PHILIPS

Services and Solutions Delivery

Operative Intelligenz

Kritische Daten, Ende-zu-Ende-Sicherheit

Executive Briefing

Das Gebot der Cybersicherheit von Medizinprodukten

„Daten sind die neue Währung und Hacking ein Geschäftsmodell. Die finanziellen Vorteile des Hackings werden bald die des weltweiten Drogenhandels übertreffen."

Stef Hoffman, Chief Information Security Officer, Philips

Innerhalb des komplexen, sich wandelnden Gesundheitssystems gibt es einen hochspezifischen Bereich der Cybersicherheit, der über den Bereich der IT hinausgeht und spezifisches Know-how für Gesundheitssysteme erfordert, wie es nur von erfahrenen Gesundheitsinformatikern und Geräteherstellern wie Philips bereitgestellt werden kann.

Diese sich schnell entwickelnde, stark regulierte und lebenswichtige Nische ist als Cybersicherheit für Medizinprodukte bekannt und ein Thema, über das sich jede Führungskraft, die den Wandel antreiben möchte, jetzt informieren muss, da es für die operative Effektivität von entscheidender Bedeutung ist.

Immerhin haben 81 % der Gesundheitsorganisationen zwischen 2013-2015 Datenschutzverletzungen durch einen Cyberangriff berichtet.[1] Dies geht aus einem Bericht von KPMG hervor. Inmitten der globalen Coronavirus-Pandemie und nach weiteren fünf Jahren der zunehmenden Vernetzung des Gesundheitswesen – stellen Sie sich einmal das Ausmaß der potenziellen Bedrohung heute vor.

[1] Zwischen 2013-2015 gemäß einem Bericht von KPMG aus dem Jahr 2015

Was ist Cybersicherheit von Medizinprodukten?
Vernetzte Medizinprodukte und andere mobile Gesundheitstechnologien sind ein zweischneidiges Schwert: Sie haben das Potenzial, eine transformative Rolle im Gesundheitswesen zu spielen, können aber auch ein Medium sein, das Patienten und Gesundheitsorganisationen Sicherheitsrisiken aussetzt.

In der zunehmend vernetzten Gesundheitslandschaft von heute befinden sich derzeit hunderttausende Medizinprodukte wie Patientenmonitore, Infusionspumpen, Beatmungsgeräte und Produkte für bildgebende Verfahren – von denen viele lebenserhaltend sind – in Krankenhausnetzwerken auf der ganzen Welt. Noch mehr Medizinprodukte sind über drahtlose Technologien zugänglich, zum Beispiel Insulinpumpen und Herzschrittmacher.

Effektive Cybersicherheit für Medizinprodukte – wie die Strategien und Angebote von Philips – ist ein Ende-zu-Ende-Sicherheitsangebot, das den globalen Vorschriften entspricht und darauf aufbaut, um Medizinprodukte und Dienstleistungen gegen Cyberbedrohungen robust zu machen.

Die medizinischen Cybersicherheitslösungen von Philips umfassen die Bereitstellung von Experten für Medizintechnik und Sicherheit vor Ort, die durch Sicherheitsprozesse des Philips-Konzerns unterstützt und durch speziell für das Gesundheitswesen ausgewählte Technologie ermöglicht werden.
Diese einzigartige Kombination spiegelt unseren Ansatz in Bezug auf operative Intelligenz zur integrierten Betrachtung von Mensch, Prozess und Technologien auf allen Betriebsebenen wider, in diesem Fall Cybersicherheit, um bestmögliche Sicherheit und kontinuierliche Verbesserung zu gewährleisten. Gal Gnainsky, Head of Phillips Group Security, betont nachdrücklich:

„Die Patientensicherheit in der heutigen vernetzten Versorgung ist eine Aufgabe, die wir unglaublich ernst nehmen. Bei der Weiterentwicklung unserer Cybersicherheitsprogramme müssen Transparenz, Verantwortlichkeit und Reaktionsfähigkeit eine Priorität haben, die wir weiterhin beibehalten."

