PHILIPS

Services and Solutions Delivery

Operative Intelligenz

Cybersicherheit für Medizinprodukte

Executive Briefing

Cybersicherheit für Medizinprodukte – die Herausforderung im Gesundheitswesen

Krankenhäuser und ähnliche Einrichtungen des Gesundheitswesens haben in der Regel **300 %** bis **400 %** mehr medizinische Geräte als IT-Geräte.[1]

Die Gefahr von Sicherheitsverletzungen im Gesundheitswesen ist allgegenwärtig und kostspielig. Im Jahr 2018 gab es laut HIPAA Journal 365 gemeldete Datenschutzverletzungen im Gesundheitswesen, die 500 oder mehr Datensätze betrafen – ein Anstieg von 83 % gegenüber dem Jahr 2010.

Es gibt Hinweise darauf, dass finanziell motivierte Cyberkriminelle die primären Angreifer gegen Netzwerke und Medizingeräte im Gesundheitswesen sind. Ziel dieser Hacker ist es, medizinische Daten zu stehlen und dann im Dark Web zu verkaufen oder mit dem Netzwerk verbundene Geräte zu verschlüsseln, um alle Aktivitäten zum Stillstand zu bringen und Lösegeld zu fordern. Durch die Unterbrechung von Krankenhaus- und Pflegeheimnetzwerken konnten sie in den vergangenen Jahren Organisationen des Gesundheitswesens unter Druck setzen, damit diese Lösegeld zahlen, um so ihren Betrieb schneller wieder aufnehmen und dadurch Leben retten zu können.

In Anbetracht wachsender Gefahren muss der Gesundheitssektor seine Sicherheitsstrategien weiterentwickeln, um über den Schutz von Daten hinauszugehen, Ausfallzeiten von beeinträchtigten Geräten zu verhindern und die Patientensicherheit rund um die Uhr gewährleisten zu können. Angesichts der häufigen Ransomware-Angriffe und des durch Covid-19 verschärften Budgetdrucks müssen Krankenhäuser die Cybersicherheit für Medizingeräte verbessern, haben dafür aber nur sehr begrenzte Ressourcen.

Eine Umfrage von CynergisTek bei der CAPP Community Conference im Jahr 2019 ergab, dass ein Drittel der Führungskräfte die Sicherheit von Medizinprodukten als eines der fünf größten Risiken im Gesundheitswesen ansieht, doch die meisten gaben an, dass es ihnen an einer effektiven Strategie zur Bewertung der von Medizinprodukten ausgehenden Risiken fehlt.[2] Bemerkenswert ist, dass mehr als ein Viertel der Befragten angaben, überhaupt keinen Prozess zur Risikoeinschätzung zu haben.

[1] Medical Device Security, HIMSS.org
[2] https://cynergistek.com/cynergisteks-survey-data-reveals-leading-cybersecurity-concerns-for-healthcare-organization-executives/

Zusammenarbeit ist der Schlüssel für eine wirksame Cybersicherheit Ihrer Medizingeräte

Mit branchenführenden Cybersicherheitsstrategien sowohl für die eigenen Produkte als auch für die Software von Drittanbietern in den eigenen Systemen, verfolgt Philips eine Politik der proaktiven Cybersicherheit mit kollaborativem Informationsaustausch. Eine effektive Cybersicherheit für medizinische Geräte ist nicht nur eine Angelegenheit des Geräteherstellers, sondern erfordert die Zusammenarbeit zwischen Krankenhäusern, Herstellern, Aufsichtsbehörden wie der BfArM und der Forschungsgemeinschaft, die für einen erfolgreichen lückenlosen Schutz von Krankenhäusern und ihren Patienten unerlässlich ist.

