La seguridad en el sector de la asistencia sanitaria

Forescout analiza los datos de despliegue para conocer mejor los riesgos de ciberseguridad a los que se enfrentan las organizaciones sanitarias actuales.

FORESCOUT®

Resumen ejecutivo

El Internet de las cosas médicas (IoMT) sigue ofreciendo interesantes posibilidades a las organizaciones sanitarias para mejorar la atención a los pacientes. Sin embargo, esta transformación digital y el aumento de la conectividad también introducen nuevos riesgos para la privacidad y la seguridad. El panorama de dispositivos crece exponencialmente, lo que viene a sumarse a la complejidad de las redes y complica la gestión y mejora de su nivel de seguridad.

El objetivo de este informe es ofrecer a los líderes de la gestión de riesgos y de seguridad de las organizaciones sanitarias información de los distintos tipos de dispositivos que se conectan a sus redes y sus riesgos asociados. Además, en él se recomienda un enfoque holístico de la seguridad, que no solo se circunscriba a la protección de los dispositivos médicos.

Los datos de los que se nutre este informe provienen de Forescout Device Cloud, un repositorio de información de host y redes para más de 8 millones de dispositivos únicos, lo que lo convierte en uno de los repositorios de dispositivos más grandes obtenidos gracias a la colaboración. Para este estudio, los investigadores limitaron el análisis de Forescout Device Cloud a 75 despliegues de servicios sanitarios con más de 10 000 redes de área local virtual (VLAN) y 1,5 millones de dispositivos. Puesto que el objetivo principal del informe es el estado de los dispositivos médicos, muchos de los resultados se basan en el análisis de más de 1500 VLAN médicas con 430 000 dispositivos.

Conclusiones principales

- **Los entornos sanitarios actuales son cada vez más diversos:** el rápido crecimiento y la diversidad de los dispositivos médicos y los sistemas operativos conectados complican mucho la protección de las redes.

- **Los sistemas operativos Windows heredados representan una de las principales vulnerabilidades:** muchas redes utilizan sistema operativos Microsoft Windows para los que ya no se ofrecen soporte técnico. Además, se acerca un importante hito de Windows que dejará sin soporte técnico a muchos dispositivos.

- **Escasez de estrategias de segmentación:** la segmentación de la red, una mejor práctica para limitar el desplazamiento lateral malicioso al centrarse en la confidencialidad, ubicación e importancia de los datos, se aplica de manera irregular en las diversas redes actuales.

- **Es necesario controlar la expansión de proveedores de dispositivos:** la proliferación de proveedores de dispositivos genera importantes problemas de interoperabilidad y de gestión de la seguridad y de los activos.

- **Los servicios comunes descuidados convierten las redes en vulnerables:** dejar abiertos los protocoles comunes proporciona acceso sin control a los agresores.

El estado de ciberseguridad de las organizaciones sanitarias

El IoMT sigue convirtiéndose en una prioridad estratégica debido a su capacidad de mejorar la atención de los pacientes, proporcionar mejores datos clínicos, aumentar la eficacia y reducir los costes de la atención sanitaria. No resulta difícil comprender por qué las organizaciones sanitarias están adoptando rápidamente el IoMT, una infraestructura conectada de dispositivos médicos, aplicaciones de software, sistemas y servicios de atención sanitaria. Sin embargo, esta rápida adopción de dispositivos conectados está provocando un efecto secundario grave: desvía la mirada de la necesidad más amplía de abordar la seguridad general de los entornos convergentes actuales, más allá de los dispositivos médicos conectados, lo que genera importantes brechas de ciberseguridad.

El Internet de las cosas médicas es una infraestructura conectada de dispositivos médicos, aplicaciones de software, sistemas y servicios de atención sanitaria. A efectos del presente estudio, el IoMT pertenece a la categoría del Internet de las cosas (IoT) y la tecnología operativa (OT, Operational Tecnology).

La proliferación de dispositivos de IT y OT conectados en la atención sanitaria

El número de dispositivos conectados crece a una velocidad imparable, lo que amplía la superficie de ataque y complica la adaptación de la seguridad. Estos incluyen dispositivos de atención sanitaria como sistemas de identificación y seguimiento de pacientes, bombas de perfusión y sistemas de creación de imágenes médicas. También incluyen dispositivos de infraestructura, como sistemas de automatización de edificios, sistemas de seguridad física, fuentes de alimentación ininterrumpida, grupos electrógenos y otros sistemas de OT, así como otros dispositivos que se conectan cada vez con más frecuencia a redes de IT. Por consiguiente, la responsabilidad de la tecnología operativa (OT) es desplazarse al ámbito de competencia de IT. Según Gartner, "Para 2021, los departamentos del CIO, CISO o CSO se encargarán del 70 % de la seguridad de OT, en comparación con el 35 % que lo hacen en la actualidad[1]".

