LA BRECHA EN LA SALUD

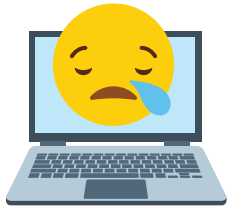
Cómo evitar la sobreexposición en la seguridad informática del sector de la salud.

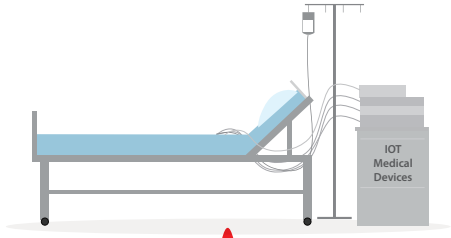
ÍNDICE

INTRODUCCIÓN

A medida que el sector de la salud continúa su cambio hacia un modelo de atención basado en el valor (generar menores costos y una mayor responsabilidad, además de enfocarse en la satisfacción del cliente), la mayoría de los establecimientos buscan las herramientas y las tecnologías adecuadas para hacerlo realidad. Con las innovaciones en la prestación de la atención que aparecen a diario en el mercado y que abren las puertas tanto a mejores tratamientos como a una mayor productividad y comunicación dentro de los establecimientos médicos, es difícil no sentirse optimista respecto de un futuro nuevo y prometedor.

Sin embargo, a pesar de todas las promesas, los establecimientos médicos no pueden dejar de lado los esfuerzos continuos para proteger los recursos de red y garantizar la privacidad. Dado que se debe tomar una dosis de hechos concretos (dos veces al día, a menos que un médico le indique lo contrario) con cualquier régimen nuevo de tecnología, este libro electrónico explorará los impulsores y avances clave del sector de la salud actual, los riesgos de seguridad de la información asociados y las soluciones que respaldan un plan saludable de implementación tecnológica.





Proliferación de la Telemedicina y los Centros de Atención

Panorama de Amenazas en Evolución

Protección de la Internet de las Cosas Médicas

Mantenimiento del Cumplimiento y la Acreditación

IMPULSORES DE MERCADO

Proliferación de la Internet de las Cosas Médicas (IoMT)

El negocio de la IoT está en auge y en expansión. Con la necesidad de tratamientos más avanzados y personalizados ejerciendo presión en el mercado, se prevé que la atención médica conectada alcanzará los **USD 117 mil millones para 2020**.

"State of the App Economy, 4th Edition", ACT.

Evolución de la Prestación de la Atención

Al facilitar las consultas médicas necesarias sin tener que pedir permisos en el trabajo o ir a una clínica, la Telemedicina está conquistando pacientes. De hecho, el **83 % de los pacientes que participaron en una cita médica de telesalud** expresaron haber **recibido atención de calidad**.

"20 Telemedicine Statistics Private Practices Should Know", iSalus Healthcare, (5 de abril de 2017).

Cumplimiento Normativo

La cantidad de días promedio entre una pérdida de datos de atención médica y el informe del incidente a la Oficina de Derechos Civiles (OCR) era de 174 días. Las organizaciones de la salud tardaban un promedio de **123,5 días** en descubrir que se había producido una pérdida de datos.

"Summary of January 2017 Healthcare Data Breaches", HIPAA Journal, emitido el 14 de febrero de 2017.

Ransomware en Aumento

La información de atención médica es única; por eso, su privacidad y seguridad son tan importantes. Mientras que las tarjetas de crédito pueden cancelarse en caso de robo, las historias clínicas pueden estar en peligro por años. Dicho esto, se estima que los **ataques de ransomware** dirigidos a **organizaciones** de la salud **se cuadruplicarán para 2020**.

"Ransomware Damage Report", Cybersecurity Ventures, 18 de mayo de 2017.