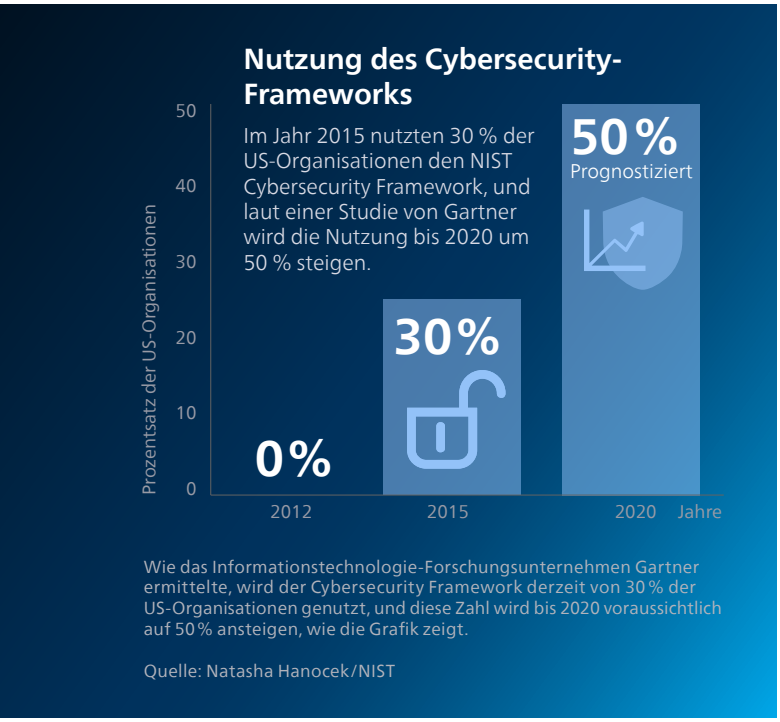
Gal Gnainsky von Philips Group Security erklärt, wie Philips sich dafür engagiert, proaktiv die Sicherheitsbelange seiner Kunden in den Mittelpunkt zu stellen und Partnerschaften schmiedet, um seine visionären Cybersicherheitsstrategien für medizinische Geräte umzusetzen:

„Wir betrachten das Gesundheitswesen als das Lieferorgan, in das wir Kernfunktionen für allgemeine und für medizinische Cybersicherheit einführen müssen. Dies ist jedoch ein komplexer Prozess, denn wenn er nicht effizient organisiert ist, führt er zu betrieblichen Herausforderungen, wie z. B. zu erhöhten Ausfallzeiten und erhöhten Fixkosten. Um dem zu begegnen, stimmen unsere Lösungen betriebliche technische Wartungsabläufe und Cybersecurity-Workflows aufeinander ab, wo immer es möglich ist. Unsere Cybersecurity-Services sind auf unsere technischen Dienstleistungen abgestimmt und decken alle angeschlossenen Geräte im medizinischen Bereich ab.

Als Medizinprodukthersteller und Unternehmen der Gesundheitstechnologie arbeiten wir bei Philips partnerschaftlich mit unseren Kunden zusammen, um umfassende Cybersicherheits- und Datensicherheitsstrategien für Medizingeräte zu definieren und zu implementieren. Um unsere Bemühungen zu koordinieren, haben wir eine globale Richtlinie erstellt, die sich mit der sich ständig weiterentwickelnden Sicherheit in der Medizintechnik befasst, einschließlich der Anforderungen an Produkteigenschaften, der Bewertung und Verfolgung von Sicherheitsbedrohungen und in Übereinstimmung mit den Anforderungen der lokalen Behörden."

NIST-basierte Dienstleistungen helfen, die Herausforderungen der Cybersicherheit für Medizingeräte zu meistern

Philips bietet Kunden eine umfassende Palette an Cybersicherheitsdiensten für den medizinischen Bereich, um sie bei der Bewältigung ihrer Cybersicherheitsrisiken bei vernetzten Medizingeräten und dem Schutz ihrer kritischen Ressourcen zu unterstützen. Unsere Lösungen wurden im Einklang mit globalen Best Practices für Cybersicherheit entwickelt und basieren auf dem NIST-Cybersicherheits-Framework (US National Institute of Standards and Technology). Sie decken so das gesamte Spektrum von Identifizierung, Schutz, Erkennung, Reaktion und Wiederherstellung ab.



