ivanti Neurons

Gesundheitswesen, IT, Biomedizin, Sicherheit

Leitfaden zur Verbesserung der Sichtbarkeit und zur Minderung von Sicherheitsrisiken für medizinische Geräte

Inhaltsverzeichnis

Einführung

Vernetzte medizinische Geräte stellen eine große Herausforderung für IT-, Biomedizin- und Sicherheitsorganisationen im Gesundheitswesen dar. Sie sind von Natur aus anfällig für Cyber-Bedrohungen und erfolgreiche Cyber-Angriffe können dramatische Folgen haben. Dennoch können herkömmliche Cyber-Sicherheitsmaßnahmen nicht auf diese Geräte angewandt werden und riskieren womöglich sogar die Beeinträchtigung kritischer klinischer Abläufe.

In diesem Leitfaden gehen wir einen dreistufigen Prozess durch, der dabei hilft, die Einblicke in medizinische Geräten zu erhöhen und Sicherheitsrisiken zu minimieren. Die Etablierung von Cybersicherheitsschichten für medizinische Geräte ist ein mehrstufiger, fortlaufender Prozess, der erfolgreich sein kann, wenn er von einer starken Basis ausgeht und einen methodischen, systematischen Ansatz verfolgt.

Erfahren Sie, wie Sie Cybersecurity-Risiken im Zusammenhang mit vernetzten medizinischen Geräten erkennen, bewerten und abmildern können. Die drei Phasen, die wir in diesem Leitfaden vorstellen, sind kein einmaliger Prozess, sondern sollten vielmehr als Zyklus behandelt werden. IT- und Sicherheitsteams in Gesundheitszentren sollten diese Phasen kontinuierlich durchführen – die Umgebung untersuchen, Risiken bewerten und Sicherheitsprobleme angehen, die sie im Alltag entdecken.

Wie anfällig sind medizinische Geräte für Cyberangriffe?

Immer mehr medizinische Geräte sind mit Netzwerken oder anderen Geräten verbunden, was eine große Sicherheitslücke für Krankenhäuser und Gesundheitsdienstleister darstellt. Viele dieser Geräte sind nicht sicher und werden nicht aktiv verwaltet, was Tür und Tor für eine Vielzahl von Cybersicherheitsbedrohungen öffnet.

Warum sind medizinische Geräte verwundbar?

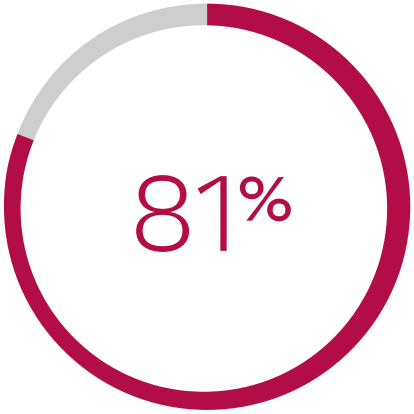
- Der Softwarecode wurde keiner Sicherheitsüberprüfung unterzogen.
- Die Authentifizierung ist schwach oder nicht vorhanden.
- Datenübertragungswege sind oft unsicher und unverschlüsselt.
- Begrenzte Einblicke, welche Geräte aktiv genutzt werden.
- Fehlende Möglichkeiten zur Überwachung von Geräteaktivitäten und Sicherheitsvorfällen.
- Außer Betrieb genommene Geräte werden nicht sicher entsorgt.
- Software-Updates sind nicht verfügbar oder werden nur selten bereitgestellt.

Die Umgebung verstehen
Entdecken Sie, welche IT- und Medizingeräte es gibt, klassifizieren Sie diese genau, verstehen Sie ihren klinischen Kontext und identifizieren Sie die jeweiligen Netzwerkanforderungen.

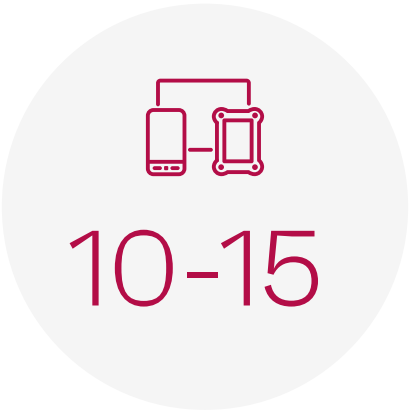
Risikobewertung
Identifizieren Sie Geräte-Schwachstellen und netzwerkbezogene Risiken, weisen Sie jedem Gerät einen Risiko-Index zu und stellen Sie Empfehlungen für Abhilfemaßnahmen bereit.

