Ein genauer Blick auf die Sicherheit im Gesundheitswesen

Forescout analysiert die Bereitstellungsdaten, um die aktuellen Cybersicherheitsrisiken in medizinischen Einrichtungen besser zu verstehen.

FORESCOUT®

Kurzfassung

Das Internet der medizinischen Dinge (Internet of Medical Things, IoMT) bietet weiterhin interessante Möglichkeiten für medizinische Einrichtungen, die Versorgung der Patienten zu verbessern. Die digitale Transformation und die zunehmende Vernetzung bringen jedoch auch neue Datenschutz- und Sicherheitsrisiken mit sich. Die Vielfalt der eingesetzten Geräte nimmt exponentiell zu, sodass die Netzwerke immer komplexer und schwerer verwaltbar werden und der Aufwand für die Verbesserung der Sicherheit zunimmt.

Dieser Bericht soll leitenden Mitarbeitern in medizinischen Einrichtungen mit Verantwortung für Sicherheits- und Risiko-Management wichtige Einblicke dazu liefern, welche Geräte in ihren Netzwerken eingesetzt werden und welche Risiken mit ihnen verbunden sind. Zudem empfiehlt der Bericht einen ganzheitlichen Sicherheitsansatz, der über die Absicherung medizinischer Geräte hinausgeht.

Die für diesen Bericht verwendeten Daten basieren auf der Forescout Device Cloud, einem Repository für Host- und Netzwerkinformationen zu mehr als 8 Millionen individuellen Geräten und damit einem der größten Crowdsourcing-Repositorys für Geräteinformationen. Für diese Untersuchung beschränkten die Forscher die Device Cloud-Analyse auf 75 Bereitstellungen in medizinischen Einrichtungen, die insgesamt mehr als 10.000 virtuelle LANs (VLANs) und 1,5 Millionen Geräte umfassen. Da der Fokus dieses Berichts auf dem aktuellen Stand bei medizinischen Geräten liegt, basieren die hier vorgestellten Ergebnisse zum größten Teil auf der Analyse von mehr als 1.500 medizinischen VLANs mit 430.000 Geräten.

Wichtigste Erkenntnisse

- **Heutige Umgebungen in medizinischen Einrichtungen werden immer heterogener:** Das schnelle Wachstum bei der Zahl und Vielfalt der verbundenen medizinischen Geräte und Betriebssysteme erschwert zunehmend die Absicherung der Netzwerke.
- **Ältere Windows-Versionen stellen eine erhebliche Schwachstelle dar:** Die in vielen Netzwerken weiterhin verwendeten Windows-Versionen werden nicht mehr von Microsoft unterstützt. In Kürze wird der nächste Microsoft Windows-Meilenstein erreicht, sodass zahlreiche weitere Geräte bald nicht mehr unterstützt werden.
- **Es fehlen Segmentierungsstrategien:** Netzwerksegmentierung, eine Best Practice zur Begrenzung lateraler Bewegungen (basierend auf Vertraulichkeit, Speicherort und Bedeutung der Daten) wird in heutigen heterogenen Netzwerken nicht konsequent umgesetzt.
- **Vielfalt bei Geräteanbietern muss eingedämmt werden:** Die wachsende Zahl der Geräteanbieter führt zu erheblichen Kompatibilitätsproblemen sowie zu Problemen mit der Sicherheit und Asset-Verwaltung.
- **Aktivierte gängige Services führen zu anfälligen Netzwerken:** Wenn gängige Protokolle offen zugänglich sind, erhalten Angreifer unkontrollierten Zugang zum Netzwerk.

Cybersicherheit in medizinischen Einrichtungen

Das IoMT erhält auch weiterhin strategische Priorität, da mithilfe dieser Geräte die Patientenbetreuung verbessert, Effizienzen gesteigert und Kosten für das Gesundheitswesen gesenkt werden können. Es ist daher nachvollziehbar, dass medizinische Einrichtungen das IoMT – eine vernetzte Infrastruktur medizinischer Geräte, Software-Anwendungen sowie Systeme und Services zur Patientenversorgung – verstärkt einsetzen. Die schnelle Einführung vernetzter Geräte führt jedoch zu einem schwerwiegenden Nebeneffekt: Sie lenkt davon ab, dass in heutigen konvergenten Umgebungen, die über vernetzte medizinische Geräte hinausgehen, grundlegende Sicherheitsfragen beantwortet werden müssen, sodass schwerwiegende Cybersicherheitslücken entstehen.

Das Internet der medizinischen Dinge (IoMT) ist eine vernetzte Infrastruktur medizinischer Geräte, Software-Anwendungen sowie Systeme und Services zur Patientenversorgung. Im Rahmen dieser Untersuchung wird das IoMT in die Kategorien IoT (Internet of Things, Internet der Dinge) und OT (Operational Technology, operative Technologie) unterteilt.