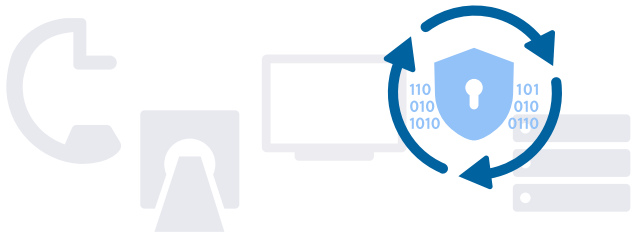
Was ist ein Medizinprodukt?
Gemäß Artikel 2 Absatz 1 der Verordnung (EU) 2017/745 (MDR) bezeichnet ein Medizinprodukt ein Instrument, ein Apparat, ein Gerät, eine Software, ein Implantat, ein Reagenz, ein Material oder ein anderer Gegenstand, das dem Hersteller zufolge für Menschen bestimmt ist und allein oder in Kombination einen oder mehrere der folgenden spezifischen medizinischen Zwecke erfüllen soll:

Diagnose, Verhütung, Überwachung, Vorhersage, Prognose, Behandlung oder Linderung von Krankheiten,Diagnose, Überwachung, Behandlung, Linderung von oder Kompensierung von Verletzungen oder Behinderungen,Untersuchung, Ersatz oder Veränderung der Anatomie oder eines physiologischen oder pathologischen Vorgangs oder Zustands, Gewinnung von Informationen durch die In-vitro-Untersuchung von aus dem menschlichen Körper – auch aus Organ-, Blut- und Gewebespenden – stammenden Proben und dessen bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologische oder immunologische Mittel noch metabolisch erreicht wird, dessen Wirkungsweise aber durch solche Mittel unterstützt werden kann.

Warum ist eine effektive, stets verfügbare Cybersicherheit für Medizinprodukte für die operative Effektivität von entscheidender Bedeutung?

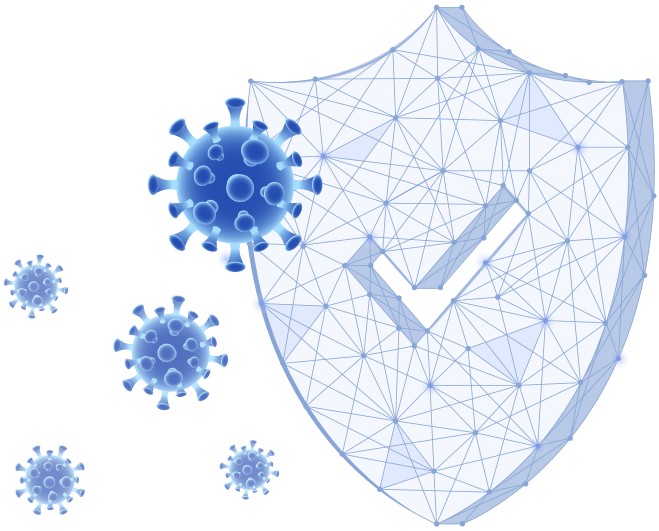
In einer Folge der Fernsehserie Homeland aus dem Jahr 2012 wurde der Vizepräsident der Vereinigten Staaten ermordet, als eine Terrororganisation seinen Herzschrittmacher über eine Drahtlosverbindung hackte. Obwohl dieses Szenario weit hergeholt erscheinen mag, gibt es immer mehr Beispiele aus der Praxis, bei denen Medizinprodukte für vorsätzliche Angriffe (z. B. das Hacken von Insulinpumpen) missbraucht werden, was die Bedenken hinsichtlich Cybersicherheitsbedrohungen für vernetzte Medizinprodukte unterstreicht.