Geräte schützen
Berücksichtigen Sie die Sicherheit auf Geräteebene, indem Sie Geräte innerhalb des LANs isolieren und unerwünschte Kommunikation über LAN/WAN verhindern. Bereiten Sie darüber hinaus eine Strategie zur Erkennung von Sicherheitsvorfällen vor, sollten diese auftreten.

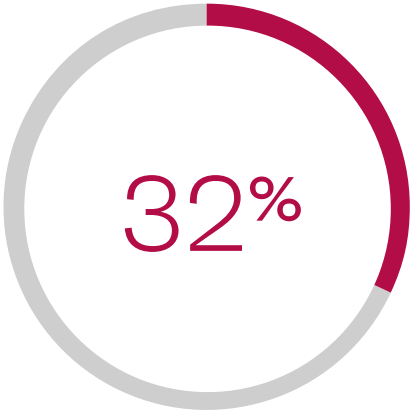
Wie groß ist das Problem?



81 % der Organisationen im Gesundheitswesen gaben an, in den letzten zwei Jahren von einem Cyberangriff betroffen gewesen zu sein.



Krankenhäuser unterhalten 10 - 15 angeschlossene medizinische Geräte pro Bett, mit über 3,7 Millionen Geräten im aktiven Einsatz.



32 % der Organisationen im Gesundheitswesen geben an, dass medizinische Geräte ihr größtes Sicherheitsproblem sind.

Quelle: KPMG, Wired

Welche Bedrohungsvektoren betreffen medizinische Geräte?

Malware
Medizinische Geräte haben in der Regel keinen Endpunktschutz und sind besonders anfällig für Malware.

Bedrohungen von innen
Aufgrund der schwachen Authentifizierung können böswillige Insider leicht unbefugten Zugriff erhalten und Geräte manipulieren.

Angriffe auf Webanwendungen
Einige medizinische Geräte können über eine Weboberfläche verwaltet werden, was eine Reihe von Cyber-Risiken wie Code-Injektion, Cross-Site-Scripting (XSS) und Path-Traversal birgt.

Geräte-Missbrauch
Vernetzte medizinische Geräte basieren oft auf Windows-PCs. Das Krankenhauspersonal kann die Geräte nutzen, um im Internet zu surfen oder Software zu installieren, was ein zusätzliches Risiko darstellt.

Wie können Sie das Cybersecurity-Risiko und die Auswirkungen eines Angriffs bewerten?

Die FDA-Richtlinien für Medizinprodukte bieten eine nützliche Klassifizierung der Geräterisikostufen.

Stufe 1: Erhöhtes Cybersecurity-Risiko	Stufe 2: Standard-Cybersicherheitsrisiko
Das Gerät:	**Das Gerät:**
Kann an ein anderes medizinisches oder nichtmedizinisches Produkt, an ein Netzwerk oder an das Internet angeschlossen werden. ODER Ein Cybersicherheitsvorfall, der das Gerät betrifft, könnte einem oder mehreren Patienten direkt schaden.	Kann eine Verbindung zu einem anderen Gerät oder Netzwerk herstellen, kann aber Patienten nicht direkt schaden. ODER Kann Patienten direkt Schaden zufügen, kann aber keine Verbindung zu einem Netzwerk herstellen.

Um eine detailliertere Bewertung des Risikos zu erhalten, verwenden Sie ein Framework wie die CVSS-Risikoberechnung. Berücksichtigen Sie bei der Bewertung des Cybersicherheitsrisikos die folgenden Faktoren:

- Software-Schwachstellen
- Authentifizierung
- Vernetzung
- Patientensicherheit
- Datenschutz
- Serviceunterbrechung

Phase I:

Verstehen der Connected-Device-Umgebung

Der erste Schritt zur Lösung eines Problems ist zu erkennen, dass es existiert und zu seinen Umfang zu vernetzten. Das Problem der vernetzten medizinischen Geräte wird von den IT-, Biomedizin- und Sicherheitsteams in Krankenhäusern und Gesundheitsorganisationen aufgrund der extrem eingeschränkten Sichtbarkeit nicht gut verstanden.