Comprensión y priorización del riesgo

La convergencia de estas dos redes anteriormente dispares puede crear una nueva clase de riesgos para la seguridad. Los ciberdelincuentes pueden ahora desplazarse lateralmente por las redes de IT y OT interconectadas. El aumento de las fusiones y las adquisiciones, que predominan en el sector de la atención sanitaria, amplifica todavía más estos retos de seguridad.

Al igual que el diagnóstico y tratamiento clínicos, los CISO deben detectar los riesgos pronto y dar prioridad a la mejor forma de proceder. Los equipos de gestión de riesgos y de seguridad que intentan mitigar cada riesgo conseguirán resultados insignificantes. A través del conocimiento detallado de las amenazas de la red y de la identificación de los dispositivos que esconden el mayor riesgo, es posible maximizar la productividad, aumentar la rentabilidad y reducir el riesgo en toda la red.

Los costes reales de aplazar la contención de riesgos

Una vez más, los sectores de la ciberseguridad y de la atención sanitaria tienen un rasgo común: la detección y el tratamiento tempranos consiguen extraordinarios resultados y reducen drásticamente los costes totales. Considere las siguientes estadísticas: según el *HIPAA (Health Insurance Portability and Accountability Act, Ley de transferibilidad y responsabilidad del seguro sanitario)* Journal, en 2018, las violaciones de la seguridad en el sector de la asistencia sanitaria involucraron de media 17

[1] "Strategic Roadmap for Integrated IT and OT Security," Gartner, Inc., May 2018, www.gartner.com/doc/3873972/-strategic-roadmap-integrated-it

[2] "Analysis of 2018 Healthcare Data Breaches," HIPAA Journal, January 2019, www.hipaajournal.com/analysis-of-healthcare-data-breaches/

974 registros[2]. Ponemon calculó el coste de resolución medio per cápita/por registro de información médica protegida (PHI) en el sector de la asistencia sanitaria durante 2018 en 408 dólares[3]. Esto sitúa el coste medio de la *contención, investigación y notificación* en 7,3 millones de dólares por incidente. Por supuesto, el destrozo financiero no termina ahí, ya que las organizaciones sanitarias también deben hacer frente al importante daño reputacional y a la marca que afecta negativamente a la lealtad de los pacientes durante años, sobre todo en EE. UU. Además, deben programar un ciclo de auditorías continuas y permanentes de cara al futuro. El axioma de paga ahora o paga después no ha sido nunca más adecuado.

El sector de la asistencia sanitaria es objetivo prioritario de los ciberataques

La superficie de ataque en el sector de la asistencia sanitaria se amplía a diario a medida que crece el número de dispositivos médicos que se conectan a las redes y el interés de los hackers por la información médica protegida, que se encuentra entre el tipo de información de consumidor más sensible. Los ciberdelincuentes codician esta información ya que trae una bonita recompensa por la abundancia de datos personales de valor, que puede incluir la fecha y lugar de nacimiento, detalles de tarjetas de crédito, número de identificación personal y de la Seguridad Social, dirección física y dirección de correo electrónico.

Ciberataques comunes que afectan a las organizaciones sanitarias

- Ransomware como WannaCry y los troyanos de NotPetya: este malware cifra los archivos, lo que impide al personal de asistencia sanitaria utilizar los sistemas o acceder a la historia clínica electrónica para ofrecer atención hasta que no se paga un rescate y se restauran los sistemas. *Los ataques de WannaCry de mayo de 2018 perturbaron la atención a los pacientes en todo el Servicio Nacional de Salud británico (NHS, National Health Service) y obligaron a cancelar más de 19 000 citas médicas.* El departamento de salud calculó en 92 millones de libras esterlinas el coste financiero de los ataques de WannaCry[4]. En 2016, un ataque similar inutilizó los ordenadores del Hollywood Presbyterian Medical Center durante una semana, inutilizando su capacidad de ofrecer servicios médicos hasta que el centro pagó un rescate de 17.000 dólares[5].