Die sensible und private Natur von Patientendaten hat Cybersicherheit zu einem besonders wichtigen Thema in der Medizintechnikbranche gemacht. Medizinprodukte sind heute nicht mehr nur Maschinen, die am Patienten befestigt oder von ihm benutzt werden. Stattdessen sind sie oft mit der digitalen Patientenakte kabelgebunden oder drahtlos vernetzt, und ein typischer Intensivpatient könnte problemlos mit zehn oder mehr vernetzten Geräten verbunden werden. Während die Informationen auf dem Medizingerät für einen Hacker möglicherweise nicht von Nutzen sind, kann das Medizinprodukt als Zugangsweg für den Zugriff auf sensible Patientendaten wie die Privatadresse und andere Formen der Identifizierung verwendet werden, die für Identitäts- oder echten Diebstahl während des Krankenhausaufenthaltes des Patienten verwendet werden könnten. Potenzielle Bedrohungen bei Medizinprodukten sind beispielsweise der Vitaldatenmonitor, der auf einem veralteten Betriebssystem läuft, das Beatmungsgerät mit USB-Anschluss oder hartkodierte Benutzernamen und Passwörter für Außendiensttechniker des Herstellers und Haustechniker.



Aufsehenerregende Vorfälle haben Medizinprodukte in den Fokus gerückt

Mehrere hochkarätige Vorfälle haben die Cybersicherheit von Medizinprodukten in den Vordergrund der Sorgen von leitenden Führungskräften gebracht. So haben beispielsweise das weltweite Ransomware-Ereignis WannaCry – und andere Angriffe wie Petya/NotPetya – gezeigt, wie die Leistung anfälliger Medizinprodukte durch einen Exploit beeinträchtigt werden kann, unabhängig davon, ob er absichtlich auf das Gesundheitssystem abzielt oder rein zufällig ist. Ein mit Malware infiziertes Gerät kann den Krankenhausbetrieb lahmlegen, sensible Patientendaten preisgeben, andere angeschlossene Geräte gefährden und Patienten schaden.



Mögliche Bedrohungen sind:

- Elektromagnetische Interferenz
- Ungetestete oder defekte Software oder Firmware
- Falsch konfigurierte Netzwerke oder schlechte Sicherheitspraktiken
- Versäumnis, rechtzeitige Sicherheitssoftware-Updates und -Patches des Herstellers auf Medizinprodukten zu installieren und Bedenken hinsichtlich der Verursachung von Dienstunterbrechungen bei funktionsfähigen Geräten
- Unkontrollierte Weitergabe von Passwörtern, z. B. Unachtsamkeit der Mitarbeiter, wenn sie ein Passwort in der Öffentlichkeit unbeaufsichtigt lassen
- Deaktivierte Passwörter oder hartkodierte Passwörter für Software, die für den privilegierten Zugang zu medizinischen Geräten bestimmt ist (z. B. für Verwaltungs-, Technik- und Wartungspersonal)
- Netzwerkübertragung (per E-Mail, Fernzugriffskanal oder Dateiübertragung)
- Unbefugte Änderungen der Geräteeinstellungen, Neuprogrammierung oder Infektion durch Malware
- Ausrichtung auf mobile Gesundheitsgeräte mit drahtloser Technologie, um auf Patientendaten, Überwachungssysteme und implantierte medizinische Geräte zuzugreifen
- Unterbrechung der Versorgung/Dienstleistung (einschließlich potenzieller Todesfälle von Patienten) z. B.
- Täuschung von Mitarbeitern mit gefälschten E-Mails oder gefälschten Websites, um Zugangsdaten zu erhalten oder Malware zu installieren
- Spyware und Malware
- Spearphishing-Angriff
- Diebstahl oder Verlust vernetzter Medizinprodukte (extern oder tragbar)
- Unbeabsichtigte oder vorsätzliche „Insiderbedrohung“, die aufgrund der Vertrauensstellung innerhalb einer Organisation eine erhebliche Bedrohung darstellen kann
- Verlust von Patienteninformationen – insbesondere elektronisch geschützte Gesundheitsdaten
- Datenschutzverletzung, Informationsexfiltration und Verlust von Anlagen
- Manipulation, Diebstahl, Zerstörung, unbefugte Offenlegung oder fehlende Verfügbarkeit von Patientendaten für Anbieter
- Erpressung und Nötigung durch die Ausnutzung herausgefilterter sensibler Daten, z. B. Denial-of-Service-Attacken