Sicherheitsteams sehen medizinische Geräte als Blackbox oder können sie überhaupt nicht sehen

Die Sicherheit medizinischer Geräte wird zu einer gemeinsamen Aufgabe von klinischen Entwicklungsteams und IT-Abteilungen. Die Informationen über diese Geräte sind zwar in den Organisationen des Gesundheitswesens vorhanden, aber die Sicherheitsteams können nicht ohne Weiteres darauf zugreifen.

Die folgenden wichtigen Fragen bleiben unbeantwortet:

1. Wie viele Geräte sind angeschlossen?
2. Um welche Arten von Geräten handelt es sich?
3. Mit welchen anderen Geräten oder Netzwerken kommunizieren sie?
4. Ist das Netzwerkverhalten normal und erwartet oder anomal?

Warum ist es schwierig, ein Inventar der angeschlossenen medizinischen Geräte zu erstellen?

Sie können nicht einfach einen Netzwerkscan durchführen und medizinische Geräte identifizieren, wie Sie es in einem normalen IT-Netzwerk tun würden:

- Geräte sind empfindlich – aktives Scannen des Netzwerks kann den Betrieb medizinischer Geräte stören, daher müssen Sie die passive Erkennung verwenden.
- Unsichtbar für Netzwerkerkennungs-Tools – herkömmliche Tools erkennen die große Mehrheit der angeschlossenen medizinischen Geräte nicht oder zeigen fälschlicherweise an, dass es sich bei dem Gerät um eine Windows-Workstation handelt. Die meisten angeschlossenen medizinischen Geräte geben ihre Informationen nicht bekannt, und ihre Erkennung über das Netzwerk erfordert eine sorgfältige Analyse des Datenverkehrs auf der Anwendungsebene.
- Große Anzahl und Vielfalt von Geräten – es kann Zehntausende von Geräten unterschiedlicher Typen, Hersteller und Versionen geben.
- Ständiger Wandel – Geräte werden ständig hinzugefügt, ausgetauscht oder aus dem Netzwerk entfernt, oft ohne Beteiligung der IT-Abteilung, so dass die Erkennung und Inventarisierung ein kontinuierlicher Prozess sein muss.

Schritt 1. Entdeckung

Zielen Sie darauf ab, eine Datenbank mit Daten zu den einzelnen medizinischen Geräten aufzubauen. Konzentrieren Sie sich auf hochwertige Daten, mit denen Sie Risiken und Schwachstellen ermitteln können. Im Besonderen:

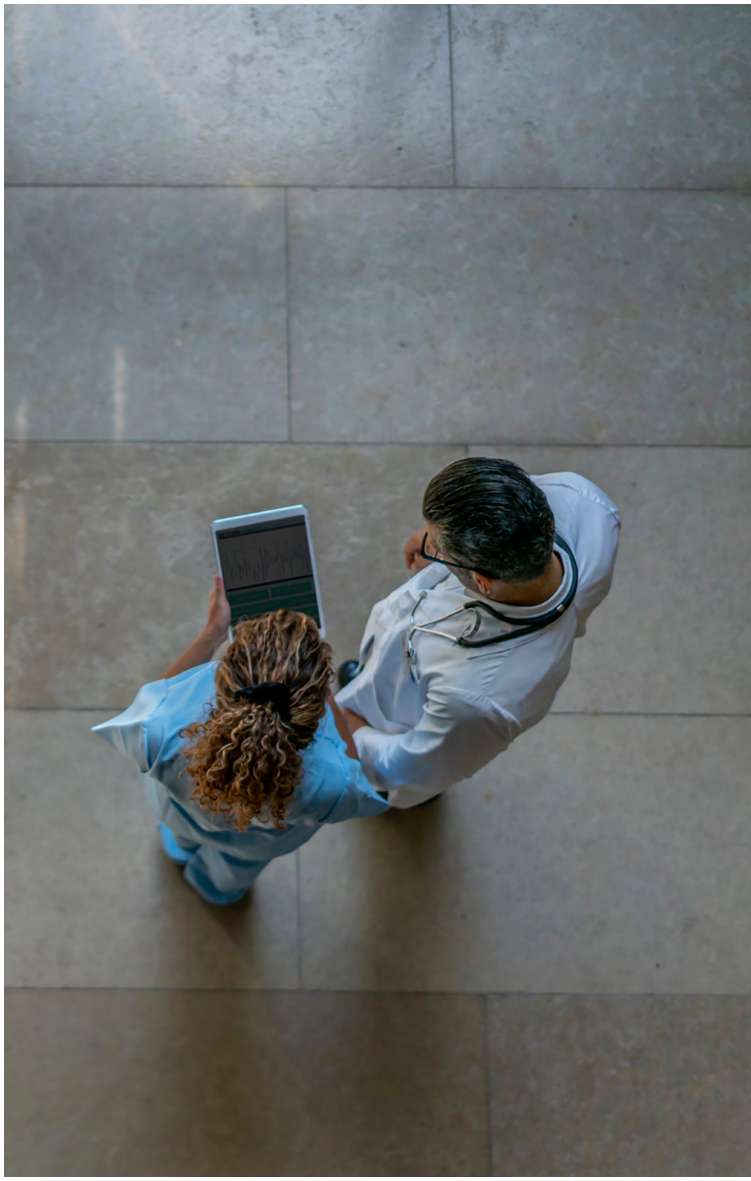
- Gerätetyp
- Abteilung und Raum
- Verkäufer
- Modell
- IP-Adresse
- Betriebssystem
- Version der Anwendungssoftware
- Aktuelle Sicherheitspatches