- Denegación de acceso y denegación de servicio dedicado: un agresor inunda la red y los servidores conectados a Internet con paquetes, impidiendo el flujo de tráfico normal y ralentizando el rendimiento de sistemas y aplicaciones hasta provocar una paralización casi total. Estos ataques también se utilizan en ocasiones para desviar la atención de los equipos de seguridad mientras se lleva a cabo un ataque de robo de datos. *En 2014, el grupo de hacktivistas Anonymous lanzó un ataque DDoS contra el Children's Hospital de Boston.* Según el Center for Internet Security, el hospital gastó más de 300 000 dólares en responder y mitigar el daño causado por el ataque[6].

- Suplantación de dispositivos: un dispositivo se conecta a la red y se comporta como un dispositivo autorizado, pero en realidad no lo es y aprovecha para recopilar datos. Los agresores utilizan esta técnica para robar información sanitaria personal o para infiltrarse en sistemas backend. *Las preocupaciones sobre el MedJacking, una forma común de suplantación de dispositivos médicos, surgieron por primera vez cuando el vicepresidente de Estados Unidos, Dick Cheney, solicitó cambios en su marcapasos para protegerse mejor contra los hackers. Según Wired, en la actualidad hay agresores de MedJack (o pirateo de dispositivos médicos) que utilizan de forma intencionada malware antiguo para dirigir sus ataques contra dispositivos médicos que ejecutan sistemas operativos obsoletos, como Windows XP y Windows Server 2003* [7].

[3] "2018 Cost of a Data Breach Study: Global Overview," Ponemon Institute, July 2018, https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf

[4] "Securing Cyber Resilience in Health and Care," October, 2018, www.gov.uk/government/publications/securing-cyber-resilience-in-health-and-care-october-2018-update

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

[6] "DDOS Attacks: In the Healthcare Sector," Center for Intenet Security, www.cisecurity.org/blog/ddos-attacks-in-the-healthcare-sector/

[7] "Medical Devices are the Next Security Nightmare," WIRED, March 2017, www.wired.com/2017/03/medical-devices-next-security-nightmare/

- Ataque de intermediario: un agresor se infiltra en mitad de las comunicaciones de dos partes (normalmente mediante un timo de phishing) con la intención de espiar o de suplantar. *En abril de 2017, la oficina del Departamento de Salud y Servicios Sociales de EE. UU. aconsejó a las entidades afectadas y a sus empresas asociadas utilizar el protocolo Secure Hypertext Transport Protocol (HTTPS) para garantizar la total seguridad de la información médica protegida*[8].

- Malware sin archivos: los agresores han aprendido a eludir las herramientas antimalware tradicionales con un nuevo tipo de malware que reside solo en la memoria dinámica del ordenador del host. El Ponemon Institute prevé que en 2019, el malware sin archivos representará el 38 % de los ataques9. Además de llevarse a cabo a través de navegadores obsoletos o sin parches, estos ataques en memoria a menudo aprovechan puntos débiles de Microsoft Windows, como PowerShell y Protocolo de escritorio remoto (RDP).

[8] "Healthcare Organizations Warned of Risk of Man-In-The-Middle Attacks," HIPPA Journal, April 2017, www.hipaajournal.com/healthcare-organizations-warned-risk-man-middle-attacks-8757/

[9] "State of Endpoint Security Risk," Ponemon Institute, October 2018, https://cdn2.hubspot.net/hubfs/468115/whitepapers/state-of-endpoint-security-2018.pdf

Conocimiento de los dispositivos conectados y de los riesgos asociados

Metodología

Este informe es un análisis transversal de Forescout Device Cloud, un repositorio de información de host y redes para más de 8 millones de huellas digitales de dispositivos únicos, lo que lo convierte en uno de los repositorios de dispositivos más grandes obtenidos gracias a la colaboración. Los datos de Device Cloud contienen miles de tipos de dispositivos distintos procedentes de más de 1000 clientes de Forescout que comparten información anónima sobre dispositivos. Forescout analiza las huellas digitales de los dispositivos desde su Device Cloud para identificar la función, proveedor y modelo, además del sistema operativo y la versión de los dispositivos, para proporcionar una clasificación automática de una amplia gama de dispositivos.

