PHILIPS

Patientenüberwachung

Bessere Aussichten bei der **Cybersicherheit im Gesundheitswesen**

Schulungen zur Patientenüberwachung, Risikomanagement und Cybersicherheitslösungen für klinische Netzwerke von Philips

IT-Experten sind bestens mit Sicherheitsbedrohungen wie Ransomware, Phishing und Cyberdiebstahl vertraut. Für die Absicherung regulierter Medizinprodukte bedarf es jedoch völlig neuer Prozesse, Genehmigungen und Kooperationen.

Verstehen und Anwenden von Risikomanagementprozessen

Durch die Implementierung bewährter Abläufe (Best Practices) im Risikomanagement können wir Sie bei der Abwehr potenzieller Cyberbedrohungen unterstützen und die Risiken mindern.

- **Geräte für die Patientenüberwachung – ein Zugriffspunkt für Cyberangriffe.** Hacker interessieren sich für die Gesundheitsbranche, da sie anderen Branchen in Bezug auf die Cybersicherheit häufig hinterherhinkt. Laut Beazley, einer global operierenden, auf Cybersicherheit spezialisierten Versicherungsgesellschaft, zielten 45% aller Ransomware-Angriffe, die 2017 im Zuge einer Studie untersucht wurden, auf medizinische Versorgungseinrichtungen ab.[1] Auf dem Schwarzmarkt sind medizinische Daten 10 Mal mehr wert als Kreditkartendaten.[2]

  Geräte für die Patientenüberwachung gehören zu den besonders einfachen Eingangspforten für Hacker, um auf sensible HIPAA- oder geschützte Gesundheitsdaten von Patienten zuzugreifen. Da diese Geräte zudem mit Sensoren und Monitoren verbunden sind, können sie darüber hinaus auch noch als Zugang zu größeren Krankenhausnetzwerken ausgenutzt werden.

  Virenschutz. Jede Änderung an einem regulierten Medizinprodukt – auch wenn es sich nur um die Installation einer Virenschutzsoftware handelt – erfordert eine Validierung. Ein Medizinprodukt, dass nach einer Installation nicht erneut geprüft wurde, ist nicht sicher.
- **Die richtigen Entscheidungsträger.** Die Cybersicherheit fällt nicht ausschließlich in den Aufgabenbereich von IT-Experten, insbesondere nicht im Gesundheitswesen. Für mehr Cybersicherheit und Effizienz empfehlen wir unseren Kunden, auf Teamwork und Zusammenarbeit zu setzen. Die Einblicke und Beiträge von Vertretern der Klinikteams, der medizintechnischen Abteilung und der Führungsebene sind für Ihren Erfolg unerlässlich. Eine Entscheidung im Bereich der Cybersicherheit, die Auswirkungen auf die Mitarbeiter, die Patienten und die Zukunft Ihres Krankenhauses hat, ist ein bedeutender Schritt mit großer Tragweite. In Abbildung 1 sind die Personen aufgeführt, die in den Entscheidungsprozess eingebunden werden sollten.
- **Verantwortungsbereiche der Entscheidungsträger.** Wir empfehlen die Ausarbeitung von Vereinbarungen (Verträgen) über die jeweiligen Zuständigkeiten. Diese stärken das Verantwortungsgefühl und sorgen für einen effektiven Arbeitsablauf.