Schritt 2. Netzwerk-Mapping und klinischer Kontext

Wenn Sie das Netzwerkverhalten eines Geräts verstehen, können Sie nachvollziehen, wie anfällig es für externe und interne Bedrohungen ist. Versuchen Sie, die folgenden Informationen für jedes Ihrer angeschlossenen Geräte zu erhalten:

- Mit welchen anderen Geräten kommuniziert es?
- Hat dieses Gerät unnötigen Zugriff auf andere Geräte, Netzwerke oder das Internet?
- Ist die Netzwerkkommunikation dieses Geräts in einem VLAN isoliert?
- Welche Arten von Protokollen werden verwendet?
- Wohin sendet oder empfängt das Gerät Gesundheitsdaten (Public Health Information, PHI) und welche Art von PHI?
- Kommuniziert es extern über das Internet?
- Muss das Gerät laufend mit dem Gerätehersteller kommunizieren?
- Ist die Internetkommunikation für diesen Gerätetyp normal?
- Ist die Internetkommunikation dieses Geräts durch einen VPN-Tunnel isoliert?

Klären Sie die klinische Verwendung jedes Geräts und damit auch sein Gefährdungspotenzial. Diese Daten können ohne die Hilfe von automatisierten Tools extrem schwierig zu erhalten sein.



Phase II:

Risikobewertung

Sobald Sie ein besseres Verständnis für Ihre angeschlossenen medizinischen Geräte haben und ein Inventar der Geräte, ihres Kontexts und ihres Netzwerkverhaltens erstellt haben, können Sie dieses Inventar nutzen, um die Risiken für jedes Gerät und deren Auswirkungen auf das Unternehmen zu bewerten.

Schritt 1. Identifizieren von Geräteschwachstellen und Möglichkeiten zur Behebung

Sammeln Sie Daten über Sicherheitslücken für jedes Ihrer Gerätemodelle, Betriebssysteme und Anwendungsversionen. Genauso wichtig ist es, den Besitzer des Geräts und Ihre Zugriffsebene für die Behebung von Sicherheitsproblemen zu ermitteln.

Auswirkungen von Software-Schwachstellen
Verwenden Sie die CVSS-Risikoberechnung, um die Auswirkungen bekannter Software-Schwachstellen in Ihren angeschlossenen Geräten zu ermitteln.

Fehlkonfigurationen
Prüfen Sie auf allgemeine Schwachstellen wie fest kodierte oder voreingestellte Passwörter, ungepatchte Betriebssysteme oder Software.

Geräteauthentifizierung
Stellen Sie fest, ob das Gerät über eine Authentifizierung verfügt und wenn ja, wie stark diese ist und ob sichere Passwörter festgelegt wurden.