DESAFÍO

Proliferación de la Telemedicina y los Centros de Atención

Demasiadas personas y pocos asientos, inmersos en una cacofonía de estornudos, tos, resfríos y una sensación perturbadora de salir de allí con más gérmenes que con los que entró. La experiencia promedio en la sala de espera no es algo que los pacientes desean; es decir, suponiendo que pueden programar una consulta, en primer lugar. Con una escasez nacional de médicos causada por el crecimiento de la población y el envejecimiento de la generación de la posguerra, los pacientes ahora esperan un promedio de 24 días[1] para una cita programada con el médico. La experiencia puede ser estresante también para los proveedores de atención. Con salas de espera normalmente a punto de explotar, muchos médicos se sienten en conflicto si hacen pausas cortas entre consultas.

Conozca la telemedicina. Al permitir que los profesionales de atención médica puedan evaluar, diagnosticar y tratar a pacientes sin importar la distancia utilizando la tecnología de las telecomunicaciones, la telemedicina permite horarios de oficina más flexibles, menos pacientes en las salas de espera y menos incumplimiento de planes de tratamiento por parte de los pacientes, ya que es posible hacer un seguimiento más sistemático a través de videollamadas en lugar de visitas clínicas. Además, la telemedicina brinda un nuevo flujo de ingresos para los médicos; de hecho, con un adicional de cinco llamadas de telesalud al día, cinco días a la semana, un médico puede sumar potencialmente USD 3500 a sus ingresos mensuales*.

Sin embargo, como sucede con todas las comunicaciones digitales, la telemedicina trae aparejadas preocupaciones considerables en cuanto a la seguridad informática y la privacidad. El robo de identidades médicas ha aumentado significativamente en los últimos años, y si bien la mayoría de los consultorios requieren que los pacientes presenten credenciales de seguro médico y DNI, los pacientes de telemedicina son remotos, lo que facilita la obtención de un tratamiento usando una identidad robada. La telemedicina también brinda un mar de información nueva que debe registrarse, que viaja desde el dispositivo del paciente hasta el proveedor, y continúa hasta su parada final en la Historia Clínica Electrónica (EMR) del paciente. Todas las etapas del recorrido de la información, desde la transmisión hasta el almacenamiento, deben realizarse priorizando la seguridad de los datos.

Con la incorporación de **cinco** llamadas de telesalud por día, **cinco** días a la semana, un médico puede incorporar potencialmente **USD 3500 a sus ingresos mensuales.**

1. "2017 Survey of Physician Appointment Wait Times" Merritt Hawkins.

SOLUCIÓN

Para: Proliferación de la Telemedicina y los Centros de Atención

Rx

Verificación de Identidad

Solicitar imágenes de la tarjeta médica de identificación de un paciente remoto y su DNI durante la "visita" médica es un gran avance hacia la prevención del robo de identidad en entornos de telemedicina. Del mismo modo, la autenticación multifactor y las contraseñas complejas ayudan a garantizar que solo los usuarios autorizados puedan acceder a los sistemas de atención médica para realizar consultas.

Acceso Remoto Seguro

Contar con una conexión segura entre los médicos y los pacientes remotos es un requisito ineludible. Las soluciones de Gestión Unificada de Amenazas (UTM) Firebox® de WatchGuard incluyen la creación de VPN con drag-and-drop, lo que protege el recorrido desde el paciente a la EMR mediante el cifrado de las comunicaciones de datos.

Rendimiento

Sería extremadamente negativo que el sistema dejara de funcionar en medio de un examen o un diagnóstico. Por ello, para mantener las operaciones de telemedicina, los dispositivos de firewall deben admitir altas velocidades, voz sobre protocolo de Internet (VoIP) y un gran ancho de banda con configuraciones de Calidad de Servicio (QoS) y la agrupación en clústeres para contar con los tiempos de actividad más altos posibles.

Privacidad de la Cita

Se debe aconsejar a los pacientes que realicen las citas de telemedicina desde una ubicación privada, de ser posible, y que no compartan con terceros accesos, contraseñas ni ninguna otra información de acceso.