Bekannte Fälle von Cyberkriminalität bei Medizinprodukten:
Im Jahr 2017 zielte der Cyberangriff WannaCry auf Computer auf der ganzen Welt ab, die das Windows-System von Microsoft nutzten, und die Daten von Personen verschlüsselte und Zahlungen in der Kryptowährung Bitcoin forderte, bevor der Zugriff darauf gewährt wurde. Bei solchen Ransomware-Angriffen drohen Cyberkriminelle, die Daten des Opfers zu veröffentlichen oder den Zugriff darauf zu verweigern, es sei denn, es wird ein Geldbetrag gezahlt. Die Hacker hinter WannaCry verursachten die Absage von Zehntausendne von Arztterminen und die Umleitung von NHS-Krankenwagen.

Im Jahr 2017 erhielt MedStar Health mit Sitz in den USA Bitcoin-Forderungen nach der Verschlüsselung von Computersystemen. Auf infizierten Computern wurden Benachrichtigungen angezeigt, die einen Datenverlust nach 10 Tagen androhten. Patientenakten von 10 Krankenhäusern und 250 ambulanten Zentren waren entweder nicht verfügbar oder konnten nicht aktualisiert werden, während MedStar Backups zur Wiederherstellung der Daten verwendete. Operationen an Patienten wurden abgesagt und Krankenwagen umgeleitet. Krankenschwestern und Ärzte wiesen auf Probleme der Patientensicherheit hin, da sich Verzögerungen von Laborergebnissen auf die Behandlung auswirkten.[2]

Im April 2018 rief die FDA zwei Defibrillatormodelle des amerikanischen Gesundheitsunternehmens Abbott zurück, nachdem sie eine potenzielle Schwachstelle in ihren Cybersicherheitssystemen gefunden hatte. Anfang 2019 entwickelte eine israelische Forschungsgruppe an der Ben-Gurion-Universität des Negev eine Malware, die es Angreifern ermöglichen könnte, realistische Bilder von bösartigen Tumoren in CT- oder MRT-Scans einzufügen, bevor sie von Ärzten untersucht wurden. Schlimmer noch, sie bewiesen, dass dieselbe Malware in der Lage war, echte Krebstumore aus diesen Bildern zu entfernen, was zu schwerwiegenden Fehldiagnosen führen und eine dringende Intensivpflege oder Operation für Patienten verhindern könnte. Glücklicherweise hatte die Gruppe diese Malware entwickelt, um die Notwendigkeit einer verbesserten Cybersicherheit im Gesundheitswesen hervorzuheben, und hatte nicht die Absicht, sie jemals böswillig zu verwenden. Und doch zeigt die Existenz der Forschung das Potenzial für Angreifer, Patienten ernsthaft zu schaden.

Im Jahr 2019 gab die FDA Empfehlungen zu den potenziell ausnutzbaren Schwachstellen bei den implantierbaren Herzgeräten von St. Jude Medical und dem entsprechenden Merlin@home-Transmitter ab. Die FDA-Prüfung des Merlin@home-Transmitter von St. Jude Medical bestätigte, dass ein nicht autorisierter Benutzer im Falle einer Ausnutzung der Schwachstellen aus der Ferne auf das RF-fähige implantierte Herzgerät eines Patienten zugreifen könnte, indem er den Merlin@home-Transmitter verändert. Der geänderte Merlin@home-Transmitter könnte dann verwendet werden, um an das implantierte Gerät gesendete Programmierbefehle zu modifizieren, was zu einer schnellen Entladung der Batterie und/oder zur Verabreichung von unangemessener Stimulation oder Schocks führen könnte. Es wurde ein validierter Software-Patch herausgegeben, der den Transmitter automatisch aktualisiert. In dem Bericht heißt es, dass keine Berichte über Patientenschäden aufgrund dieser Schwachstellen vorliegen.[3]