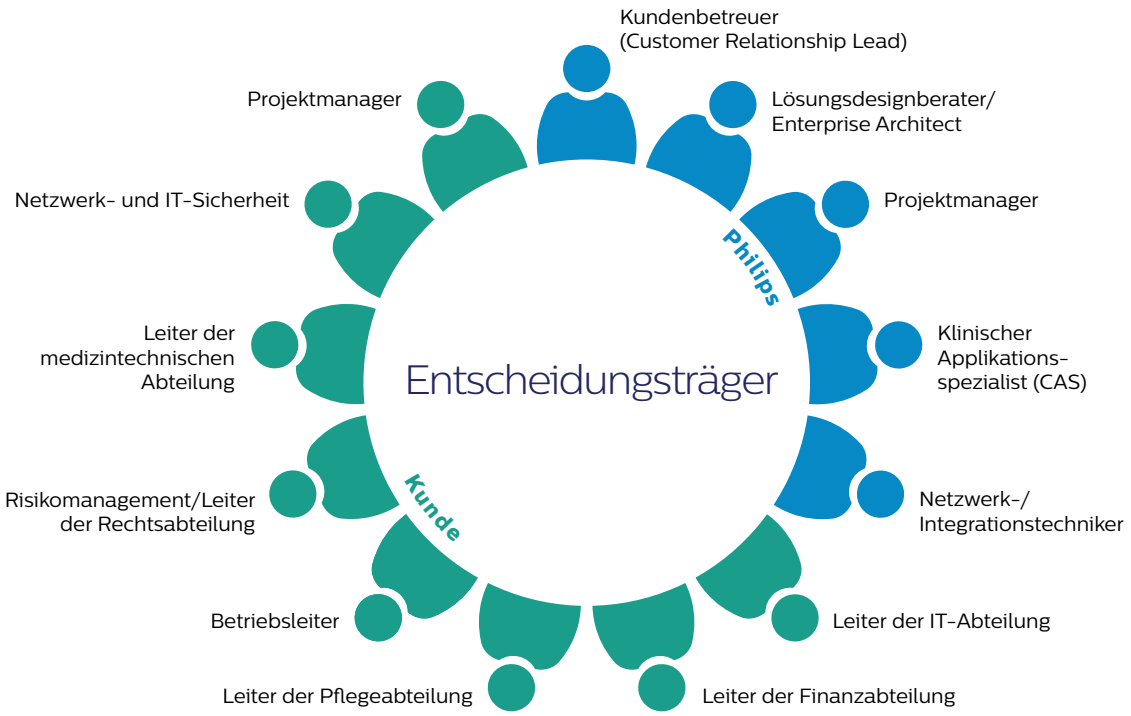


Abbildung 1: Die wichtigsten einzubeziehenden Entscheidungsträger

Klinische und IT-bezogene Anforderungen

Die Geräte für die Patientenüberwachung und das klinische Netzwerk müssen aufeinander abgestimmt sein, um die Sicherheitsstandards erfüllen und die Schutzmaßnahmen umsetzen zu können. Die integrierte Patientenüberwachungslösung von Philips muss sich dazu mit zahlreichen Geräten für die Patientenversorgung sowie Krankenhaussystemen verbinden können.

Im Referenz-Architekturdiagramm in Abbildung 2 können Sie sehen, wie die klinischen und IT-bezogenen Krankenhausanforderungen kombiniert werden, um unsere Kunden zu unterstützen und ihren Ansprüchen an die Patientenversorgung gerecht zu werden.