_ WatchGuard

DESAFÍO

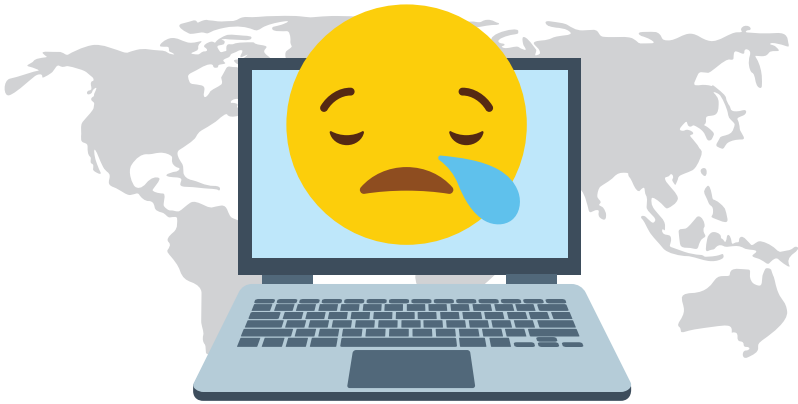
Un Panorama de Amenazas en Evolución

Con consecuencias que van desde inconvenientes costosos a catástrofes, el ransomware se ha arrastrado desde la Internet obscura hacia las noticias principales de todo el mundo. La primera vez que llamó la atención fue alrededor del 2005 en Europa del Este. Esta variante de malware trabaja de la siguiente manera: infecta una computadora, bloquea al usuario del sistema (normalmente mediante el cifrado de la información del disco duro) y luego se apodera del descifrado o de otra clave de liberación hasta que la víctima hace un pago, generalmente en Bitcoin.

Al contar con acceso a información precisa de las historias clínicas electrónicas para brindar atención crítica, la industria de la salud emergió como un objetivo popular para las extorsiones de ransomware, principalmente porque hay mucho en juego. Debido a la necesidad urgente de reestablecer el servicio para los pacientes, es posible que los hospitales paguen a los criminales a fin de reponer los sistemas críticos.

Cuando un hacker tomó control de su red y se negó a liberarla sin el pago, el Hollywood Presbyterian Medical Center pagó no menos de USD 17.000 en Bitcoin para reanudar las operaciones normales. No tan lejos de esa historia de advertencia, WannaCry, la ahora famosa variante de ransomware que aprovechó una vulnerabilidad en las versiones anteriores del sistema operativo Windows, infectó a una multitud de computadoras a su paso: cerca de 200.000 en 150 países. El sector de la salud se vio muy afectado, lo que causó un estado de crisis en hospitales y clínicas alrededor del mundo. Los establecimientos del Servicio Nacional de Salud (NHS) en Inglaterra experimentaron interrupciones en las computadoras y los sistemas telefónicos, fallas en el sistema y, finalmente, una ola de demoras en cirugías, citas canceladas y confusión luego de que las computadoras del hospital mostraran un mensaje de rescate que demandaba un pago en Bitcoin. Uno de los mayores fabricantes de medicamentos de la industria, Merck, confirmó que cayeron en manos de esta fuerte variante, con ataques que se extendieron a todas sus oficinas en el mundo. Estos incidentes no solamente tienen gran impacto en los resultados de los pacientes a corto plazo, sino que también afectan la capacidad del establecimiento para competir a largo plazo si su reputación se ve dañada.