[2] Verfügbar: https://www.washingtonpost.com/local/medstar-health-turns-away-patientsone-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce -f06b5ba21f33_story. html. [Zugriff am 29. Januar 2017]. 12. ICS-CERT, „Hospira LifeCare PCA Infusion System Vulnerabilities (Update B)", 10. Juni 2015. [Online]. Verfügbar: https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01B. [Zugriff am 7. August 2016].
[3] FDA, „Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication", 9. Januar 2017. [Online]. Verfügbar: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm. [Zugriff 23. Januar 2017]. 11. John Woodrow Cox, „MedStar Health turns away patients after likely ransomware cyberattack," The Washington Post, 29. März 2016. [Online].

Kritische Daten, Ende-zu-Ende-Sicherheit

Wie führt Philips die Anstrengungen im Bereich Cybersicherheit von Medizinprodukten an?

Philips war ein Vorreiter bei der Erkenntnis, dass es bei effektiver Cybersicherheit nicht mehr um den Schutz der „Box" oder des einzelnen Produkts geht, sondern um einen systematischen Ansatz, der berücksichtigt, wo und wie Geräte eingesetzt werden.

Bei Philips ist „Security Designed in" eine Ende-zu-Ende-Denkweise: Die Einführung von Sicherheitsprinzipien beginnt mit dem Produktdesign und der Entwicklung, über das Testen und die Bereitstellung – gefolgt von umfassenden Richtlinien und Verfahren für die Überwachung, effektiven Updates und, falls erforderlich, Vorfallmanagement. Philips hat ein eigenes Sicherheitsprogramm für Produkte und Lösungen ins Leben gerufen, um umfassende und effektive Ansätze zur Erfüllung der Kundenanforderungen zu entwickeln, zu implementieren und zu aktualisieren. Das Philips Security Center of Excellence teilt Informationen mit führenden Cybersicherheitsforschern und Testeinrichtungen auf der ganzen Welt, um sie bei der schnellen Beseitigung, Verringerung und Entschärfung von Cyberbedrohungen zu unterstützen.

Mit dem Fokus des Unternehmens auf Gesundheitstechnologie sind Datenschutz und Sicherheit von strategischer Bedeutung geworden, da Gesundheitsdaten zu den sensibelsten Arten personenbezogener Daten gehören. Tatsächlich hängt die Wettbewerbsposition des Unternehmens stark von der Verwendung dieser Daten ab, und das öffentliche Vertrauen ist von größter Bedeutung. Die Verpflichtung für den Datenschutz geht weit über die Einhaltung gesetzlicher Vorschriften hinaus, wobei Privatsphären- und Datenschutzkontrollen in den gesamten Lebenszyklus aller Daten eingebettet sind. Privatsphäre und Datenschutz sind integraler Bestandteil der allgemeinen Geschäftsprinzipien von Philips, in denen wir uns einer Reihe von Verpflichtungen unterwerfen.