Rasante Zunahme vernetzter IT- und OT-Geräte im Gesundheitswesen

Die Zahl vernetzter Geräte wächst mit zunehmender Geschwindigkeit und führt zu einer vergrößerten Angriffsfläche, sodass die Sicherheitsmaßnahmen kaum Schritt halten können. Zu diesen Geräten zählen nicht nur medizinische Geräte wie Systeme zur Patientenüberwachung und -identifizierung, Infusionspumpen sowie Bildgebungssysteme, sondern auch Infrastrukturgeräte wie Systeme für Gebäudeautomatisierung, physische Sicherheit, unterbrechungsfreie Stromversorgung, Notstromgeneratoren sowie weitere operative Technologiesysteme und Geräte, die immer häufiger in IT-Netzwerkumgebungen zu finden sind. Aus diesem Grund fällt die OT auch zunehmend in den Verantwortungsbereich der IT-Abteilung. Laut Gartner werden „bis zum Jahr 2021 ganze 70 % aller OT-Sicherheitssysteme von der CIO-, CISO- oder CSO-Abteilung verwaltet, während es heute lediglich 35 % sind“.[1]

Verstehen und Priorisieren der Risiken

Die Konvergenz dieser beiden zuvor getrennten Netzwerke kann zu einer neuen Kategorie von Sicherheitsrisiken führen, da Cyberkriminelle die Möglichkeit erhalten, sich lateral zwischen den miteinander verbundenen IT- und OT-Netzwerken zu bewegen. Die Zunahme der in der Gesundheitsbranche häufigen Fusionen und Übernahmen verstärkt diese Sicherheitsprobleme zusätzlich.

Ebenso wie bei klinischen Diagnosen und Behandlungen müssen CISOs mögliche Risiken schon frühzeitig erkennen und die beste Vorgehensweise priorisieren. Sicherheits- und Risiko-Management-Teams haben jedoch praktisch keine Chance, sämtliche Risiken zu beseitigen. Dennoch ist es durch ein vollständiges Verständnis von Netzwerkbedrohungen und die Lokalisierung der gefährdetsten Geräte möglich, die Produktivität zu maximieren, die Rendite zu steigern und gleichzeitig Risiken im gesamten Netzwerk zu minimieren.

Die wahren Kosten verzögerter Risikoeindämmung

Cybersicherheit und das Gesundheitswesen haben eine weitere Gemeinsamkeit: Die frühzeitige Erkennung und Behandlung führt zu besseren Ergebnissen und kann die Gesamtkosten erheblich senken. Die Statistiken sprechen dafür: Laut *HIPAA (Health Insurance Portability and Accountability Act) Journal* waren im Jahr 2018 bei einer durchschnittlichen Kompromittierung im Gesundheitswesen jeweils 17.974 Datensätze betroffen.[2] Laut Ponemon lagen die durchschnittlichen Behebungskosten pro betroffener Person/personenbezogenem Datensatz im Gesundheitswesen im Jahr 2018 bei 408 USD.[3] Somit liegen die Kosten für die *Eindämmung, Untersuchung und Bekanntmachung pro Kompromittierung* bei 7,3 Millionen USD. Das deckt jedoch nicht alle Kosten ab, da die erheblichen Schäden für die Marke und Reputation der medizinischen Einrichtungen

[1] „Strategic Roadmap for Integrated IT and OT Security“ (Strategische Roadmap für integrierte IT- und OT-Sicherheit), Gartner, Inc., Mai 2018, www.gartner.com/doc/3873972/-strategic-roadmap-integrated-it

[2] „Analysis of 2018 Healthcare Data Breaches“ (Analyse von Datenkompromittierungen im Gesundheitswesen 2018), HIPAA Journal, Januar 2019, www.hipaajournal.com/analysis-of-healthcare-data-breaches/

[3] „2018 Cost of a Data Breach Study: Global Overview“, (Studie zu Kosten von Datenkompromittierungen: Weltweite Übersicht), Ponemon Institute, Juli 2018, https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf

hinzugerechnet werden müssen, die vor allem in den USA zu jahrelang verringerten Patientenzahlen führen können. Außerdem müssen diese Unternehmen in Zukunft mit häufigeren und dauerhaften Audits rechnen. Der Grundsatz, jetzt gleich oder später zahlen zu müssen, beweist sich wieder einmal als wahr.

Gesundheitswesen als Hauptziel für Cyberangriffe

Die Angriffsfläche im Gesundheitswesen wächst mit jedem Tag, da immer mehr medizinische Geräte mit den Netzwerken verbunden werden und Hacker sich auf die Jagd nach Patientendaten machen, die zu den sensibelsten Verbraucherinformationen zählen. Für Cyberkriminelle sind Patientendaten eine besonders willkommene Beute, da sie aufgrund der Vielzahl personenbezogener Informationen wie Geburtsdatum und -ort, Kreditkartendaten, Sozialversicherungsnummer (oder vergleichbaren Angaben), Postanschrift und E-Mail-Adresse satte Gewinne versprechen.