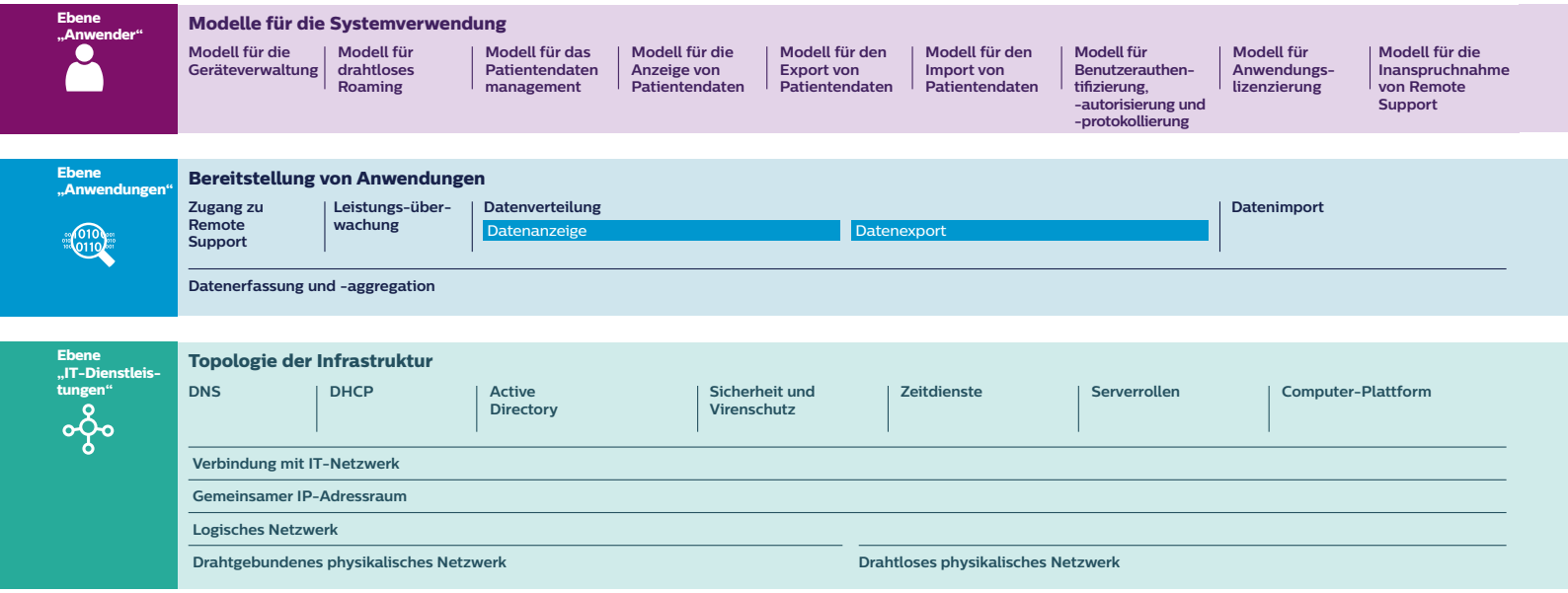
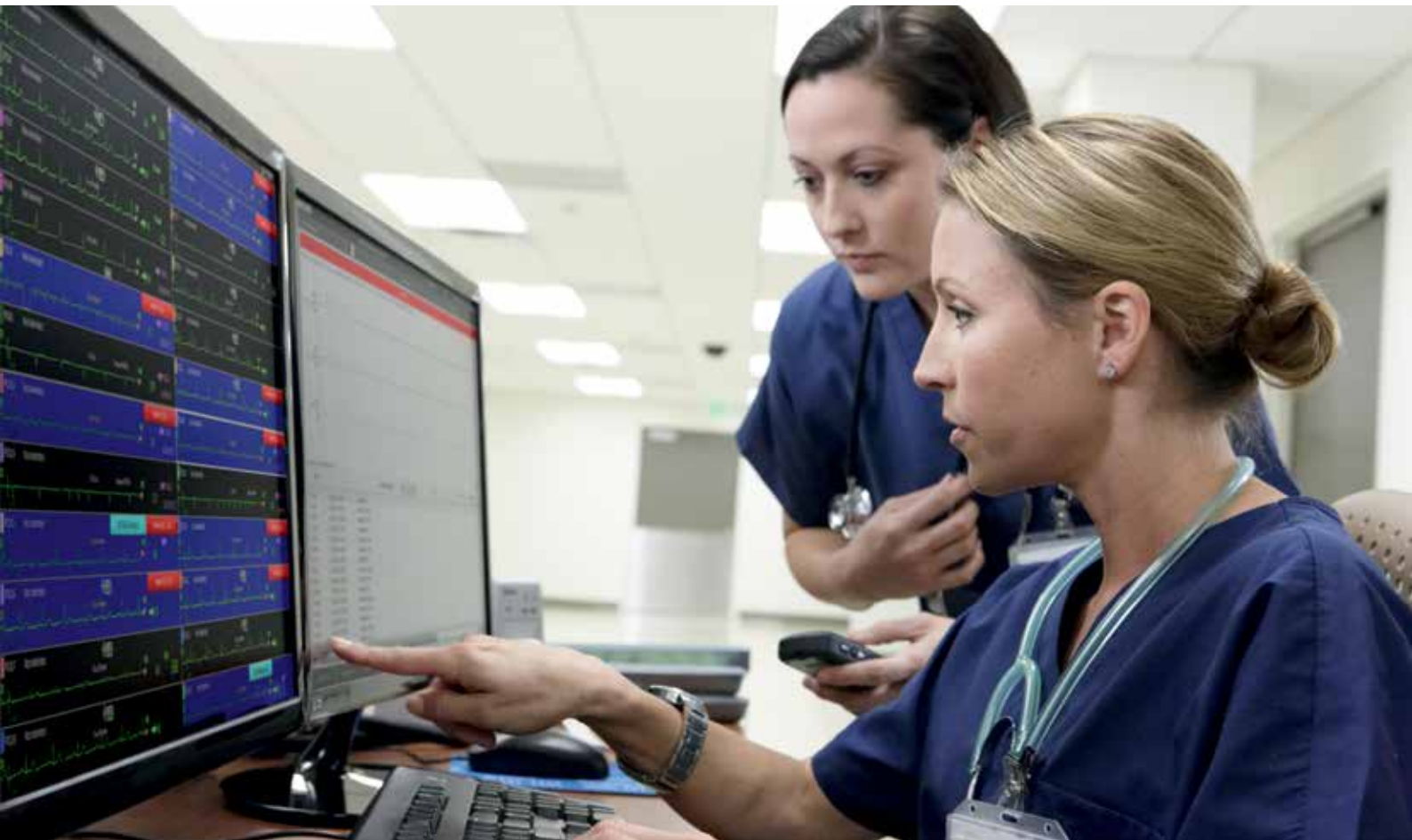