WannaCry, la variante de ransomware que aprovechó una vulnerabilidad en las versiones anteriores del sistema operativo Windows, infectó a una multitud de computadoras a su paso: cerca de **200.000** en **150 países.**



SOLUCIÓN

Para: Panorama de Amenazas en Evolución

Rx

Defensas en Capas

La proliferación de estos ataques prueba que la seguridad en capas de nivel empresarial ya no es un lujo, sino una necesidad para todas las organizaciones. El 38 %[2] del malware pasa desapercibido ante el antivirus heredado, razón por la cual los servicios como el Servicio de Prevención de Intrusiones (IPS), los espacios aislados y la detección y respuesta son tan importantes: ninguna solución única brindará 100% de cobertura. Total Security Suite de WatchGuard ofrece un conjunto integral de servicios coordinados de seguridad, entre ellos, APT Blocker y Threat Detection and Response. A las ya sólidas defensas perimetrales basadas en firmas con Gateway AntiVirus (GAV) e IPS se les suma el análisis de comportamientos y la inteligencia correlacionada para detener el malware avanzado y brindar soluciones en tiempo casi real.

Actualización del Enfoque de Seguridad

Verifique regularmente su configuración de firewall en busca de vulnerabilidades; no establezca una configuración "para siempre". De hecho, las pruebas continuas y las actualizaciones posteriores o su infraestructura completa de seguridad de red son clave para una protección efectiva. Las amenazas están evolucionando constantemente; sus defensas también deberían hacerlo.

Educación del Personal

El programa de formación de consciencia sobre la seguridad para el personal es elemental a fin de evitar que las personas hagan clic en correos de suplantación de identidad, un lugar de entrada común para el ransomware. La educación del usuario debe incluir a todos, desde el personal administrativo hasta los ejecutivos de alto nivel, ya que cualquier persona puede hacer clic en un enlace equivocado en el momento correcto. Dado que tener un programa efectivo sobre conciencia de seguridad requiere un enfoque profesional con la presencia de un especialista, los establecimientos de la salud pueden beneficiarse del programa de formación externo a través de una compañía de consciencia sobre la seguridad.

Copias de Seguridad

Parece obvio, pero hay una razón por la cual las compañías pagan los rescates que demandan los hackers: no hacen copias de seguridad de la información. Los proveedores de servicios administrados que se especializan en el proceso de hacer copias de seguridad y salvaguardar la información pueden brindar asistencia y tienen muchos conocimientos para ayudar a las organizaciones a protegerse de ataques informáticos como el ransomware.

– WatchGuard

2. "Q1 2017 Internet Security Report", WatchGuard Technologies.

DESAFÍO

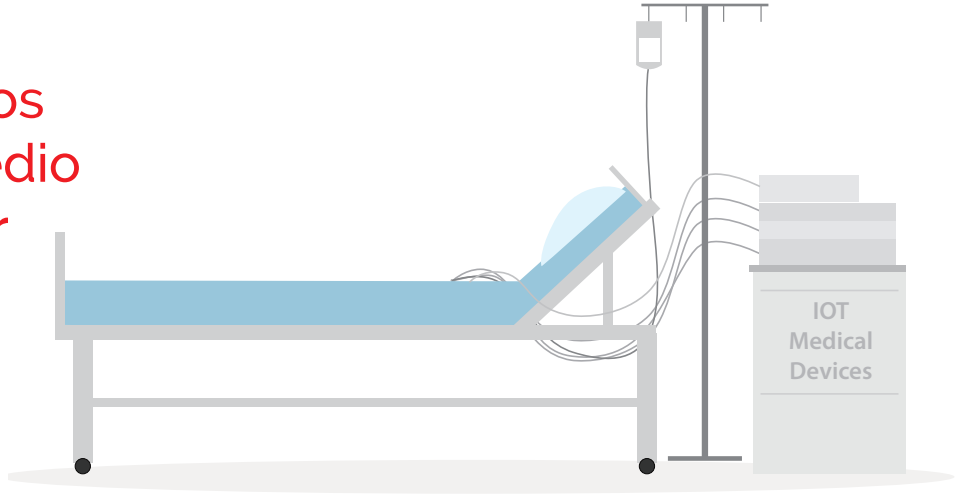
Protección de la Internet de las Cosas Médicas (IoMT)