Zu den wichtigsten Initiativen zur Produktsicherheit von Philips gehören:

Philips Produktsicherheitsrichtlinie

Die Philips Produktsicherheitsrichtlinie ist eine branchenweit fortschrittliche, öffentlich verfügbare Richtlinie, die aus Richtlinien, Verfahren und Standards besteht, die es dem Unternehmen ermöglichen, bewährte Sicherheitspraktiken umzusetzen. Es beschreibt die strategische Organisation und Verfahren des Unternehmens für Folgendes:

- Pflege eines globalen Netzwerks von Sicherheits- und Datenschutzexperten, die gemäß der Philips Produktsicherheitsrichtlinie arbeiten
- Entwicklung und Bereitstellung von Best Practices für unsere Produkte und Dienstleistungen
- Anleitung zur Risikobewertung und Reaktion auf Vorfälle in Bezug auf potenzielle und identifizierte Sicherheits- und Datenschutzbedrohungen sowie Schwachstellen
- Steuerung der in Produkte und Dienstleistungen über ihren Lebenszyklus hinweg eingebetteten Sicherheit, einschließlich Risikobewertung und Reaktion auf identifizierte Schwachstellen in Produkten und Dienstleistungen

Implementierung von Sicherheitsstandards, die aktuelle behördliche Anforderungen und Best Practices der Branche erfüllen oder übertreffen, einschließlich:

- Produktsicherheits- und Datenschutzanforderungen für Produkte und Dienstleistungen, die nicht nur auf den von der FDA empfohlenen Standard ISO/IEC-80001 ausgerichtet sind, sondern sogar als Grundlage für den Standard 80001-2-2 verwendet wurden.
- Sicherheits- und Datenschutzanforderungen der Dienste, die auf anerkannte Standards wie NIST 800-53 Rev 4, ITIL v3.1.24 und ISO/IEC-27000-Reihe abgestimmt sind.
- Erstellung von kundenorientierten Informationen, wie z. B. der dem Industriestandard entsprechenden Herstellererklärung für die Sicherheit von Medizinprodukten (MDS2).
- Unterstützung der FDA-Leitlinien zum Premarket-Management zu Cybersicherheit bei Medizinprodukten und FDA-Postmarket-Management zur Cybersicherheit bei Medizinprodukten.

Abstimmung mit Aufsichtsbehörden, einschließlich der FDA

Philips hat sich der Bereitstellung umfassender Sicherheitspläne verschrieben, die die Sicherheit von Medizinprodukten, Unternehmensinformationen und personenbezogenen Daten gewährleisten. Und das tun wir in der stark regulierten Branche für Medizinprodukte. Zulassungsbehörden wie die US-amerikanische Food and Drug Administration (FDA) verlangen, dass Hardware- und Software-Releases und -Änderungen strengen Verifizierungs- und Validierungsmethoden unterzogen werden, um sicherzustellen, dass die hohen Standards in Bezug auf Sicherheit, Wirksamkeit, Qualität und Leistung in allen anwendbaren Philips Produkten und Dienstleistungen eingehalten werden.

Leitlinienentwurf der FDA: Inhalt von Premarket-Einreichungen für Management der Cybersicherheit bei Medizinprodukten (Juni 2013).
Dieser Leitlinienentwurf schlägt vor, Cybersicherheitsfunktionen in die Produktentwicklungsphase zu integrieren und identifiziert Informationen, die in die Einreichungen vor der Markteinführung für Medizinprodukte aufgenommen werden sollten. Sicherheitsfunktionen sollten drei spezifische Bereiche abdecken:

1. Beschränkung des Zugriffs nur auf vertrauenswürdige Benutzer
2. Festlegung von vertrauenswürdigen Inhalten
3. Verwendung von Ausfallsicherungs- und Wiederherstellungsfunktionen

Hersteller sollten Folgendes definieren und dokumentieren:

- Identifizierung von Anlagen, Bedrohungen und Schwachstellen
- Folgenabschätzung der Bedrohungen und Schwachstellen auf die Gerätefunktionalität
- Abschätzung der Wahrscheinlichkeit einer Bedrohung und der Ausnutzung einer Schwachstelle
- Ermittlung von Risikoniveaus und geeigneten Minderungsstrategien
- Restrisikobewertung und Risikoakzeptanzkriterien