Häufige Cyberangriffe auf medizinische Einrichtungen

- **Ransomware wie die Trojaner WannaCry und NotPetya:** Diese Malware verschlüsselt Dateien und verhindert auf diese Weise, dass das Personal auf Systeme oder elektronische Patientenakten zugreifen kann, bis das Lösegeld bezahlt wurde und die Systeme wiederhergestellt sind. *Die WannaCry-Angriffe im Mai 2018 führten in Großbritannien zu Unterbrechungen bei der Patientenbetreuung durch den National Health Service und erzwangen die Stornierung von mehr als 19.000 Sprechstundenterminen. Laut dem britischen Gesundheitsministerium lagen die finanziellen Kosten durch die WannaCry-Attacken bei 92 Millionen GBP.*[4] *Ähnliche Angriffe im Jahr 2016 legten die Computer des Hollywood Presbyterian Medical Center eine ganze Woche lang lahm, sodass die medizinische Einrichtung erst nach Zahlung eines Lösegeldes von 17.000 US-Dollar wieder die Patientenversorgung aufnehmen konnte.*[5]

- **Denial-of-Access und Dedicated Denial-of-Service:** Ein Angreifer überflutet das Netzwerk sowie mit dem Internet verbundene Server mit Datenpaketen. Dadurch unterbricht er den normalen Datenverkehr und verlangsamt die System- und Anwendungsgeschwindigkeit bis zur völligen Unbenutzbarkeit. Manchmal wird mit diesen Angriffen die Aufmerksamkeit des Sicherheitsteams gebunden, um von einem Datendiebstahl abzulenken. *Im Jahr 2014 griff das Hacktivistenkollektiv Anonymous das Boston Children's Hospital mit einer DDoS-Attacke an. Laut dem Center for Internet Security musste das Krankenhaus Kosten von mehr als 300.000 USD tragen, um die Schäden durch diesen Angriff zu beheben und zu beseitigen.*[6]

- **Betrügerisches Imitieren von Geräten:** Ein nicht autorisiertes Gerät verbindet sich mit dem Netzwerk und gibt sich als legitimes Gerät aus, um auf Daten zuzugreifen. Angreifer nutzen diese Technik für den Diebstahl von Patientendaten oder das Eindringen in Backend-Systeme. *Das „MedJacking", eine häufige Form des Imitierens medizinischer Geräte, wurde erstmals einer breiten Öffentlichkeit bekannt, als der damalige US-Vizepräsident Dick Cheney Änderungen an seinem Herzschrittmacher veranlasste, um diesen besser vor Hackerangriffen zu schützen.* Laut dem US-Magazin Wired setzen MedJack-Angreifer mittlerweile bewusst auf alte Malware, um medizinische Geräte mit veralteten Betriebssystemen wie Windows XP und Windows Server 2003 anzugreifen.[7]

- **Man-in-the-Middle-Angriff:** Ein Angreifer klinkt sich in die Kommunikation zweier Parteien ein (meist per Phishing-Betrug), um Daten abzufangen oder eine fremde Identität vorzugaukeln. *Im April 2017 gab das Office for Civil Rights des US-Gesundheitsministeriums eine Empfehlung für die unterstellten Einrichtungen und ihre Geschäftspartner heraus, wonach diese das Secure Hypertext Transfer Protocol (HTTPS) verwenden sollten, damit Patientendaten nicht ungeschützt übertragen werden.*[8]

- **Dateilose Malware:** Angreifer können herkömmliche Malware-Schutztools heute mit einer neuen Malware-Art umgehen, die sich ausschließlich im dynamischen Speicher des Host-Computers befindet. Das Ponemon Institute sagt für 2019 voraus, dass dateilose Malware für 38 % aller Angriffe verantwortlich sein wird.[9] Diese speichergebundenen Attacken werden nicht nur durch veraltete oder ungepatchte Browser verbreitet, sondern sie nutzen auch Microsoft Windows-Schwachstellen wie PowerShell und das Remote Desktop Protocol (RDP) aus.

[4] „Securing cyber resilience in health and care" (Gewährleistung von Cyber-Resilienz in Gesundheits- und Pflegeeinrichtungen), Oktober 2018, www.gov.uk/government/publications/securing-cyber-resilience-in-health-and-care-october-2018-update

[5] Los Angeles Times-Artikel vom 18. Februar 2016, www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

[6] „DDOS Attacks: In the Healthcare Sector", (DDoS-Attacken im Gesundheitswesen), Center for Internet Security, www.cisecurity.org/blog/ddos-attacks-in-the-healthcare-sector/

[7] „Medical Devices are the next security nightmare" (Medizinische Geräte sind der nächste Sicherheitsalptraum), WIRED, März 2017, www.wired.com/2017/03/medical-devices-next-security-nightmare/

[8] „Healthcare Organizations Warned of Risk of Man-In-The-Middle Attacks" (Medizinische Einrichtungen vor Risiko von Man-in-the-Middle-Attacken gewarnt), HIPAA Journal, April 2017, www.hipaajournal.com/healthcare-organizations-warned-risk- man-middle-attacks-8757/