Abbildung 2: Referenzarchitektur für die Patientenüberwachung



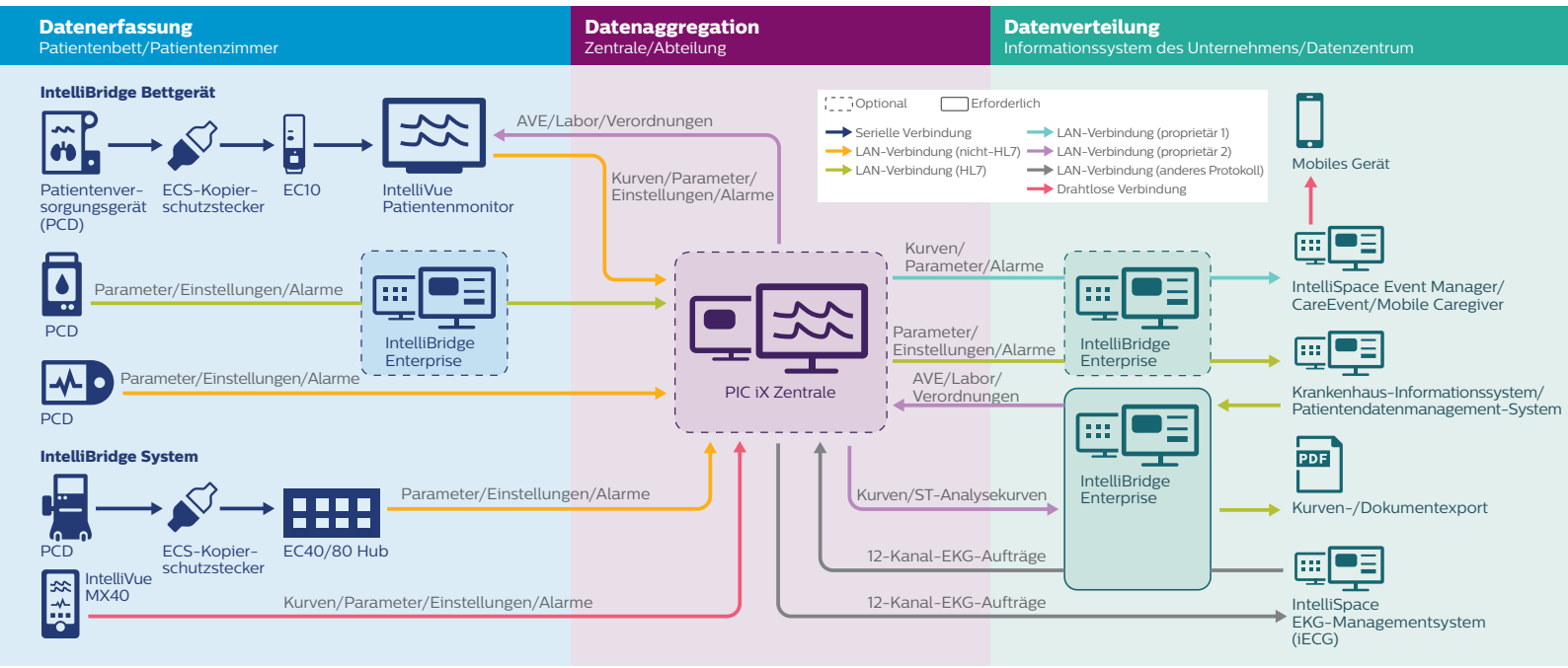
Die Infrastruktur der Patientenüberwachung – der Schlüssel zur Cybersicherheit im Gesundheitswesen