Eine Erkenntnis aus den Leitlinien ist die Notwendigkeit für Hersteller von Medizinprodukten, den Nachweis zu erbringen, dass ihr Risikobewertungsprozess (wie in ISO 14971:2007 beschrieben) sowohl „absichtliche“ als auch unbeabsichtigte Sicherheitsrisiken für das Medizinprodukt berücksichtigt und diese Risiken mit geeigneten Sicherheitskontrollen als Teil des Gerätedesigns angeht. Der Nachweis sollte als Teil des Pakets zur Einreichung der Premarket-Zulassung (z. B. 510K, PMA) enthalten sein. Hersteller von Medizinprodukten sollten in den frühen Phasen des Softwarelebenszyklus die Prozesse und Akteure (z. B. Hacker, organisierte Kriminalität, Terroristen und Nationalstaaten) berücksichtigen, die beabsichtigen, ein Medizinprodukt zu kompromittieren, um entweder a) dem Patienten zu schaden oder b) geschützte Gesundheitsinformationen zu extrahieren. Hersteller sollten außerdem erwägen, mit den Medizintechnikern und Ärzten ihrer Kunden zusammenzuarbeiten, um einen Katalog von Anwendungsfällen zu entwickeln, aus dem Schwachstellen speziell für ihr Medizinprodukt und dessen beabsichtigter Verwendungszweck abgeleitet werden können.

https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices-0

FDA-Sicherheitsmitteilung: Cybersicherheit für Medizinprodukte und Krankenhausnetzwerke (Juni 2013).
In dieser Mitteilung wird den Herstellern von Medizinprodukten und Gesundheitseinrichtungen empfohlen, geeignete Sicherheitsvorkehrungen zu treffen, um das Risiko eines Geräteausfalls aufgrund eines Cyberangriffs zu verringern. Von den Herstellern wird erwartet, dass sie Schritte unternehmen, um den unbefugten Zugriff auf Medizinprodukte einzuschränken und Richtlinien und Praktiken hinsichtlich geeigneter Sicherheitsvorkehrungen zu überprüfen. In Übereinstimmung mit der FDA-Mitteilung sollten Hersteller:

- den Zugriff auf vertrauenswürdige Benutzer beschränken
- einzelne Komponenten vor Ausbeutung schützen
- die kritische Funktionalität eines Produkts aufrechterhalten

Gesundheitseinrichtungen sollten:

- die Netzwerksicherheit bewerten und das Krankenhaussystem schützen
- den unbefugten Zugriff auf das Netzwerk und vernetzte Medizinprodukte einschränkten
- sicherstellen, dass geeignete Antivirensoftware und Firewalls auf dem neuesten Stand sind
- die Netzwerkaktivität auf unbefugte Nutzung überwachen
- einzelne Netzwerkkomponenten durch routinemäßige und periodische Evaluierung schützen

http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm

Wie kann man jetzt handeln und Medizinprodukte schützen?

Angesichts der Bedrohungen der Cybersicherheit von Medizinprodukten, die zu den am schnellsten wachsenden Risiken für mit privaten oder öffentlichen Netzwerken verbundenen Geräte gehören, verlangen Regulierungsbehörden, darunter die US-amerikanische Food and Drug Administration (FDA) und die Europäische Arzneimittel-Agentur (EMA), jetzt von den Entwicklern von Medizinprodukten, dass sie Cybersicherheit in Risikomanagementprogramme für jedes Gerät einbeziehen, das mit einem Netzwerk oder einem anderen Gerät verbunden werden könnte, sei es öffentlich oder privat, kabelgebunden oder drahtlos (1, 2, 3).

Netzwerkverbindungen setzen Medizinprodukte potenziell Bedrohungen aus vielen Quellen aus – nicht nur über einen lokalen Router oder Server in einem Krankenhaus oder einer Arztpraxis, sondern von jedem Computer, Tablet, Smartphone oder sogar einer intelligenten Glühbirne, die irgendwo auf der Welt mit dem Internet verbunden ist. Infolgedessen betrachten die Aufsichtsbehörden die Cybersicherheit als gemeinsame Verantwortung.