[9] „State of Endpoint Security Risk" (Bericht zu Sicherheitsrisiken für Endgeräte), Ponemon Institute, Oktober 2018, https://cdn2.hubspot.net/hubfs/468115/whitepapers/state-of-endpoint-security-2018.pdf

Vernetzte Geräte und damit verbundene Risiken

Methodik

Dieser Bericht ist eine bereichsübergreifende Analyse der Forescout Device Cloud, einem Repository für Host- und Netzwerkinformationen zu mehr als 8 Millionen individuellen Geräte-Fingerabdrücken und damit einem der größten Crowdsourcing-Repositorys für Geräteinformationen. Die Device Cloud-Daten umfassen tausende unterschiedliche Gerätetypen von mehr als 1.000 Forescout-Kunden, die anonymisierte Geräteinformationen teilen. Forescout analysiert die in Device Cloud gespeicherten Geräte-Fingerabdrücke, um Funktion, Anbieter und Modell sowie Betriebssystem und Version der Geräte zu identifizieren. Auf diese Weise lassen sich zahlreiche Geräte automatisch detailliert und umfangreich klassifizieren.

Für diese Untersuchung beschränkten die Forscher die Device Cloud-Analyse auf 75 Bereitstellungen in medizinischen Einrichtungen, die insgesamt mehr als 10.000 virtuelle LANs (VLANs) und 1,5 Millionen Geräte umfassen. Da der Fokus dieses Berichts auf dem aktuellen Stand bei medizinischen Geräten liegt, basieren die hier vorgestellten Ergebnisse zum größten Teil auf der Analyse von mehr als 1.500 medizinischen VLANs mit 430.000 Geräten.

Geräteklassen in medizinischen VLANs

Viele Netzwerke werden weiterhin voneinander isoliert betrieben, sodass keine lückenlose Sicherheit gewährleistet werden kann. Klinische Technikmitarbeiter konzentrieren sich häufig auf die Absicherung der vernetzten medizinischen Geräte, während sich die für Betriebsanlagen verantwortlichen Teams auf die Gebäudeautomatisierungssysteme beschränken. Wenn jedes Team eng eingegrenzte Prioritäten hat – wer ist für den ganzheitlichen Blick auf die Sicherheit verantwortlich?

Als absolute Grundlage müssen medizinische Einrichtungen alle IT-, IoT- und OT-Geräte kennen, die sich mit ihren Netzwerken verbinden. Mit diesem Wissen können sie die Isolierung der Sicherheitsmaßnahmen überwinden und somit die richtigen Gruppen zusammenbringen, die gemeinsam Sicherheitsstrategien besprechen und die Grundlage für einen ganzheitlichen Sicherheitsansatz schaffen.

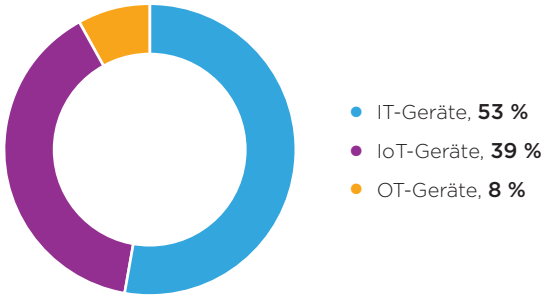
Die einzelnen Geräteklassen werden wahrscheinlich wachsen, da immer mehr medizinische Geräte mit den Netzwerken verbunden werden. Daher ist die regelmäßige Überprüfung und Anpassung der Sicherheitsstrategien von großer Bedeutung.

Abbildung 1. Geräteklassen in medizinischen VLANs

IT-Geräte: PCs, Laptops, Workstations mit fester Funktion, Server, Thick Clients und Thin Clients, Virtualisierungs-Hypervisoren und Netzwerkausrüstung für Unternehmen

OT-Geräte: Medizinische Geräte, Intensivpflegesysteme, Gebäudeautomatisierung/HLK-Anlagen, Notstromgeneratoren, Ausweisscanner und andere Zugangskontrollgeräte sowie IP-fähige Sicherheitskameras und Systeme für physische Sicherheitskontrollen

IoT-Geräte: VoIP-Telefone, Netzwerkdrucker, mobile Geräte, Tablets, Controller und Konverter, Videokonferenzgeräte, Präsentationssysteme, Smart TVs, Spielekonsolen und Zubehör