Para este estudio, los investigadores limitaron el análisis de Forescout Device Cloud a 75 despliegues de servicios sanitarios con más de 10 000 redes de área local virtual (VLAN) y 1,5 millones de dispositivos. Puesto que el objetivo principal del informe es el estado de los dispositivos médicos, muchos de los resultados se basan en el análisis de más de 1500 VLAN médicas con 430 000 dispositivos.

Clases de dispositivos en VLAN médicas

Muchas redes siguen operando en silos organizativos, y esto genera brechas de seguridad. Los ingenieros clínicos a menudo dan prioridad a la protección de los dispositivos médicos conectados, mientras que los equipos de instalaciones y operaciones se centran en proteger los sistemas de automatización de edificios. Habida cuenta de estas prioridades aisladas, ¿quién es responsable de considerar la seguridad de forma global?

En el nivel más básico, las organizaciones sanitarias necesitan conocer los dispositivos de IT, IoT y OT que se conectan a sus redes. Este conocimiento ayuda a derribar los silos de seguridad, reunir a los grupos adecuados para tratar las estrategias de seguridad, y sentar las bases de un enfoque holístico de la seguridad.

Las clases de dispositivos probablemente cambiarán de tamaño a medida que crezca el número de dispositivos médicos que se conectan a las redes, lo que hará que sea fundamental revisar y adaptar las estrategias de seguridad.

Dispositivos de IT: ordenadores personales, portátiles, estaciones de trabajo especialmente diseñadas, servidores, clientes pesados y ligeros, hipervisores de virtualización y equipos de redes empresariales.

Dispositivos de OT: dispositivos médicos, sistemas de cuidados intensivos, sistemas de automatización de edificios/HVAC, generadores de energía, dispositivos de credencialización y otros relacionados con edificios, así como cámaras de seguridad y sistemas de seguridad física con IP.

Dispositivos IoT: teléfonos VoIP, impresoras de red, dispositivos móviles, tabletas, controladoras y conversores, dispositivos de videoconferencia, sistemas de presentación, smart TV, consolas de entretenimiento, distintos accesorios.

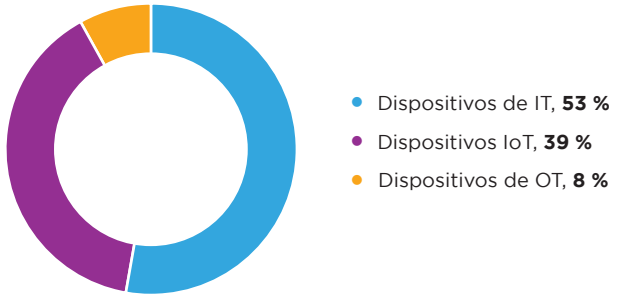

Figura 1: Clases de dispositivos en VLAN médicas

Los dispositivos médicos conectados más comunes

Las instalaciones médicas hospitalarias suelen tener un porcentaje mayor de dispositivos “conectados” a un paciente Los dispositivos por paciente, como sistemas de identificación y seguimiento de pacientes, bombas de perfusión y monitores de pacientes representan la mayoría de los dispositivos de atención sanitaria de las redes clínicas. Esto tiene sentido ya que son dispositivos que realizan un seguimiento y una supervisión de los pacientes en una proporción de 1:1.

Dispositivos como los que se utilizan en diagnósticos de laboratorio o de obtención de imágenes médicas representan un número menor ya que son dispositivos compartidos. Estos sistemas más caros suelen convertirse en dispositivos muy duraderos a los que resulta complicado aplicar parches y actualizaciones