Philips hat sich diesem Ansatz der Risikoteilung verschrieben und bietet umfassende Strategien für das Cybersicherheits-Risikomanagement, die Beiträge aller Beteiligten einbeziehen. Durch die Zusammenarbeit im gesamten Ökosystem des Gesundheitswesens kann die Branche auf den Fortschritten anderer wichtiger Infrastrukturbranchenaufbauen.

Das unterstützt die Vorteile der digitalen Konnektivität für die Patientenversorgung. „Es gibt nicht die eine goldene Lösung. Anstatt es zu einer Last zu machen, müssen wir Sicherheit und Datenschutz in unseren Unternehmen mit offenen Armen angehen“, so Michael McNeil, Head of Global Product & Security Services, Philips Healthcare. „Jeder von uns in diesem Ökosystem muss seine Rolle bei der Abwehr dieser Bedrohung spielen.“ Die Pläne für das Cybersicherheits-Risikomanagement decken die gesamte Lebensdauer eines Produkts ab, von der Entwicklung und Prüfung bis hin zu seiner Verwendung durch medizinisches Fachpersonal und/oder mit Patienten. Sie befassen sich auch mit dem breiten Spektrum potenzieller Bedrohungen, einschließlich absichtlicher oder versehentlicher Unterbrechung der Gerätefunktion, Störung der Datenübertragung zwischen Geräten und Servern und der Offenlegung privater medizinischer Daten oder des Standorts oder der Identität des Patienten. Und weil Hacker sehr erfinderisch und hartnäckig sind, werden unsere Cybersicherheitspläne ständig aktualisiert, wobei wahrscheinlich aktuelle und zukünftige Bedrohungen identifiziert, überwacht und neue Abwehrstrategien entwickelt werden.

Fünf Tipps zur Prävention von Datenschutzverletzungen und für eine bessere Datensicherheit im Gesundheitswesen

1. Verschaffen Sie sich einen klaren Überblick
Erfassen Sie genau, welche Produkte und Anlagen sich in Ihrer Umgebung befinden.

2. Konzentrieren Sie sich auf ältere Produkte
Arbeiten Sie mit Technologiepartnern an allen älteren Produkten und Lösungen, die möglicherweise nicht aktualisiert, gepatched und gesichert werden können.

3. Entwickeln Sie Best Practices
Stellen Sie sicher, dass Sie ein Verständnis dafür haben, was aus Sicht der Branche Best Practices sind.

4. Steuern Sie die Cybersicherheit über die gesamte Lieferkette hinweg
Es ist wichtig, an Ihren Beschaffungsprozessen zu arbeiten und die Komponenten der von Ihnen bereitgestellten Lösungen zu verstehen.

5. Schließen Sie Partnerschaft mit Herstellern, Anbietern
Sicherheit ist – wie Qualität – eine Voraussetzung für das Vertrauen in die Marke Philips. Kunden und Verbraucher müssen sich auf die Sicherheit und Qualität unserer Produkte und Dienstleistungen verlassen können und den Wert der Weitergabe ihrer Daten erkennen – andernfalls werden die gesundheitlichen Vorteile, die sich aus der Konnektivität und Analyse großer Datenmengen ergeben, möglicherweise nie realisiert. Als leitende Führungskräfte können Sie sicher sein, dass wir weiterhin proaktiv die Vorteile der vernetzten Gesundheitstechnologie hervorheben und weiterhin in sichere Systeme investieren, auf die sich unsere Kunden verlassen können. Die Cybersicherheit von Medizinprodukten ist eines unserer wachsenden Kompetenzzentren, das auf dem Verständnis und der Wertschätzung der gegenseitigen Abhängigkeit von Menschen, Prozessen und Technologie basiert.

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