La Internet de las Cosas Médicas está transformando al sector de la salud; redefine la manera en que interactuamos, nos sanamos, vivimos y nos desarrollamos. Los dispositivos quirúrgicamente embebidos, que incluyen desfibriladores, bombas de infusión, marcapasos y mucho, mucho más, ahora incorporan Wi-Fi, monitoreo remoto y tecnologías de comunicación de campo cercano. A su vez, permiten a los profesionales de la salud modificar y ajustar los dispositivos implantados sin procedimientos invasivos. Otro subgrupo de IoT médicas, los dispositivos médicos parlantes, ofrecen señales de audio con recordatorios sobre medicamentos, información de los procedimientos y más. Este tipo de dispositivos no solo pueden ser utilizados por los pacientes, sino también por el personal del hospital. Hay termómetros parlantes que leen las temperaturas actuales con solo hacer clic en un botón, e incluso hay planes de desarrollar "vendajes inteligentes", capaces de indicar si una herida ha sanado y enviar un informe de progreso al médico.

Con una mejor experiencia del paciente, con costos de la atención médica reducidos significativamente y mejores resultados en los tratamientos. Los beneficios de la IoT médica son, sin lugar a dudas, emocionantes. Sin embargo, a medida que los hackers toman ventaja de la seguridad generalmente débil de los dispositivos embebidos, defender a estos dispositivos y a las personas que están conectadas a ellos ha generado una nueva urgencia, ya que la naturaleza intrínsecamente personal de esos dispositivos puede producir consecuencias graves.

En primer lugar, hay una necesidad imperiosa de proteger a los pacientes que están conectados, ya que los atacantes podrían acceder a una bomba de infusión desprotegida y administrar una dosis fatal. Los dispositivos médicos vulnerables también se conectan a una amplia variedad de sensores y monitores, y eso los convierte en puntos de entrada a las grandes redes del hospital y al robo de historias clínicas electrónicas confidenciales, o a un ataque devastador de ransomware que puede capturar sistemas claves. Teniendo en cuenta que la mayoría de los hospitales normalmente tienen un promedio de 10 a 15 dispositivos conectados por cama, la exposición a esos riesgos es elevada y aumenta cada vez más.

Teniendo en cuenta que la mayoría de los hospitales normalmente tienen un promedio de **10 a 15 dispositivos conectados por cama**, la exposición a esos riesgos es elevada y **aumenta** cada vez más.



SOLUCIÓN

Para: Protección de la Internet de las Cosas Médicas (IoMT)

Rx

Segmentación de IoT

Los firewalls protegen los dispositivos de IoT y previenen así que hackers, virus y gusanos alcancen sus dispositivos conectados por Internet al denegar el tráfico no autorizado. Segmente su red de IoT para una mejor protección del servicio de Gestión Unificada de Amenazas (UTM). Mientras más segmente sus redes, más difícil será para los hackers acceder a todos sus dispositivos e información.

Secure Wi-Fi con Administración en la Nube

Tanto los dispositivos de IoT de los pacientes como los del personal requieren acceso Wi-Fi sistemático y confiable, pero es indispensable que el acceso también sea seguro. Los puntos de acceso con administración en la nube de WatchGuard tienen un Sistema de Prevención de Intrusiones Inalámbricas (WIPS) integrado para garantizar la protección y extender y mejorar nuestra seguridad para los dispositivos IoT inalámbricos. Al aprovechar la tecnología patentada Marker Packet, WatchGuard brinda el WIPS más confiable de la industria con la tasa más baja de falsos positivos. Esta solución puede utilizarse como seguridad inalámbrica solo en conjunto con una infraestructura existente de Wi-Fi; no tiene que ser una solución que se quita y reemplaza.

– WatchGuard

2. "Q1 2017 Internet Security Report", WatchGuard Technologies.