Kontaktstelle
Wer verwaltet das Gerät - die klinische Technik, die IT, der Hersteller oder ein Drittanbieter?

Einfacher Zugang
Hat das Sicherheitsteam Zugriff auf dieses Gerät, um Sicherheitskontrollen zu implementieren oder auf Vorfälle zu reagieren?

Sicherung
Verfügt das Gerät über ein Backup oder eine Redundanz, und wie wirkt sich eine Betriebsunterbrechung aus?

Schritt 2. Identifizieren von Risiken auf Netzwerkebene

Schwachstellen bei medizinischen Geräten sind nur ein Aspekt des Risikos. Analysieren Sie die Netzwerkkonnektivität und identifizieren Sie Vektoren, über die sich Angreifer mit Ihren Geräten verbinden können.

Internetverbindung
Prüfen Sie, ob das Gerät über das Internet eine Verbindung zu anderen Systemen herstellt, z. B. zu einer Fremdfirma oder dem Hersteller für Wartung oder Updates.

Verbindungen zu unsicheren Geräten
Prüfen Sie, ob das Gerät eine Verbindung zu einem weniger sicheren Gerät oder Endpunkt herstellen kann, z.B. der Workstation eines Arztes, und ob es Management- oder Datendienste wie FTP oder SSH offenlegt.

Verschlüsselung
Prüfen Sie, ob das Gerät unverschlüsselte Datenströme sendet oder empfängt.

Unsichere Protokolle
Prüfen Sie, ob das Gerät Protokolle verwendet, die eine schwache oder keine Authentifizierung bieten oder Sicherheitslücken aufweisen.

Schritt 3. Identifizieren Sie die Schwere des Risikos

Fragen Sie sich selbst: Was wären die Auswirkungen eines erfolgreichen Cyber-Angriffs auf jedes Ihrer Geräte? Im Gegensatz zu Angriffen auf IT-Systeme im Gesundheitswesen sind die Auswirkungen eines Angriffs auf verbundene Geräte nicht auf die Datensicherheit und den Datenschutz beschränkt. Ein erfolgreicher Cyberangriff könnte die klinische Versorgung unterbrechen und Patienten direkt schädigen.

Wir empfehlen, den Schweregrad des Risikos anhand der drei Auswirkungsmetriken in der CVSS-Risikoberechnung zu ermitteln:

- Vertraulichkeit – entspricht dem Risiko der Exposition geschützter Gesundheitsinformationen (PHI), die im Gerät gespeichert sind oder von diesem übertragen werden.
- Integrität – bezieht sich auf das Risiko für die Patientensicherheit bei Produkten, die direkt in der Patientenversorgung eingesetzt werden.
- Verfügbarkeit – entspricht dem Risiko einer Dienstunterbrechung.

Patientensicherheit	Datenschutz	Betriebsunterbrechung
NIEDRIG: FDA-Medizinprodukt der Klasse I; geringes bis mäßiges Risiko für den Patienten oder Anwender.	**NIEDRIG:** Gerät speichert keine PHI.	**NIEDRIG:** Geräteausfall kann die Patientenversorgung nicht stören.
MITTEL: Medizinprodukt der FDA-Klasse II; mittleres bis hohes Risiko.	**MITTEL:** Das Gerät speichert eine geringe Menge an PHI für einen begrenzten Zeitraum rund um einen Test oder eine Behandlung.	**MITTEL:** Geräteausfall kann die Patientenversorgung stören, aber nicht eine kritische medizinische Behandlung.
HOCH: Gerät der FDA-Klasse III; hohes Risiko, Geräte, die Leben erhalten oder unterstützen, implementiert sind oder ein hohes Risiko für Krankheiten oder Verletzungen darstellen.	**HOCH:** Gerät speichert große Mengen von PHI über mehrere Tests oder Behandlungen.	**HOCH:** Geräteausfälle können kritische medizinische Behandlungen wie Operationen, Beatmungsgeräte oder die Verabreichung von lebenserhaltenden Medikamenten unterbrechen.

Phase III:

Schutz von angeschlossenen medizinischen Geräten

Der Vorteil unseres strukturierten Prozesses für die Erkennung und Risikobewertung ist, dass Sie die Geräte nach den Risiken einstufen können, die sie darstellen. Jedes Gerät sollte einen Risikoauswirkungs-Score haben (für Patientensicherheit, Datenschutz und Serviceunterbrechung).