Wie das Informationstechnologie-Forschungsunternehmen Gartner ermittelte, wird der Cybersecurity Framework derzeit von 30 % der US-Organisationen genutzt, und diese Zahl wird bis 2020 voraussichtlich auf 50 % ansteigen, wie die Grafik zeigt.

Quelle: Natasha Hanocek/NIST

Da der privilegierte Zugriff, der für Fernwartungsdienste erforderlich ist, ein erhebliches Risiko für Leistungserbringer im Gesundheitswesen darstellen kann, bietet Philips außerdem eine umfassende Überwachung des Fernzugriffs und eine mögliche Integration mit führenden Lösungen für das Fernwartungszugriffsmanagement an. Und da viele Leistungserbringer im Gesundheitswesen wirtschaftliche Gründe haben, Altsysteme weiter zu nutzen, helfen die sicheren Lebensdauerverlängernden Services von Philips den Kunden, die Nutzungsdauer ihrer medizinischen Geräte zu maximieren, indem sie Upgrade-Pfade und entschärfende Kontrollen zur Aufrechterhaltung akzeptabler Sicherheitsbedingungen bereitstellen. Durch die integrierte Betrachtung von Mensch, Prozess und Technologie helfen die Beratungsdienstleistungen von Philips den Kunden bei der Einhaltung gesetzlicher Vorschriften sowie bei der Risiko- und Schwachstellenbewertung von medizinischen Systemen. Wir implementieren Sicherheitsstandards, welche die aktuellen gesetzlichen Vorschriften und die Best Practices der Branche erfüllen oder übertreffen, darunter:

- Die Risikoanalysen zur Produktsicherheit von Philips sind mit dem von der FDA empfohlenen Standard ISO/IEC-80001 und zahlreichen anderen Standards wie NIST 800- 53 Rev 4, ITIL v3.1.24 und den Standards der ISO/IEC-27000-Serie abgestimmt.
- Philips ist sowohl konform mit der ISO 14971, der EU-Richtlinie 95/46/EC als auch den HIPAA-Sicherheits- und Datenschutzbestimmungen.
- Erstellung von kundenorientierten Informationen, wie z. B. das branchenübliche „Manufacturer Disclosure Statement for Medical Device Security" (MDS2).
- Unterstützung beim FDA-Leitfaden zum Premarket Management der Cybersicherheit bei Medizinprodukten und dem FDA Postmarket Management der Cybersicherheit bei Medizinprodukten.
- Geschulte Philips Fachleute verfügen über beträchtliches Fachwissen in den Bereichen Cybersicherheit und Medizinprodukte. Zertifizierungen wie ISO27001, SOC 2 und HIPAA helfen beim Aufbau einer Vorreiterrolle und Glaubwürdigkeit im Bereich Cybersicherheit für Medizinprodukte.

Und natürlich bietet die Philips Healthsuite Plattform (HSP) auch die Grundlagen und den Rahmen für Sicherheit und Datenschutz in der vernetzten Cloud. Innerhalb der vernetzten Philips Healthsuite Cloud bildet das Information Security Management System (ISMS) diesen Rahmen, der Sicherheits- und Datenschutzaspekte bei der Erstellung von Plattformprodukten und -services sowie die Prozesse zur Risikobewertung und zum Vorfallmanagement steuert. Sicherheitsmaßnahmen sind auf verschiedenen Ebenen eingebettet – Anwendungssicherheit, Rechnersicherheit, Datensicherheit, Informationssicherheit, Netzwerksicherheit – sowie administrative und betriebliche Schutzmaßnahmen. Sicherheits- und Datenschutzmaßnahmen sind im Entwicklungsprozess von Beginn an vorgeschrieben, um einen effizienten Datenschutz über alle Plattformfunktionen hinweg zu gewährleisten.