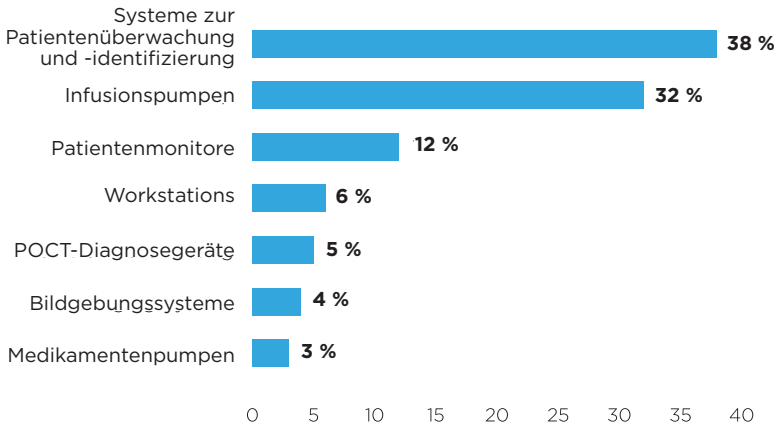


Gängige vernetzte medizinische Geräte

In stationären Einrichtungen ist der Anteil mit Patienten verbundener Geräte meist höher. Patientenbezogene Geräte wie Systeme zur Patientenüberwachung und -identifizierung, Infusionspumpen und Patientenmonitore bilden den größten Teil der medizinischen Geräte in Kliniknetzwerken. Das ist auch nachvollziehbar, da jedes dieser Geräte jeweils einen Patienten überwacht.

Labordiagnostik-Geräte oder medizinische Bildgebungssysteme machen hingegen einen geringeren Anteil aus, da sie gemeinsam verwendet werden können. Diese teureren Systeme werden meist über einen langen Zeitraum genutzt, sodass Aktualisierungen und Patch-Installationen eine Herausforderung darstellen.

Abbildung 2. Gängige vernetzte medizinische Geräte



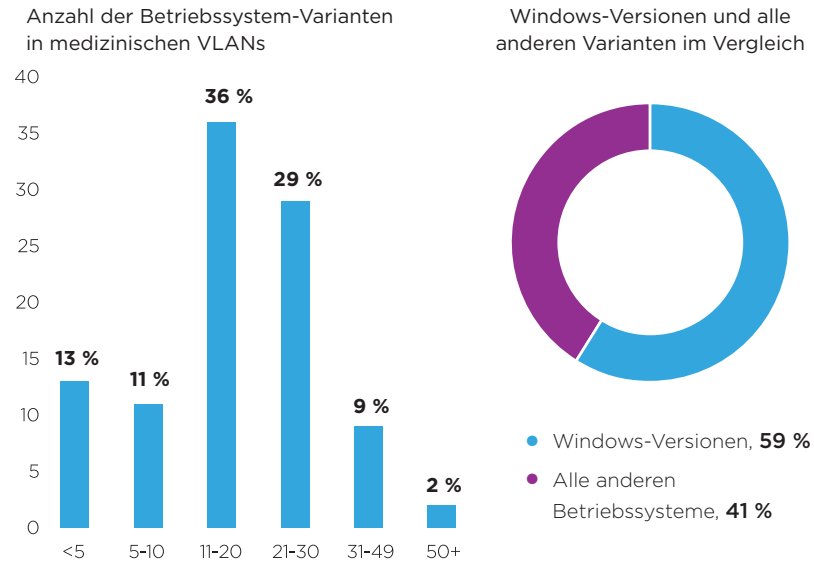
Vielfalt der Geräte-Betriebssysteme

Die Vielfalt der Geräte-Betriebssysteme kann die Sicherheitsverwaltung deutlich erschweren. Die Untersuchung zeigte, dass 40 % der Bereitstellungen mit medizinischen VLANs mehr als 20 verschiedene Betriebssysteme umfassten.

Ein genauerer Blick auf diese Betriebssysteme ergab, dass es sich bei mehr als der Hälfte (59 %) um Windows-Betriebssysteme und bei 41 % um andere Betriebssysteme handelt, d. h. eine Mischung aus Betriebssystemen für Mobilgeräte, eingebettete Firmware und Netzwerkinfrastrukturen. Das Patchen und Aktualisieren von Betriebssystemen in medizinischen Umgebungen (insbesondere in Einrichtungen zur Akutversorgung) kann eine Herausforderung bedeuten und voraussetzen, dass diese Geräte ununterbrochen online und verfügbar bleiben. Einige medizinische Geräte können nicht gepatcht werden, benötigen möglicherweise die Zustimmung des Anbieters oder erfordern manuelle Schritte zur Patch-Implementierung.

> In 40 % der Bereitstellungen mit medizinischen VLANs waren mehr als 20 verschiedene Betriebssysteme vertreten.

Abbildung 3. Vielfalt der Betriebssysteme in medizinischen VLANs



Probleme durch veraltete Windows-Versionen

Die Microsoft-Unterstützung für mehr als 70 % der in unseren Stichprobendaten enthaltenen Geräte, die Windows (z. B. Windows 7, Windows 2008 und Windows Mobile) ausführen, läuft planmäßig am 14. Januar 2020 aus. Die Verwendung nicht mehr unterstützter Betriebssysteme stellt ein Risiko dar, das die Compliance mit zahlreichen Vorschriften beeinträchtigen kann.