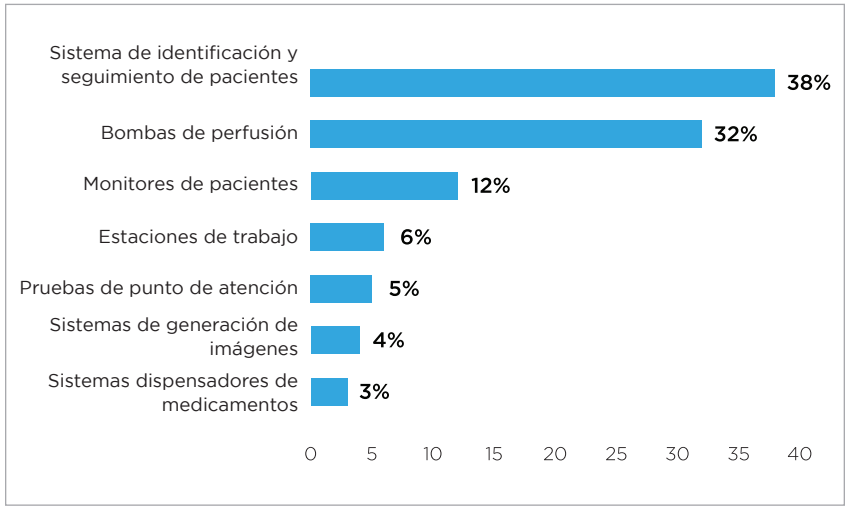

Figura 2: Dispositivos médicos conectados más comunes

Diversidad de sistemas operativos de dispositivos

La diversidad de sistemas operativos de dispositivos puede complicar cada vez más la administración de la seguridad. El estudio revela que el 40 % de los despliegues tenían más de 20 sistemas operativos distintos en sus VLAN médicas.

Si examinamos los distintos tipos de sistemas operativos encontrados en las VLAN médicas, más de la mitad (59 %) eran sistemas operativos Windows y el 41 % una mezcla de otras variantes, incluidos móviles, firmware incrustado e infraestructura de red. La aplicación de parches y la actualización de sistemas operativos en los entornos de asistencia sanitaria —en particular las instalaciones de cuidados intensivos— puede ser complicada y requerir que los dispositivos permanezcan online y disponibles. Puede no ser posible aplicar parches a algunos dispositivos médicos, hacer falta la aprobación del proveedor o bien que sea necesaria la aplicación manual de los mismos.

El 40 % de los despliegues tenían más de 20 sistemas operativos distintos en sus VLAN médicas.

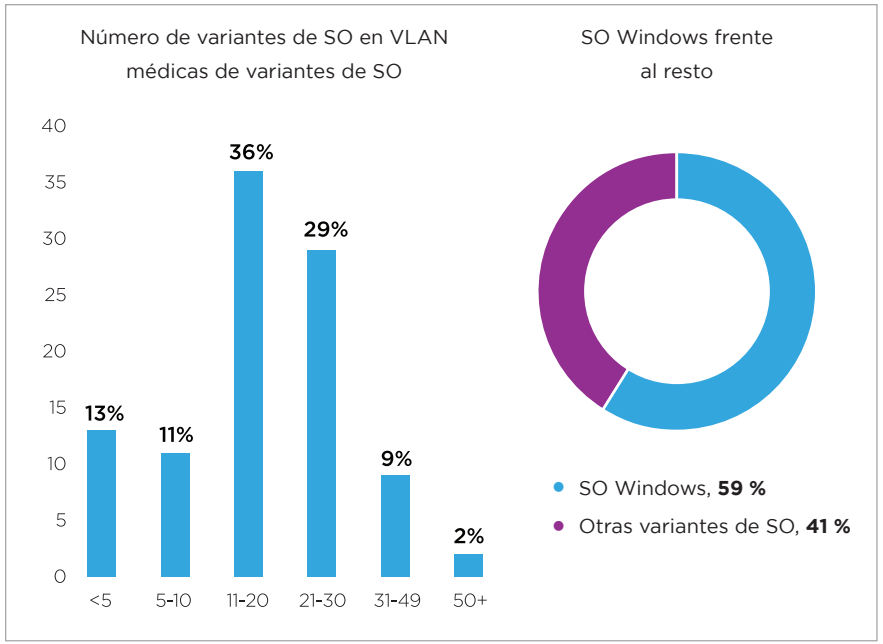

Figura 3: Diversidad de sistemas operativos en VLAN médicas

El problema de las versiones heredadas de Windows

En nuestra muestra datos, el soporte técnico de Microsoft para más del 70 % de dispositivos que ejecutan Windows (lo que incluye Windows 7, Windows 2008 y Windows Mobile) está previsto que caduque el 14 de enero de 2020. El uso de sistemas operativos sin soporte técnico representa un riesgo que afecta negativamente al cumplimiento de muchas normativas.

Es muy probable que las redes sigan teniendo dispositivos médicos con sistemas operativos heredados ya que las actualizaciones son costosas. El tiempo de inactividad asociado a la actualización de un sistema operativo podría no ser aceptable para los sistemas de cuidados críticos. Además, algunas aplicaciones antiguas simplemente no funcionarán en versiones más recientes de Windows debido a la falta de soporte técnico, compatibilidad o problemas de modalidades de licencias. La necesidad empresarial de ejecutar sistemas operativos antiguos en dispositivos médicos no va a desaparecer en el corto plazo, por lo que es necesario segmentar adecuadamente estos dispositivos para proteger el acceso a información y servicios críticos.