Ihr Unternehmen kann ein akzeptables Risikoniveau definieren. Das Sicherheitsteam kann sich auf den Schutz von Geräten konzentrieren, deren Risikowert über dem akzeptablen Niveau liegt, und kann die entsprechenden Sicherheitsmaßnahmen auf Geräte mit unterschiedlichen Risikowerten anwenden.

Wir empfehlen, angeschlossene medizinische Geräte in vier Schritten zu schützen:

Schritt 1. Geräteabsicherung

Wie bei jedem Computergerät müssen Sie sicherstellen, dass angeschlossene medizinische Geräte über die neuesten Sicherheits-Patches und Software-Upgrades verfügen. Die Konfiguration muss abgesichert sein, um eine geschützte Authentifizierung zu ermöglichen. Schließen Sie ungenutzte Ports, beschränken Sie unnötige Funktionen und reduzieren Sie generell die Angriffsfläche.

Die meisten medizinischen Geräte laufen unter einem Windows-Betriebssystem. Das Einspielen eines Patches ist jedoch nicht so einfach wie bei einer Workstation oder einem Windows-Server.

Herausforderungen bei der Sicherung von medizinischen Geräten

- Windows-Sicherheitspatches müssen vom Gerätehersteller überprüft und freigegeben werden.
- Die Medizintechnik muss Patches oder Updates verifizieren, die die Funktionalität des Medizinprodukts nicht beeinträchtigen.

Richtlinien

- Es wird Ihnen nicht gelingen, alle Sicherheits-Patches zu installieren oder alle Geräte zu sichern.
- Konzentrieren Sie sich auf Geräte, die einen hohen Risikowert haben.
- Priorisieren Sie Sicherheitspatches oder Konfigurationsänderungen, die die bekannten Schwachstellen beheben, die Sie in Ihrer Risikobewertung identifiziert haben.

Schritt 2. Netzwerk-Isolierung

Eine Schlüsselstrategie zur Absicherung angeschlossener medizinischer Geräte besteht darin, sie so weit wie möglich von der nicht-kritischen klinischen Kommunikation zu isolieren, um die Angriffsfläche zu begrenzen. Dies hat zwei Komponenten:

- Definition einer Netzwerksegmentierung, um sicherzustellen, dass angeschlossene medizinische Geräte nur mit Geräten oder Systemen kommunizieren können, die Teil ihres klinischen Prozesses sind.
- Blockieren der externen Kommunikation, um sicherzustellen, dass angeschlossene medizinische Geräte niemals eine Verbindung mit dem Internet herstellen, es sei denn, dies ist für die Kommunikation mit dem Gerätehersteller oder anderen bekannten Einrichtungen erforderlich.

Überlegungen bei der Isolierung von medizinischen Geräten

- Isolieren Sie klinische Datenströme von nicht-klinischen Datenströmen.
- Klinische Kommunikation ist wichtig, aber jede andere Kommunikation sollte blockiert werden.

Richtlinien

- Legen Sie strenge Zugriffsrichtlinien und eine Netzwerksegmentierung fest, um die Kommunikation von/zu Geräten einzuschränken, die nicht benötigt werden.
- Legen Sie eine Segmentierungsrichtlinie fest, um Risiken und Schwachstellen zu adressieren, die in Ihrer Auswirkungsanalyse entdeckt wurden.
- Sperren Sie die Verbindung des Geräts mit dem Internet, es sei denn, dies ist für die Funktion des Geräts unbedingt erforderlich, und selbst dann nur mit bekannten Einrichtungen.
- Arbeiten Sie eng mit der Medizintechnik und dem Healthcare Technology Management (HTM) zusammen, um sicherzustellen, dass Sie kritische Datenflüsse nicht unterbrechen.

Schritt 3. Erkennung und Reaktion auf Vorfälle

Es ist unmöglich, die meisten angeschlossenen medizinischen Geräte vor allen potenziellen Bedrohungen zu schützen, da es immer kritische Altgeräte geben wird, die nicht ersetzt und nicht vollständig gepatcht oder isoliert werden können, d.h. Sie können die Angriffsfläche einschränken, aber nicht eliminieren. Darüber hinaus kann die Isolierung ein langwieriger Prozess sein, und in der Zwischenzeit werden einige Geräte anfällig bleiben. Aus diesem Grund ist es wichtig, Geräte zu überwachen und sofort zu erkennen und Alarm zu geben, wenn ungewöhnliche Aktivitäten stattfinden.