In den Netzwerken werden höchstwahrscheinlich auch weiterhin medizinische Geräte mit veralteten Betriebssystemen verwendet, da Aktualisierungen mit hohen Kosten verbunden sind. Für Intensivpflegesysteme kommen Ausfallzeiten aufgrund von Betriebssystem-Aktualisierungen möglicherweise nicht in Frage. Zudem können ältere Anwendungen aufgrund fehlender Unterstützung, Inkompatibilität oder Lizenzproblemen häufig nicht unter aktuelleren Windows-Versionen ausgeführt werden. Es wird also auch weiterhin zwingende geschäftliche Gründe dafür geben, veraltete Betriebssysteme auf medizinischen Geräten auszuführen, sodass diese Geräte angemessen segmentiert werden müssen, um den Zugriff auf kritische Informationen und Services zuverlässig zu schützen.

71 % aller Geräte werden ab dem 14. Januar 2020 nicht mehr unterstützte Windows-Versionen ausführen.

Abbildung 4. Gute, schlechte und problematische Windows-Versionen

Gut	Schlecht	Problematisch
29 %	0,4 %	71 %
Geräte mit Windows-Versionen, die noch mindestens ein weiteres Jahr unterstützt werden	Geräte mit nicht unterstützten/veralteten Windows-Versionen	Geräte mit Windows-Versionen, die ab dem 14. Januar 2020 nicht mehr unterstützt werden

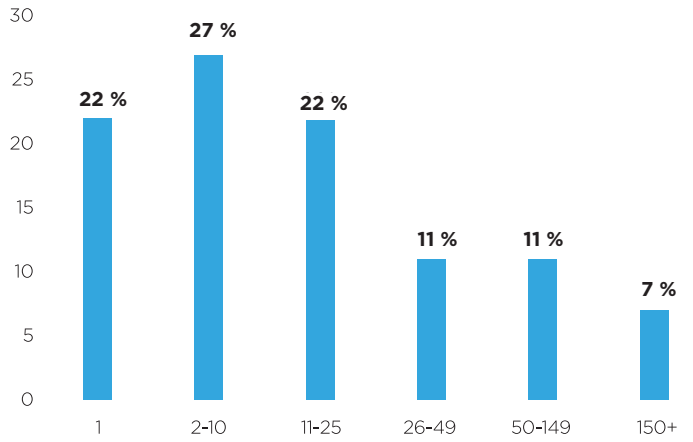
Verwendung von VLANs mit Segmentierungsunterstützung

Durch Segmentierung wird die Angriffsfläche für Systeme deutlich verkleinert. Benutzer „sehen“ nur die Server und weitere zur Erledigung ihrer täglichen Aufgaben notwendigen Geräte. Die Segmente werden durch die Gruppierung allgemeiner Benutzertypen und Begrenzung des Netzwerkzugriffs auf die für die täglichen Aufgaben dieser Benutzer erforderlichen Ressourcen erstellt.

Segmentierung kann mit verschiedenen Methoden umgesetzt werden. In der einfachsten Form können VLANs das Netzwerk basierend auf den organisatorischen Anforderungen und Prioritäten segmentieren. Auf diese Weise werden die kritischen Daten effektiv isoliert, ähnliche Geräte nach Funktion zusammengefasst oder der Zugriff auf Daten, Systeme und andere Assets mithilfe von Benutzer-Anmeldedaten beschränkt. Die Daten dieser Untersuchung zeigen, dass die Zahl der VLANs mit medizinischen Geräten gering ist. Das weist darauf hin, dass einige medizinische Einrichtungen noch in ausreichende Segmentierung investieren müssen.

Bei 49 % der Bereitstellungen sind die medizinischen Geräte über zehn oder weniger VLANs verteilt, was auf eine wenig ausgereifte Segmentierung der Implementierung hinweist.

Abbildung 5. Anzahl von VLANs mit medizinischen Geräten



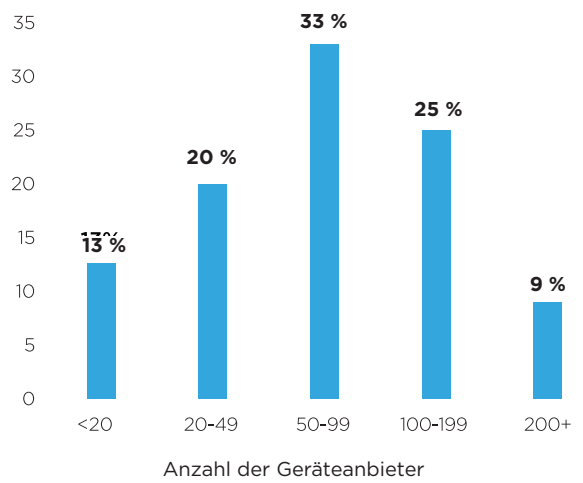
Vielfalt der Geräteanbieter nimmt zu

Die Umgebungen in medizinischen Einrichtungen sind heute vollständig durchtechnisiert. In der Vergangenheit stand die Sicherheit medizinischer Geräte bei der Entwicklung nicht an erster Stelle, was die Verwaltung und Absicherung erschwert. Zudem wenden sich die Anbieter direkt an die Mediziner, sodass die Geräte letztendlich mit dem Netzwerk verbunden werden, ohne dass die Sicherheits- und Risikoprotokolle vorher geprüft wurden. IT- und Sicherheitsteams erkennen diese nicht autorisierten verbundenen Geräte dann zwar vielleicht in ihrer Umgebung, können sie jedoch meist nicht klassifizieren oder problemlos orten.