El 71 % de los dispositivos ejecutarán sistemas operativos Windows sin soporte técnico para el 14 de enero de 2020.

Lo Bueno

El **29%**

de los dispositivos con versiones de SO Windows que recibirán soporte técnico durante más de un año.

Lo Malo

El **4%**

de los dispositivos ejecutan versiones de SO Windows sin soporte técnico/heredadas.

Lo Feo

El **71%**

de los dispositivos ejecutarán SO Windows sin soporte técnico para el 14 de enero de 2020.

Figura 4: Sistemas operativos Windows - Lo Bueno, lo Malo y lo Feo

Uso de VLAN para apoyar la segmentación

La segmentación reduce considerablemente la superficie de ataque de un sistema. Los usuarios solo “ven” los servidores y los demás dispositivos que necesitan para desempeñar su trabajo diario. Los segmentos se crean agrupando tipos de usuarios similares y limitando su acceso a los recursos de la red que necesitan para realizar sus tareas.

La segmentación puede llevarse a cabo de varias maneras. En el nivel más básico, las VLAN pueden emplearse para segmentar la red en función de las necesidades y prioridades de la empresa, aislando de forma eficaz los datos críticos, segregando dispositivos similares por función o limitando el acceso a los datos, sistemas y otros activos en función de las credenciales de usuario. Los datos de este estudio reflejan un número inferior de VLAN con dispositivos médicos, lo que sugiere que algunas organizaciones sanitarias tienen todavía que invertir adecuadamente en segmentación.

El 49 % de los despliegues tienen dispositivos médicos en 10 VLAN o menos, lo que sugiere una implementación de la segmentación inmadura.

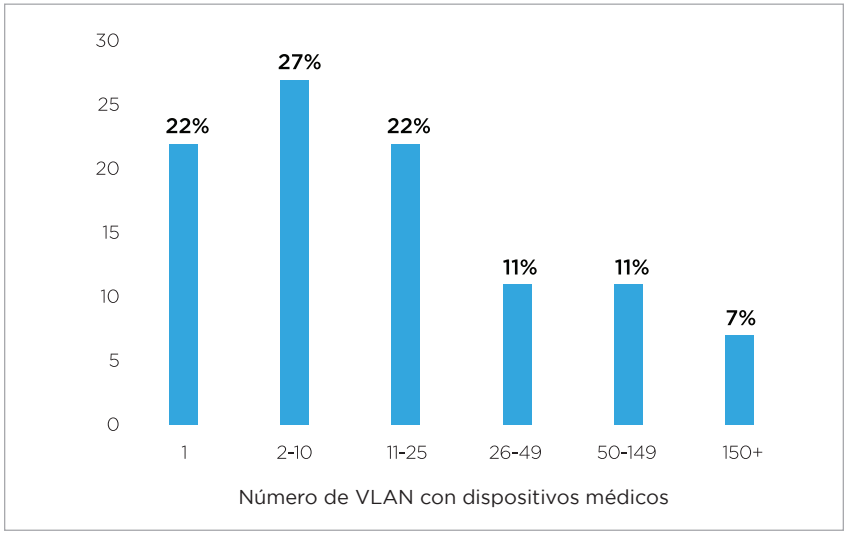

Figura 5: Número de VLAN con dispositivos médicos

Complejidad de proveedores de dispositivos en aumento

Las organizaciones sanitarias actuales están saturadas de tecnología. Históricamente, los proveedores de dispositivos no han diseñado los productos con la seguridad como prioridad principal, lo que los hace más difíciles de proteger. Además, los proveedores se dirigen a los médicos con dispositivos que acaban conectados a la red, pasando por alto los protocolos de seguridad y de riesgos. Los equipos de IT y de seguridad pueden detectar estos dispositivos conectados no autorizados, pero por lo general son incapaces de clasificarlos o localizarlos fácilmente.

Los campus de asistencia sanitaria no son en absoluto técnicamente homogéneos —más del 30 % de las VLAN médicas de las organizaciones admiten más de un centenar de proveedores de dispositivos distintos— y esa diversidad no incluye el número de proveedores de otras redes funcionales, como el back office, el front office, etc. En muchos casos, los propios proveedores son responsables de aplicar los parches y mantener los sistemas clínicos especializados.