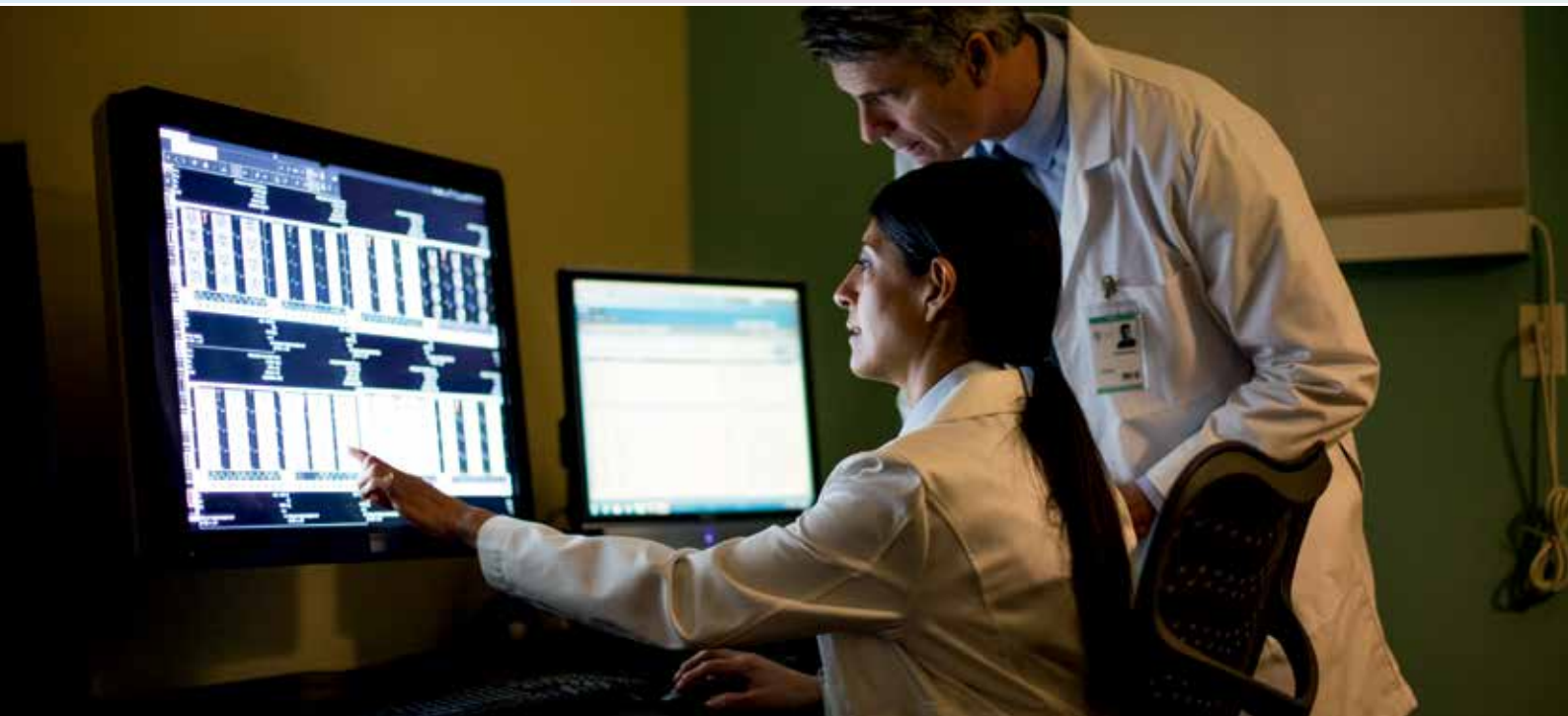
Bei der IntelliVue Lösung für die Patientenüberwachung handelt es sich um eine komplexe Systemumgebung mit verknüpften Geräten, die in Echtzeit lebenswichtige Daten liefern. Dieses System muss das ganze Jahr über rund um die Uhr betriebsbereit sein. Diese lebenswichtigen Daten umfassen Vitalparameterwerte, die direkt am Patienten gemessen und aus mehreren Quellen zusammengeführt werden, sowie die Verteilung von Kurven, Trends, Alarmen und numerischen Werten an mehrere Systeme, was auch die elektronische Patientenakte (ePA) einschließt.