Medizinische Einrichtungen mit mehreren Standorten sind in technischer Hinsicht extrem heterogen: Mehr als 30 % der medizinischen VLANs in den untersuchten Unternehmen unterstützen über 100 verschiedene Geräteanbieter. Die Anbieter für andere funktionale Netzwerke wie Backoffice und Frontoffice und andere Bereiche sind dabei noch nicht einmal berücksichtigt. In vielen Fällen sind die Anbieter selbst für die Patch-Installationen und die Wartung spezialisierter klinischer Systeme verantwortlich.

34 % der VLANs in den untersuchten Unternehmen unterstützen mehr als 100 verschiedene Geräteanbieter.

Abbildung 6. Anzahl der Geräteanbieter in medizinischen VLANs



Aktivierte gängige Services führen zu anfälligen Netzwerken

Eine überraschend hohe Zahl der Geräte in medizinischen VLANs wird mit aktivierten hochriskanten Services ausgeführt, sodass Angreifer unkontrolliert darauf zugreifen und sich hinter der Peripherie sowie lateral bewegen können. Damit die Anbieter medizinischer Geräte und externe Lieferanten auf die Geräte zugreifen können, müssen Services wie Microsoft Remote Desktop Protocol (RDP) aktiviert bleiben. In anderen Fällen werden Netzwerk-Ports standardmäßig offen gelassen, ohne dass das IT- und Sicherheitsteam davon Kenntnis hat.

- **Server Message Block (SMB):** SMB ist das Transportprotokoll, das von Windows-Systemen für zahlreiche Zwecke verwendet wird, z. B. für Dateifreigabe, Druckerfreigabe und Zugriff auf Remote-Windows-Dienste. WannaCry und NotPetya sind zwei Beispiele für Ransomware-Exemplare, die SMB-Schwachstellen erfolgreich ausnutzten.
- **Remote Desktop Protocol (RDP):** RDP ist ein weiteres typisches Protokoll, das von modernen automatisierten Bedrohungen wie dateiloser Malware ausgenutzt wird.
- **File Transfer Protocol (FTP), Secure Shell (SSH), Telnet und Digital Imaging and Communications in Medicine (DICOM):** Diese Protokolle sind weniger verbreitet, werden allerdings häufig ausgenutzt und bieten keine Absicherung oder Verschlüsselung für die Netzwerksitzungen. Sicherheitsmodelle vertragen sich schlecht mit veralteten Geräten, die sehr häufig nicht verschlüsselte grundlegende Dienste verwenden.

85 % der Geräte mit Windows-Betriebssystemen werden mit aktiviertem Server Message Block-Protokoll (SMB) ausgeführt.

Windows-Dienst	Anteil
SMB	85 %
RDP	32 %
FTP*	1 %
SSH	<1 %
Telnet-Protokoll*	<1 %
DICOM	<1 %

* Ohne Verschlüsselung

Empfehlungen

Es führt kein Weg daran vorbei: Die Zahl der Geräte, die mit den Netzwerken von Gesundheitsdienstleistern verbunden sind, wird ebenso wie die Komplexität der Umgebung weiter zunehmen. Es ist daher an der Zeit, eine proaktive und unternehmensweite Strategie zur Sicherheits- und Risikoverwaltung zu entwickeln und zu implementieren.

Implementierung agentenloser Erkennung auf allen Geräten

Obwohl die Sicherheits- und IT-Abteilung mithilfe von Software-Agenten die Kommunikation mit den Geräten und die Überwachung ihrer Aktivitäten vereinfachen kann, unterstützen die meisten medizinischen Geräte keine Agenten. Daher ist die agentenlose Erkennung aller per IP-Adresse mit dem erweiterten Netzwerk verbundenen Geräte unverzichtbar.

Erkennung und automatische Klassifizierung von Geräten

Es genügt nicht, lediglich die IP-Adresse eines Geräts zu erkennen. Zur Erfassung von Kontextinformationen zu jedem Gerät im Netzwerk sowie zur Erkennung seines Zwecks, Eigentümers und Sicherheitsstatus ist vielmehr eine schnelle und detaillierte automatische Klassifizierung unverzichtbar. Diese Informationen müssen in einem Echtzeit-Ressourceninventar zusammengeführt werden, damit sie sich für Zugriffssteuerungsrichtlinien verwenden lassen und Sicherheitsteams die Möglichkeit geben, schnell auf gezielte Attacken gegen bestimmte Betriebssysteme oder Geräte zu reagieren.