Philips übernimmt auch eine führende Rolle bei der Zusammenarbeit mit Aufsichtsbehörden wie dem BfArM oder der FDA und internationalen Regulierungsbehörden, Industriepartnern und Leistungserbringern, um Schwachstellen zu schließen und Schutzmaßnahmen zu implementieren. Das Unternehmen beteiligt sich aktiv an maßgeblichen Branchenverbänden, die sich mit Sicherheit oder Datenschutz befassen, darunter ZVEI, bvitg, AdvaMed, MITA und vielen anderen weltweit, und engagiert sich ebenfalls für Best Practices zur Identifizierung, Behebung und Veröffentlichung potenzieller Schwachstellen. Die Cybersicherheitsbeauftragten von Philips haben im Rahmen von Arbeitsgruppen für Cybersicherheit eine führende Rolle bei der Schaffung globaler Standards übernommen, darunter die International Cybersecurity Guidance Initiative des International Medical Device Regulation Forum (IMDRF).

Wie man medizinische Geräte absichert und kritische Ressourcen handhabt

Bei der Entwicklung eines Geräts – oder bei der Bewertung der Risiken, die mit der Verwendung eines Geräts verbunden sind – wendet Philips Group Security das NIST-Cybersicherheits-Framework for Improving Critical Cybersecurity Version 1.1 an.

Dieses freiwillige Rahmenwerk besteht aus Standards, Richtlinien und Best Practices zum Umgang mit Cybersicherheitsrisiken. Die Hauptakteure des Frameworks sind zwar Eigentümer und Betreiber kritischer Infrastrukturen aus dem US-Privatsektor, aber die Anwenderbasis umfasst inzwischen auch Gemeinden und Organisationen auf der ganzen Welt.

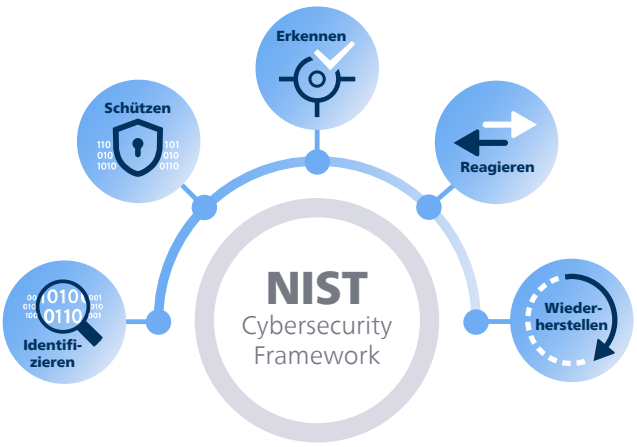
Der Kern des Frameworks besteht aus einer Reihe von Cybersicherheitsaktivitäten, angestrebten Ergebnissen und anwendbaren Referenzen, die in allen Sektoren kritischer Infrastrukturen gleich sind. Ein Beispiel für ein angestrebtes Ergebnis ist: „Physische Geräte und Systeme innerhalb der Organisation sind inventarisiert."

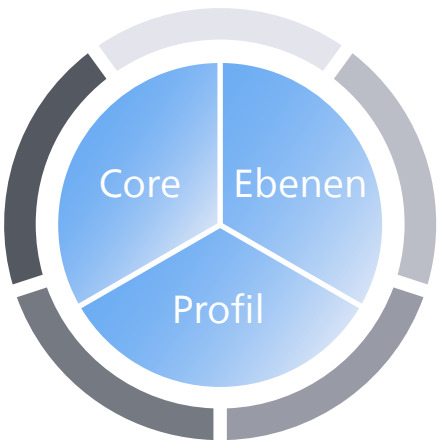
Der Kern wird aus branchenüblichen Standards, Richtlinien und Praktiken in einer Art und Weise gebildet, welche die Kommunikation von Cybersicherheitsaktivitäten und -ergebnissen in der gesamten Organisation von der Führungsebene bis zur Implementierungs-/ Betriebsebene ermöglicht.