Nur mit einem vielseitigen und ganzheitlichen Ansatz lässt sich dieses Ökosystem verwalten und sicherstellen, dass die Anforderungen an Bedienfreundlichkeit, Wartungsfreundlichkeit und Sicherheit erfüllt werden.

Auch wenn medizinische Versorgungseinrichtungen besonders anfällig sind – in einer vom Ponemon Institute im Jahr 2017 durchgeführten Studie gingen die meisten Teilnehmer davon aus, im Laufe des Folgejahres Opfer eines Cyberangriffs zu werden – unterzogen lediglich 53% der Einrichtungen ihre Geräte für die Patientenüberwachung einer Prüfung.[4]

Vorgesehener Informationsfluss bei der Patientenüberwachung mit Philips





Sichere Patientenüberwachung dank Unterstützung von Philips bei allen Herausforderungen

Für zusätzliche Sicherheit setzt Philips auf bewährte Abläufe (Best Practices), wozu neben Sicherheitsprotokollen und Risikobeurteilungen auch mehrstufige aktive Abwehrmaßnahmen sowie modernste Funktionen zählen.

Eigenmeldungen

Als Hersteller von Medizinprodukten nehmen wir ein Sicherheitsprotokoll besonders ernst: die Eigenmeldung von Sicherheitslücken. Laut einem Bericht von MedCrypt hat sich seit der Veröffentlichung des FDA-Leitfadens zur Cybersicherheit 2016 einiges getan: Seither ist die Anzahl der Meldungen von Sicherheitslücken um 400% pro Quartal gestiegen. Immer mehr Hersteller von Medizinprodukten und unabhängige Forschungseinrichtungen melden also Schwachstellen bezüglich der Cybersicherheit.[5]

Das ist ein entscheidender Vorteil für Sie. Wir bei Philips übernehmen Verantwortung für Sicherheitslücken, melden sie proaktiv und befolgen dabei die folgenden bewährten Abläufe (Best Practices):

- Sobald eine Schwachstelle entdeckt wird, melden wir diese dem Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Dabei handelt es sich um eine Unterabteilung des US-amerikanischen Ministeriums für Innere Sicherheit.
- Anschließend wird die Meldung an die Food and Drug Administration (FDA) weitergeleitet.
- Danach müssen wir die Sicherheitslücke innerhalb einer angemessenen Frist schließen.
- Über die Sicherheitslücke – und die zugehörige Behebungsmaßname – informieren wir dann die Öffentlichkeit.
- Wir führen außerdem jede Woche proaktiv Selbstprüfungen durch, um den Fortschritt bei bestehenden Lücken nachverfolgen und potenzielle Bedrohungen erkennen zu können.

Mehrstufige Abwehr

Eine einzige Maßnahme reicht nicht aus, um Ihre Geräte für die Patientenüberwachung vor Cyberangriffen zu schützen. Aus diesem Grund empfehlen Experten eine umfangreiche Sicherheitsstrategie mit mehreren Stufen. Ganz im Sinne der bewährten Abläufe (Best Practices) trägt jede dieser Verteidigungsmaßnahmen maßgeblich dazu bei, Hackerangriffe abzuwehren, vor Malware zu schützen und unbefugte Zugriffe auf Medizinprodukte zu verhindern. Dies sind die einzelnen Komponenten dieser Strategie:

- Firewall
  - Härtung des Betriebssystems und der Anwendungen gemäß den vom US-Verteidigungsministerium herausgegebenen Security Technical Implementation Guides (STIGs)
  - Authentifizierung, Autorisierung und Protokollierung
- Audit Logging
- Verschlüsselung und Knotenauthentifizierung

Philips Defense-in-Depth-Strategie

Bewährte Abläufe (Best Practices) gemäß IEC 80001-1

Diese neue internationale und freiwillige Norm bietet einen Überblick über die Aspekte, die bei der Verbindung von Medizinprodukten mit Ihrem IT-Netzwerk besonders zu beachten sind, um die Sicherheit und Wirksamkeit sowie die Daten- und Systemsicherheit zu wahren.