Kontinuierliche Überwachung von Geräten

Medizinische Geräte müssen kontinuierlich überwacht werden, um sämtliche Veränderungen des Sicherheitsstatus zu erkennen. Eine punktuelle Analyse kann dazu führen, dass sich eine Einstellen-und-Vergessen-Mentalität ausbreitet, die zu Compliance-Müdigkeit und wachsenden Risiken führt. Durch die ununterbrochene Netzwerküberwachung mithilfe passiver bzw. aktiver Techniken in klinischen und OT-Umgebungen erhalten Sicherheitsteams einen Echtzeitüberblick. Damit können sie kontinuierlich Ressourcen-informationen und Verhaltensdaten erfassen, ihre Effizienz verbessern und wertvolle Zeit sparen.

Durchsetzung von Segmentierung

Netzwerksegmentierung ist eine bekannte Best Practice. Die Umsetzung für das gesamte Netzwerk lässt sich jedoch nicht leicht verwalten oder durchsetzen. Besonders gefährdete Geräte wie bekannt anfällige veraltete Systeme sollten segmentiert werden, um potenzielle Kompromittierungen und Risiken einzudämmen.

Fazit

Führungskräfte in medizinischen Einrichtungen mit Verantwortung für Sicherheits- und Risiko-Management müssen die Absicherung aller Geräte im erweiterten Unternehmen angehen. Die alleinige Konzentration auf die Sicherheit medizinischer Geräte statt sämtlicher Geräte in der Umgebung kann zu schwerwiegenden Sicherheitslücken führen. Ein ganzheitlicher Sicherheitsansatz erfordert kontinuierliche Transparenz und Kontrolle über das gesamte vernetzte Ökosystem. Ebenso wichtig ist das Wissen, welche Bedeutung eine Plattform für Gerätetransparenz und -kontrolle für die Koordinierung von Aktionen heterogener Sicherheits- und IT-Verwaltungstools hat.

Wie bereits erwähnt kann Inaktivität enorme Kosten nach sich ziehen. Jede Sekunde, in der ein Gerät die Compliance-Vorgaben nicht erfüllt, vergrößert Ihr Anfälligkeitsfenster sowie Ihre Risiken, sodass Ihre medizinische Einrichtung mit schwerwiegenden Konsequenzen für die Patientensicherheit, die Finanzen und die Geschäftsabläufe rechnen muss. Medizinische Einrichtungen stehen vor der Wahl, entweder jetzt in proaktive Maßnahmen zur Risikominimierung zu investieren oder später zu zahlen und sich dem Zorn von Behörden, Patienten und Gerichten zu stellen.

Über Forescout Technologies

Forescout Technologies ist ein führender Anbieter für Gerätetransparenz und -kontrolle. Mit unserer einheitlichen Sicherheitsplattform können sich Unternehmen und Regierungsbehörden nicht nur einen vollständigen Überblick über ihre erweiterten Unternehmensumgebungen verschaffen, sondern auch ihre Maßnahmen koordinieren, um operative sowie Cyberrisiken zu reduzieren. Forescout-Produkte lassen sich schnell implementieren und bieten agentenlose Echtzeiterkennung und Klassifizierung aller per IP-Adresse verbundenen Geräte sowie die ununterbrochene Analyse der Sicherheitslage. Mit Stand 31. Dezember 2018 setzten 3.300 Kunden in mehr als 80 Ländern auf die Infrastruktur-neutrale Lösung zur Reduzierung des Risikos von Geschäftsunterbrechungen durch Sicherheitsvorfälle und -verstöße, Gewährleistung und Nachweis von Sicherheits-Compliance und Steigerung der Produktivität von Sicherheitsteams. Weitere Informationen erhalten Sie unter www.forescout.com.

Forescout-Forscher haben den Umfang und die Stichprobe eingegrenzt, um einen konsistenten und einfacheren Überblick zu ermöglichen. Dazu wurden Typ, Zeitraum und Umfang der Untersuchung beschränkt. Zudem unterliegt die Untersuchung Beschränkungen aufgrund der Daten-Anonymisierung, passiver Erfassungsmethoden sowie Fehlern bei der KI-basierten Klassifizierung der Gerätefunktionen, Betriebssysteme und Anbieter. Da Live-Daten aus Cloud-basierten Produktionsumgebungen verwendet werden, sind die Ausgangsdaten nicht immer absolut präzise. Die Forescout-Forscher haben in Anbetracht dieser Einschränkungen ihr Möglichstes getan, um Konsistenz, Zuverlässigkeit und hohe Integrität zu gewährleisten.

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Gebührenfreie Rufnummer (USA): +1-866-377-8771

Telefon (International): +1-408-213-3191
Support +1-708-237-6591