Überlegungen bei der Überwachung auf Sicherheitsvorfälle

- Verwenden Sie eine passive Überwachung wie z.B. einen Netzwerk-TAP oder einen Mirror-Port, um den Gerätebetrieb nicht zu unterbrechen.
- Nutzen Sie die Informationen, die Sie über den klinischen Kontext jedes Geräts gesammelt haben, um zu verstehen, was eine normale klinische Kommunikation darstellt.
- Vergleichen Sie das aktuelle Verhalten mit den Spezifikationen des Herstellers, mit dem Verhalten in der Vergangenheit und mit dem Verhalten einer Vergleichsgruppe von Geräten in Ihrer Umgebung und in anderen Unternehmen.

Richtlinien

- Kontinuierliche Überwachung aller Geräte, mit besonderem Augenmerk auf Geräte mit hohem Risikowert.
- Erstellen Sie eine Strategie zum Vergleich der laufenden Kommunikation mit der normalen klinischen Kommunikation.
- Alarmieren Sie den Sicherheitsdienst bei jeder größeren Abweichung vom normalen Verhalten.
- Integration mit Drittanbietern, die bei der schnellen Behebung von Problemen per Fernzugriff helfen können, z. B. bei der Netzwerksegmentierung auf Abruf.

Schritt 4. Metriken und Analysen

Die Cybersicherheit von Medizinprodukten ist ein langwieriger Prozess, der im Laufe der Zeit überprüft und verbessert werden muss, um sich an eine sich ständig verändernde Bedrohungslandschaft anzupassen.

Die Nachverfolgung Ihres Fortschritts kann Ihnen helfen zu verstehen, ob Sie sich in die richtige Richtung bewegen und Korrekturen vornehmen, wenn Ihre Arbeit die Sicherheitssituation nicht verbessert. Im Folgenden finden Sie einige Richtlinien zur Verfolgung des Fortschritts Ihrer Absicherung medizinischer Geräte.

- Erstellen Sie eine Scorecard für Medizinprodukte mit einer Zeitleiste der Risikobewertungen, um sicherzustellen, dass das Risiko im Laufe der Zeit reduziert wird.

- Identifizieren Sie Aktivitäten und Strategien, die KPIs verbessern und das Gesamtrisiko reduzieren.
- Legen Sie KPIs basierend auf dem Risiko wichtiger Geräte fest und überwachen Sie die Verbesserung; verknüpfen Sie die KPIs mit Geschäftszielen wie Patientensicherheit und Serviceverfügbarkeit, um die Zustimmung der Geschäftsführung zu erhalten.
- Sammeln Sie Daten über Risikoindizes und das historische Verhalten von Geräten und nutzen Sie diese für bessere Beschaffungsentscheidungen.

Verbesserte Geräte-Sichtbarkeit und Sicherheitsrisikominderung für medizinische Geräte mit Ivanti Neurons for Healthcare

Ivanti® Neurons for Healthcare verbessert die Geräte-Sichtbarkeit und mindert Sicherheitsrisiken für medizinische Geräte. Die Lösung erkennt und profiliert auf intelligente Weise medizinische Geräte und Internet of Medical Things (IoMT), bewertet Sicherheitsrisiken, meldet Bedrohungen und gleicht Geräteinformationen über mehrere Datenquellen hinweg ab. Erfahren Sie mehr über die verschiedenen gesundheitsspezifischen Geräte in Ihren Einrichtungen, einschließlich Geräteklassifizierung und Nutzungsinformationen, mit den Details, um Sicherheitsrisiken zu reduzieren oder Anomalien zu beachten. Sammeln Sie Herstellerdaten und gleichen Sie diese ab, um eine einzige vertrauenswürdige Informationsquelle für alle Ihre medizinischen Geräte zu schaffen.

Weitere Informationen finden Sie unter ivanti.de/products/ivanti-neurons-healthcare

ivanti Neurons

ivanti.de/neurons
contact@ivanti.de