Auch wenn die Anwendung der Norm IEC 80001-1 freiwillig ist, gehen wir davon aus, dass sie der neue Standard im Gesundheitswesen wird. Wir empfehlen, frühzeitig mit der Einführung der erforderlichen Richtlinien und Verfahren zu beginnen, um die Risiken für medizinische IT-Netzwerke zu senken.

Modernste Funktionen

Bestandteil unserer Unterstützung für Ihr Krankenhaus im Bereich der Cybersicherheit ist unter anderem die Bereitstellung von Funktionen ganz nach Ihren Anforderungen. So bietet Philips beispielsweise die folgenden einzigartigen Leistungen:

- Bereitstellung von Microsoft Windows 10
- Umfassende Unterstützung von validierten Sicherheitsupdates für das Betriebssystem
- Integration in Ihre Krankenhausdomäne
- Verschlüsselung
- SCCM

Zukunftsfähige proaktive Lösungen für Ihre Anforderungen

Der technologische Fortschritt schreitet rapide voran. Durch die laufende Entwicklung und Einführung neuer innovativer Funktionen bleiben wir jedoch stets einen Schritt voraus.

Gemeinsam können wir eine sichere Umgebung schaffen, indem wir wachsam bleiben und die sich laufend verändernden Gefahren im Hinblick auf die Cybersicherheit im Auge behalten. Unser Streben ist es, Ihre heutigen und zukünftigen Bedürfnisse zu erfüllen.

Weitere hilfreiche Quellen

Richtlinie des US-Verteidigungsministeriums zur Offenlegung von Sicherheitslücken
https://hackerone.com/deptofdefense

Health Insurance Portability and Accountability Act (HIPAA)
Dieses US-amerikanische Gesetz enthält umfassende Anforderungen an Datenschutz- und Sicherheitsstandards, darunter auch an die elektronische Übertragung von Gesundheitsdaten. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

