Versorgungszyklus hinweg zu schützen. Wir wissen, dass Ihre Cybersicherheit nur so stark ist wie ihr schwächstes Glied. Unser Ziel ist es daher, sicherzustellen, dass die klinischen Patientenüberwachungsnetzwerke und Systeme von Philips kein Angriffspunkt sind.

Der Ansatz des Philips-Sicherheitsprogramms deckt alle acht grundlegenden Elemente ab und beginnt mit einer soliden Strategie, Steuerung und Richtlinien. Laufende Aus- und Weiterbildung sind ebenso erforderlich wie Audits und Bewertungen.

Darüber hinaus umfasst die Produktentwicklung für medizinische Geräte von Philips detaillierte Risikobewertungen und Schwachstellentests, die die Kunden-Umgebung nachbilden. Da sich Bedrohungen ständig weiterentwickeln, verfügen wir über Programme zur Vorfallbehandlung sowie Metriken, Überwachung und Kommunikation, um Sie auf dem Laufenden zu halten.

Gal Gnainsky von Philips Group Security erklärt:
„Wir haben Jahre damit verbracht, ein robustes Ende-zu-Ende-Programm „Security by Design“ aufzubauen und in dieses zu investieren, welches Sicherheitsprinzipien und Best Practices während des gesamten Produktlebenszyklus einbettet. Wir wissen, dass unsere Kunden hohe und wachsende Erwartungen an die Sicherheit der Lösungen haben, auf die sie sich verlassen. Darüber hinaus haben die globalen Regulierungsbehörden den Umfang und das Ausmaß der Compliance-Anforderungen für die Cybersicherheit von Produkten erhöht, um Patienten und Verbraucher zu schützen. Wir freuen uns darauf, diese wichtigen Verpflichtungen weiterhin zu erfüllen.“

Umfassende Services für eine umfassende Cybersicherheitsstrategie

Security by Design geht über Produkte und Netzwerke hinaus. Mit der Philips-Lösung „Security by Design" können Sie aus einer umfassenden Palette von Diensten wählen, um Ihr Patientenüberwachungsnetzwerk, Ihre Systeme und Geräte auf dem neuesten Stand zu halten, mit Spitzenleistung zu arbeiten und vor der ständigen Bedrohung durch Cyberangriffe zu schützen. Diese umfassen:

Philips Security Center of Excellence

Das Philips Security Center of Excellence wurde 2015 ins Leben gerufen, um durch Security by Design, Risikobewertung, Schwachstellen- und Penetrationsbewertung, spezielle Schulungen und Reaktion auf Vorfälle cyberresistente Produkte und Dienstleistungen zu entwickeln.

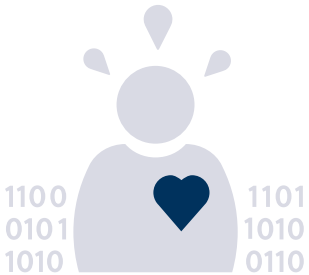
Zertifiziert von Underwriters Laboratories

Philips hat in 2020 auch als erster Hersteller von Medizinprodukten eine neue Zertifizierung für Cybersicherheitstests von Underwriters Laboratories (UL) erhalten. Underwriters Laboratories (UL) ist ein unabhängiges globales Sicherheitszertifizierungs- und Prüfunternehmen mit weltweiten Standorten.

Die UL IEC 62304-Zertifizierung wurde von Underwriters Laboratories entwickelt, um einen Gesamtrahmen zur Bewertung der Robustheit und Reife der Cybersicherheitsmaßnahmen und -fähigkeiten eines Medizinprodukteherstellers für die Produktentwicklung bereitzustellen.

Zur Unterstützung der erfolgreichen Firmenregistrierung von Philips für die Sicherheitsoption IEC 62304 führte UL ein umfassendes Audit des Philips Security Center of Excellence durch. Das Audit überprüfte und verifizierte zentrale Produktsicherheitsprozesse des Philips Security Center of Excellence, einschließlich Sicherheitsrisikomanagement und Risikokontrollmaßnahmen, Planung der Softwaresicherheitsverifizierung, Änderungsmanagement und kontinuierliche Verbesserung sowie das Qualitätsmanagementsystem des Testlabors des Centers.

Die UL-Zertifizierung kombiniert Cybersicherheitstestelemente des etablierten UL 2900-2-1 Standards für Software-Cybersicherheit für netzwerkfähige Produkte, der sich auf die anspruchsvollen Anforderungen von Gesundheits- und Wellnesssystemen sowie Sicherheitsprinzipien aus internationalen Standards (ISO 13485 und ISO14971) konzentriert.