DESAFÍO

Mantenimiento del Cumplimiento y la Acreditación

Según lo estipula la necesidad universal de recibir atención segura y de calidad, las organizaciones de la salud de cada región alrededor del mundo deben cumplir con las regulaciones de privacidad y los programas de acreditación hospitalaria locales y nacionales. La Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA), introducida en 1996, estableció las normas para la protección de la información de los pacientes en los EE. UU. Como parte de esta ley, se establecieron reglas de privacidad y seguridad que especifican los resguardos que deben implementarse a fin de proteger la confidencialidad e integridad de la Información Médica Protegida (PHI). Inicialmente, solo se les pedía a los médicos, los hospitales y las compañías de seguros que cumplieran con las especificaciones de HIPAA, pero una actualización de 2013 aumentó el alcance de la HIPAA para abordar el incremento en el uso de la tercerización y de proveedores de servicios en la nube para la atención médica. Cualquier servicio que transmita, almacene o reciba información médica protegida ahora se clasifica como "Socio comercial" y debe cumplir con la ley HIPAA. El incumplimiento origina multas desde cientos hasta millones de dólares, sin mencionar la costosa pérdida de credibilidad y la posible revocación de licencias médicas.

A escala internacional, la Comisión Conjunta Internacional (JCI) también se enfoca en mejorar la seguridad del paciente mediante la educación, servicios de asesoría y acreditación en más de 100 países. El programa de acreditación incluye una encuesta en el sitio a cargo de un equipo de la comisión que se realiza al menos una vez cada tres años y se enfoca en la calidad y la seguridad general de la prestación de atención médica en el establecimiento, incluido el programa de TI. Si bien la organización no tiene poder concreto para imponer sus normas, muchas regiones dentro de los EE. UU., por ejemplo, requieren que los hospitales alcancen la acreditación de la Comisión Conjunta incluso para reunir los requisitos de obtención de licencias y reembolsos de Medicare.

Una actualización de 2013 **aumentó el alcance de la ley HIPAA** para abordar el **uso incrementado de la tercerización** y de **proveedores en la nube** para la atención médica.

SOLUCIÓN

Para: Mantenimiento del Cumplimiento y la Acreditación

Rx

Políticas y Procedimientos Estandarizados

Establecer un conjunto de estándares personalizados para su organización puede ayudar a guiar el comportamiento del personal hacia prácticas más seguras. Las políticas son necesarias para cumplir con la norma 164.316(a) de Requisitos Organizacionales, de Políticas, Procedimientos y Documentación de HIPAA para las entidades cubiertas, y deben abordar la gestión de contraseñas, el almacenamiento/uso de la PHI, el cifrado, los procedimientos de intercambio de PHI, los filtros de privacidad, etc.

Controles de Acceso

Limite el acceso a la información confidencial de la red solo a aquellas personas cuyos roles dentro de la organización lo requieran. Los dispositivos Firebox de WatchGuard le permiten controlar y auditar fácilmente quiénes pueden acceder a los recursos confidenciales de la red.

Visibilidad

La opción de generación de informes y monitoreo granular de su red es clave para lograr y mantener el cumplimiento. Dimension, una solución de visibilidad de red apta para la nube que en su formato estándar cuenta con la plataforma de firewall de Gestión Unificada de Amenazas (UTM) de WatchGuard, incluye plantillas de informes de HIPAA que facilitan la comprobación del estado del cumplimiento.

_ WatchGuard

El potencial de la tecnología incipiente dentro del sector de la salud no tiene límites, transforma la prestación de la atención, la satisfacción del paciente y la industria en sí. Con las soluciones intuitivas de WatchGuard, la calidad y el equipamiento de la atención médica pueden seguir evolucionando de manera segura.

Oficina Central Internacional
Estados Unidos
Tel.: +1.800.734.9905
Correo electrónico:
sales@watchguard.com

Oficina Central de Europa
Países Bajos
Tel.: +31(0)70.711.20.85
Correo electrónico:
sales-benelux@watchguard.com

Oficina central de Asia, el Pacífico
y el Sudeste Asiático
Singapur
Tel: +65.6536.7717
Correo electrónico:
inquiry.sea@watchguard.com