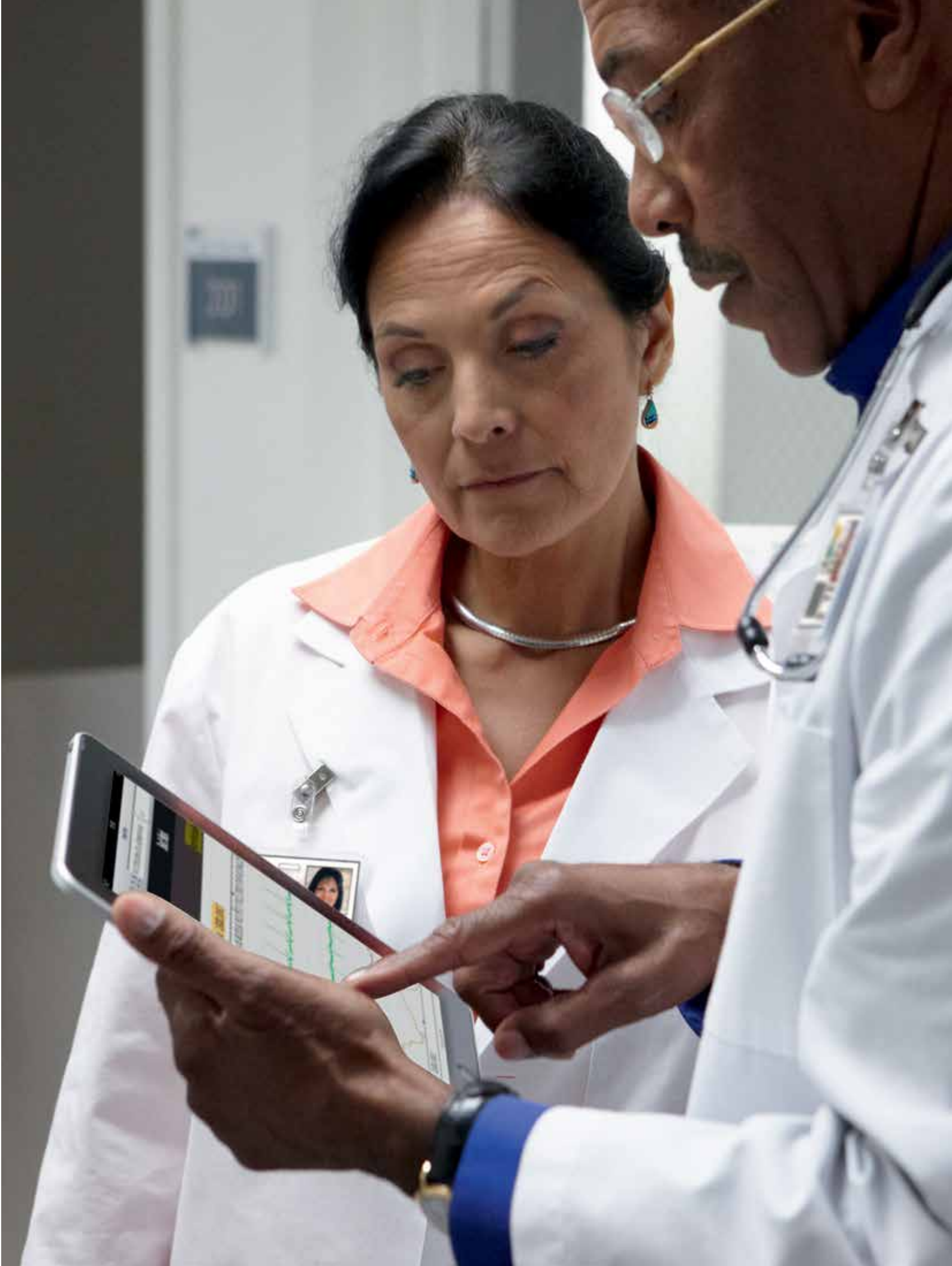
Application of Risk Management for IT-Networks Incorporating Medical Devices – Part 2-2 (IEC 80001-2-2)
Diese Norm enthält Empfehlungen für die Offenlegung von und die Information über Anforderungen, Risiken und Kontrollen für Medizinprodukte. https://www.iso.org/standard/57939.html

Federal Information Processing Standard Publication 200 (FIPS PUB 200)
Dieses Dokument enthält eine vollständige Liste aller Anforderungen an Unternehmen. https://csrc.nist.gov/publications/detail/fips/200/final

National Institute of Standards and Technology 800-53 (NIST 800-53)
Diese Norm bietet einen Überblick über die Grundlagen der Sicherheitskontrolle, die den Ausgangspunkt für die Auswahl von Sicherheitskontrollmaßnahmen bilden. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Quellen
1. Becker's Health IT & CIO Report, 'The 3 most important security statistics healthcare organizations need to know', 7. März 2018, Mike Duffy; (https://www.beckershospitalreview.com/healthcare-information-technology/the-3-most-important-security-statistics-healthcare-organizations-need-to-know.html).
2. Reuters, 'Your medical record is worth more to hackers than your credit card', 24. September 2014, Caroline Humer, Jim Finkle; (https://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924).
3.–4. HIT Consultant, 'Protecting Medical Device Security in the Age of Ransomware', 25. Juni 2018, Kayla Matthews; (https://hitconsultant.net/2018/06/25/medical-device-ransomeware/).
5. Healthcare IT News, 'Is FDA doing enough to support medical device security?', 15. August 2018, Jessica Davis; (https://www.healthcareitnews.com/news/fda-doing-enough-support-medical-device-security).

Zusätzlich verwendete Quellen:
Biomedical Instrumentation & Technology, 'The Vital Role of Device Manufacturers as Cybercitizens', November/Dezember 2015, William L. Holden; (http://www.aami-bit.org/doi/abs/10.2345/0899-8205-49.6.410).



Weitere Informationen zur Philips IntelliVue Lösung für die Patientenüberwachung erhalten Sie unter **www.philips.de/healthcare**.

4522 991 51573 * SEP 2020

www.philips.com