El 34 % de las VLAN médicas de las organizaciones admiten más de 100 proveedores de dispositivos distintos.

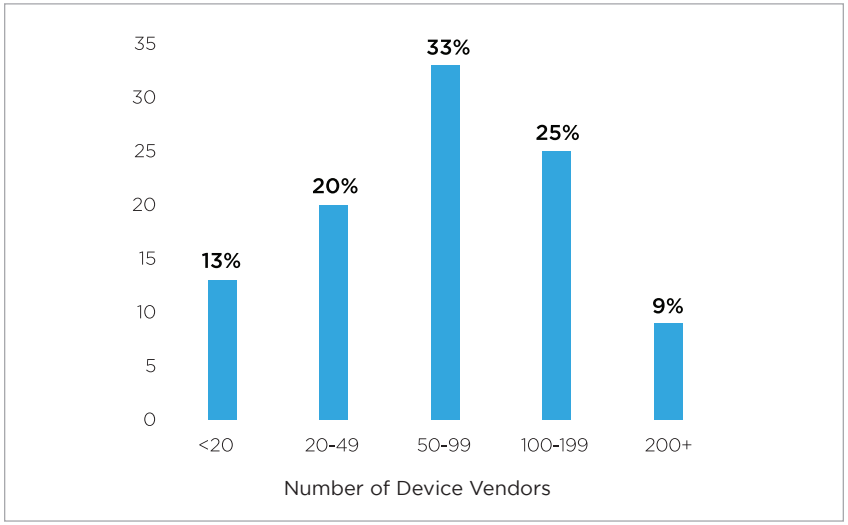

Figura 6: Número de proveedores de dispositivos en las VLAN médicas

Los servicios comunes descuidados convierten las redes en vulnerables

Un sorprendente número de dispositivos de las VLAN médicas tiene activado servicios de alto riesgo, lo que permite el acceso incontrolado que permitiría a los agresores atravesar el perímetro y desplazarse lateralmente. Los requisitos de acceso a proveedores médicos y a suministradores externos a menudo obligan a tener activados servicios como el escritorio remoto de Windows (RDP). Otras veces, los puertos de red se dejan abiertos de forma predeterminada sin el conocimiento del personal de IT y de seguridad.

- Protocolo SMB (Bloque de mensajes de servidor): SMB es el protocolo de transporte que utilizan las máquinas Windows para una serie de fines, como el uso compartido de archivos, de impresoras y el acceso remoto a servicios de Windows. WannaCry y NotPetya son dos ejemplos de ransomware que aprovechaba vulnerabilidades en el protocolo SMB.
- Protocolo de escritorio remoto (RDP): RDP es otro protocolo habitual que aprovechan las amenazas automatizadas, incluido el malware sin archivos.
- Protocolo de transferencia de archivos (FTP), Secure Shell (SSH), Telnet y el protocolo e intercambio de imágenes médicas DICOM (Digital Imaging and Communications in Medicine): vectores menos comunes, pero a menudo aprovechados, estos protocolos no protegen ni cifran las sesiones de red. Los modelos de seguridad no se combinan bien con una realidad de sistemas operativos heredados en la que demasiados dispositivos dependen de servicios básicos sin cifrar.

El 85 % de los dispositivos que ejecutan SO Windows tenían activado el protocolo SMB (Bloque de mensajes de servidor).

Servicio de Windows	Porcentaje que lo ejecuta
SMB	85%
RDP	32%
FTP*	1%
SSH	<1%
Protocolo Telnet*	<1%
Protocolo de imágenes DICOM	<1%

* Sin cifrar

Recomendaciones

Es inevitable: el número de dispositivos que se conectan a redes de asistencia sanitaria seguirá creciendo, y el entorno será cada vez más complejo. Ahora es el momento de empezar a desarrollar e implementar una estrategia de gestión de riesgos y de seguridad proactiva y en toda la empresa.

Permita el descubrimiento sin agentes de todos los dispositivos
Aunque los dispositivos con agentes de software facilitan a los encargados de la administración de la seguridad y de IT comunicarse con ellos y supervisar su actividad, la mayoría de los dispositivos médicos no admiten agentes. La detección sin agentes de todos los dispositivos conectados mediante IP en toda la red es primordial.