Das NIST Cybersecurity Framework

Der Kern des NIST-Cybersicherheits-Frameworks setzt sich aus fünf parallellaufenden und kontinuierlichen Funktionen zusammen – Identifizieren, Schützen, Erkennen, Reagieren, Wiederherstellen. Zusammen betrachtet bieten diese Funktionen eine übergeordnete, strategische Sicht auf den Lebenszyklus des Managements von Cybersicherheitsrisiken in einer Organisation. Der Kern des NIST-Cybersecurity-Frameworks identifiziert dann die zugrundeliegenden Schlüsselkategorien und Unterkategorien für jede Funktion und gleicht sie mit informativen Beispielen ab, wie z. B. bestehenden Standards, Richtlinien und Praktiken für jede Unterkategorie.

Das NIST-Cybersicherheits-Framework integriert branchenübliche Standards und Best Practices, um Organisationen beim Management ihrer Cybersicherheitsrisiken zu unterstützen. Er bietet eine gemeinsame Sprache, die es Mitarbeitern auf allen Ebenen einer Organisation – und an allen Punkten einer Lieferkette – ermöglicht, ein gemeinsames Verständnis ihrer Cybersicherheitsrisiken zu entwickeln. NIST hat mit Experten aus der Privatwirtschaft und der Regierung an der Erstellung des Frameworks zusammengearbeitet, welcher Anfang 2014 veröffentlicht und vom US-Kongress im Rahmen des Cybersecurity Enhancement Act aus dem Jahr 2014 verabschiedet wurde.





Die Implementierungsebenen des Frameworks unterstützen Organisationen, indem sie einen Kontext dafür liefern, wie eine Organisation das Cybersecurity-Risikomanagement sieht. Die Ebenen leiten Organisationen an, das angemessene Maß an Stringenz für ihr Cybersicherheitsprogramm zu bestimmen, und werden oft als Kommunikationsinstrument verwendet, um Risikobereitschaft, Auftragspriorität und Budget zu thematisieren.

Framework-Profile sind die individuelle Ausrichtung der organisatorischen Anforderungen und Ziele, der Risikobereitschaft und der Ressourcen einer Organisation für die angestrebten Ergebnisse des NIST Cybersecurity Frameworks. Profile werden in erster Linie verwendet, um Möglichkeiten zur Verbesserung der Cybersicherheit in einer Organisation zu identifizieren und zu priorisieren.

Ausgerichtet auf unseren Philips Fokus der Operativen Intelligenz und Zusammenarbeit bietet das NIST Cybersecurity Framework eine Anleitung, die für die gesamte Organisation nützlich ist. Der volle Nutzen des Frameworks wird nicht ausgeschöpft, wenn nur die IT-Abteilung ihn verwendet. Das Framework bietet ein umfassendes Risikomanagement, welches an die jeweilige Zielgruppe anpassbar ist. Genauer gesagt entsprechen die Funktions-, Kategorie- und Unterkategorie-Ebenen des Frameworks gut den verschiedenen Ebenen der Fachleute auf Organisations-, Projekt-, Geschäfts- und IT-Ebene sowie IT- und IoT-Systemen. Dies ermöglicht eine genaue und sinnvolle Kommunikation, von der Unternehmensleitung bis hin zu den einzelnen Geschäftseinheiten und mit Partnern in der Lieferkette. Es kann besonders hilfreich bei der Verbesserung der Kommunikation und des Verständnisses zwischen IT-Spezialisten, IoT-Betreibern und den Führungskräften in der Organisation sein.

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