Philips Patientenüberwachung

Philips Patientenüberwachung ist ein reguliertes medizinisches IT-System, das eine kontinuierliche Überwachung und Kommunikation der Vitalwerte von Patienten ermöglicht und gleichzeitig die Anforderungen an Verwaltbarkeit, Wartungsfreundlichkeit und Sicherheit erfüllt. Folgende Medizinprodukte sind in unserer Sicherheitslösung enthalten:

- Patienteninformationszentrum iX (PIC iX) B.02 und höher
- IntelliVue Bettmonitore Release M und höher
- IntelliSpace Intensivpflege und Anästhesie (ICCA)
- CareEvent B.01 und höher
- IntelliSpace Perinatal (nur Integrationstest)
- CompuRecord (nur Integrationstest)

Der Ansatz von Philips Patientenüberwachungssystemen zum Schutz von Patienten, medizinischen Geräten und Informationen umfasst:

Lebenszyklusverwaltung
Wenn neue Software oder ein Betriebssystem veröffentlicht werden, geben wir das Supportendedatum für von Ihnen verwendete ältere Produkte bekannt. Dies gibt Ihnen Zeit, Ihr Budget und Upgrades zu planen und das Risiko nicht unterstützter Medizinprodukte und Betriebssysteme zu vermeiden.

Sicherung des klinischen Netzwerks
Wir bieten bewährte, produktspezifische Sicherheitsempfehlungen, um die kabelgebundenen und drahtlosen Geräte des IntelliVue-Patientenüberwachungssystems effektiv zu schützen.

Systemhärtung
Umfasst Planung, Testen, Implementieren und Auditieren von Patch-Management-Software und Schutz vor vom Hersteller offengelegten Schwachstellen. Schaffen Sie Vertrauen bei den IT-Stakeholdern. Das Philips PIC iX System implementiert Sicherheitshärtung basierend auf den Security Technical Implementation Guides (STIGs) des US-Verteidigungsministeriums. Die anwendbaren STIGs beinhalten, sind aber nicht beschränkt auf: Windows®-Betriebssystem, .NET, SQL und Internet Explorer®.

Sicherheitsbewertung und Penetrationstests
Mit zwei Arten von Tests bewerten wir die Schwachstellen des Systems und messen, welche Schwachstellen das System dem größten Risiko aussetzen. Umfasst produktspezifische NESSUS®-Scans und Penetrationstests.

Active Directory-Authentifizierung und -Autorisierung
Durch die Nutzung von Active Directory übernimmt PIC iX die Einstellungen der Kundenauthentifizierung und der Passwortrichtlinien. Dies verbessert die Authentifizierung und Autorisierung.
Ein strenger Konfigurationsmanagementprozess sichert die Integrität während des gesamten Produktlebenszyklus, indem der Entwicklungs- und Bereitstellungsprozess kontrollierbar und wiederholbar gemacht wird.

Remote Enablement
Unsere Remote-Enablement-Lösung, unterstützt von Performance Bridge Focal Point, ermöglicht es Ihnen, die Leistung Ihrer klinischen und Netzwerkgeräte von Philips zu bewerten. Sie hilft, die Diagnose zu beschleunigen, die Leistung zu steigern und Ihr Betriebssystem und die Gerätesoftware auf dem neuesten Stand zu halten. Experten von Philips überwachen Ihren Gerätebestand und verwalten Software-Revisionen aus der Ferne, um die Bereitstellung der neuesten Cybersicherheits-Updates zu vereinfachen.

Netzwerkmanagement
Unser Managementsystem verwendet Authentifizierung, Autorisierung und Nutzerkonten und beinhaltet folgende Empfehlungen:

- Verwenden Sie Protokollierungsmethoden für globale Netzwerkkonfigurationszugriffs- und Netzwerkänderungsprüfungen. Diese Methoden verfolgen nicht nur Konfigurationsänderungszeiten, sondern auch die Benutzer-ID, die die Änderung vornimmt. Nutzen Sie Dienste wie TACACS+ oder RADIUS.
- Konfigurieren Sie alle Benutzerkonten für eine automatische Zeitbegrenzung.
- Setzen Sie sichere Protokolle (HTTPS, SSH, SNMPv3 usw.) für die Systemverwaltung ein und deaktivieren Sie ungesicherte Protokolle (HTTP, Telnet und SNMP), wenn möglich.

Philips Remote Support (PRS)
Um Ihre Systeme aus der Ferne zu warten und zu schützen.

Technologielösungen
Unterstützen die höchsten Sicherheitsstandards und die besten IT-Praktiken.

Sie möchten mehr erfahren?

Lassen Sie uns reden. Oder besser: Lassen Sie uns zusammenarbeiten.

Wir würden Ihnen gerne helfen, Operative Intelligenz anzuwenden, um Ihre wichtigsten Herausforderungen in Bezug auf Mitarbeiter, Prozesse und Technologie zu lösen.

Mehr erfahren Sie unter **www.philips.de/cybersecurity-services**

So erreichen Sie uns
Besuchen Sie uns auf www.philips.com
healthcare@philips.com