Identifique y clasifique los dispositivos automáticamente
No basta simplemente con detectar la dirección IP de un dispositivo. La clasificación automática rápida y granular es esencial para extraer la información contextual de cada dispositivo de la red y determinar su finalidad, propietario y nivel de seguridad. Esta información debe incorporarse a un inventario de activos en tiempo real para impulsar directivas de control de acceso y ayudar a los equipos de seguridad a responder rápidamente a los ataques selectivos sobre sistemas operativos o dispositivos específicos.

Supervise los dispositivos continuamente
Los dispositivos médicos deben supervisarse continuamente para detectar cualquier cambio en su nivel de seguridad. Un análisis puntual puede generar la costumbre de configurar y olvidarse, que generaría una fatiga de cumplimiento de normativas y propagaría el riesgo. La supervisión ininterrumpida de la red mediante técnicas pasivas y/o activas en entornos clínicos y de OT proporciona a los equipos de seguridad conocimiento situacional en tiempo real para vigilar continuamente la información y comportamiento de los activos, al tiempo que se aumenta la eficacia de los equipos de seguridad.

Implemente la segmentación
La segmentación de la red es una mejor práctica conocida, pero no es fácil de gestionar o implementar en toda la red. Los dispositivos de alto riesgo, como sistemas heredados, de los que se conocen sus vulnerabilidades, deberían segmentarse para contener una brecha potencial o limitar el riesgo.

Conclusión

Es fundamental que los líderes de la seguridad y gestión de riesgos de las organizaciones sanitarias se planteen la protección de todos los dispositivos de los entornos empresariales ampliados. Centrarse únicamente en proteger los dispositivos médicos en lugar de proteger todos los tipos de dispositivos puede provocar brechas importantes en su nivel de seguridad. Un enfoque holístico de la seguridad requiere de visibilidad y control permanentes de todo el ecosistema de dispositivos conectados, incluido el conocimiento del papel que puede jugar una plataforma de Device Visibility and Control en la organización de las acciones entre herramientas heterogéneas de administración de la seguridad y de IT.

Como se ha indicado anteriormente, los costes de la inacción pueden ser enormes. Cada segundo que un dispositivo permanece no conforme amplía su ventana de vulnerabilidad y su factor de riesgo, lo que expone a su organización sanitaria a importantes consecuencias financieras, comerciales y pone en riesgo la seguridad de los pacientes. Las organizaciones sanitarias tienen una opción: invertir en iniciativas de planificación y mitigación de riesgos proactivas ahora o pagar más tarde, y enfrentarse a la ira de las agencias normativas conscientes de la seguridad, los pacientes y los legisladores.

Acerca de Forescout Technologies

Forescout Technologies es líder en visibilidad y control de dispositivos. Nuestra plataforma unificada de seguridad permite a las empresas y organismos oficiales obtener información completa sobre el estado de sus entornos empresariales ampliados y orquestar medidas destinadas a reducir el riesgo operativo y de ciberseguridad. Los productos de Forescout se despliegan rápidamente y ofrecen descubrimiento y clasificación en tiempo real y sin agentes de todos los dispositivos conectados mediante IP, así como una evaluación continua de estado. A fecha de 31 de diciembre de 2028, 3300 clientes de más de 80 países confían en la solución independiente de la infraestructura de Forescout para reducir el riesgo de interrupciones de la actividad empresarial por incidentes de seguridad o fugas, garantizar y demostrar el cumplimiento en materia de seguridad y aumentar la productividad de las operaciones de seguridad. Descubra cómo en www.forescout.com.

Los investigadores de Forescout limitaron el ámbito de aplicación y la muestra de datos por razones de coherencia y la conveniencia de generar un informe único. Hemos observado limitaciones debidas al tipo de estudio, al momento, ámbito, anonimización de los datos, métodos de captura de datos pasiva, y errores en la clasificación basada en inteligencia artificial de las funciones, sistemas operativos y proveedores de los dispositivos. La realidad de utilizar datos de nube de entornos de producción reales significa asumir imperfecciones en el suministro de datos. Dentro de estos límites, los investigadores de Forescout han hecho todo lo posible para garantizar la coherencia, fiabilidad e integridad del informe.

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA
C. e.: info-espana@forescout.com
Tel. (internacional) +1-408-213-3191
Soporte técnico +1-708-237-6591