Akamai

DOCUMENTO

Ciberseguridad para proveedores de atención sanitaria

Introducción

Para competir en un mercado en constante cambio, los proveedores de atención sanitaria adoptan nuevos dispositivos y aplicaciones con el fin de proporcionar a sus pacientes un servicio de primera calidad y una experiencia de nivel superior. Cada nueva incorporación aporta sus propias ventajas a los pacientes, pero también toda una serie de riesgos de seguridad a la organización.

Este complejo entorno de TI, combinado con el alto valor de la información sanitaria protegida (PHI), crea una oportunidad irresistible para los ciberdelincuentes, que no cesan en sus ataques a los sistemas. Según un informe del Departamento de Salud y Servicios Humanos (HHS) y una investigación de IBM, el sector sanitario ha experimentado un aumento del 50 % en ciberataques desde el inicio de la pandemia, y esos ataques fueron los más caros, con un coste medio de 7,13 millones de dólares por incidente. Dicho informe de IBM destacó que los ataques de ransomware eran la amenaza más común, ya que los agentes maliciosos se aprovechaban de la necesidad de restaurar rápidamente los sistemas hospitalarios y sanitarios, seguidos del robo de datos y el acceso a servidores. En concreto, los proveedores de atención sanitaria resultan objetivos muy atractivos para el ransomware, ya que los historiales médicos electrónicos (EHR) pueden alcanzar un precio de 1000 dólares en la Dark Web, un alto valor si se compara con la información de tarjetas de crédito, que se vende a unos 110 dólares, y los números de la seguridad social, que tienen un valor de 1 dólar.

Con un número cada vez mayor de amenazas contra sus sistemas, muchas organizaciones no están preparadas adecuadamente para mitigarlas. Lo que es peor, algunas ya han sufrido una filtración y no lo saben. Es posible que los atacantes ya estén exfiltrando datos o esperando el momento adecuado para atacar.

Ahora es el momento de obtener más claridad sobre la superficie de ataque de su organización haciendo un inventario de los dispositivos y cómo se conectan a su infraestructura. Con un mejor conocimiento de dónde existen vulnerabilidades, poner en marcha un plan de mitigación sólido evitará o minimizará el posible impacto de los ciberataques.

Cómo cubrir los mayores riesgos de ciberseguridad para su organización

Amenaza n.º 1: Ataques de phishing

El phishing es uno de los vectores de ciberataques más comunes en todos los sectores. Según Health Sector Cybersecurity Coordination Center, el año 2021 trajo un considerable aumento en los ataques de phishing en el sector sanitario. De hecho, durante el año 2020, Akamai observó que los delincuentes se aprovecharon de la situación generada por la pandemia y de la promesa de ayudas económicas, o del estrés generado por las dificultades económicas, para arremeter contra personas de todo el mundo a través del phishing.

El phishing intenta conseguir datos confidenciales a través de correos electrónicos o páginas web fraudulentos. Cuando se verifica, incita al usuario, no consciente de que es una trampa, a introducir sus credenciales de inicio de sesión, lo que básicamente proporciona a los autores una puerta abierta a la red.

Esto le sucedió a los solicitantes del subsidio por desempleo de Nueva York. Según un informe sobre phishing de Steve Ragan, antiguo editor de CSO Online y actual investigador de seguridad de Akamai, a principios de 2021 hubo varios kits de phishing dirigidos a programas de Asistencia de Desempleo por la Pandemia (Pandemic Unemployment Assistance, PUA). Se trataba de programas diseñados para ayudar a quienes lo necesitasen durante los confinamientos a causa de la COVID-19 y que proporcionaron servicios esenciales a millones de estadounidenses.

En un anuncio retransmitido por CBS News en todo el país, Ragan habló sobre un kit de phishing dirigido a personas desempleadas de Nueva York y de cómo los delincuentes recopilaban y vendían información personal comprometida en la estafa. Desde que se emitió esa noticia, descubrió estafas de PUA dirigidas a personas de Wisconsin, Indiana, Pensilvania y Massachusetts.

Cómo detener y mitigar los ataques de phishing

En función de cómo estén configurados los permisos y de las medidas de seguridad establecidas, el acceso a una única cuenta de usuario puede proporcionar a los delincuentes vía libre para acceder a partes críticas de la red, y a menudo les permiten ampliar su radio de acción una vez que están dentro de la red de la organización.

La microsegmentación limita el acceso de los atacantes solo a la parte de la red a la que inicialmente obtienen acceso, lo que les impide moverse lateralmente e infligir más daños en otras áreas. Limita el impacto de una vulneración al impedir que los delincuentes utilicen cualquier punto de entrada para acceder a la red de su organización en general.

Además de la microsegmentación, la autenticación multifactorial (MFA) es una de sus mejores líneas de defensa contra los ataques de phishing. Proporciona una capa extra de protección al requerir una verificación de identidad adicional antes de permitir el acceso a una cuenta, lo que evita que se aprovechen las credenciales comprometidas.

La MFA, en concreto una solución aprobada por FIDO2, garantiza la protección contra los ataques más recientes y requiere que los usuarios introduzcan un código único que se genera a través de una aplicación de autenticación o mensaje de texto en el dispositivo móvil del usuario. Este paso adicional en el inicio de sesión ayuda a frustrar los ataques de phishing, incluso cuando los delincuentes tienen credenciales de inicio de sesión precisas.

Es fundamental formar a su personal sobre las tácticas de los ataques de ingeniería social, como el phishing. La realidad es que el phishing es uno de esos problemas que no tienen una solución infalible, porque hay muchas variables en juego. Es difícil predecir qué harán los criminales a continuación. Dado que los seres humanos siguen siendo un aspecto vital del phishing, seguirán siendo el eslabón más débil de la cadena.

Esto significa que facilitar la seguridad es esencial. Akamai ofrece una solución MFA antiphishing fluida para proteger incluso contra los ciberdelincuentes más astutos.

Amenaza n.º 2: Software heredado obsoleto

El software desactualizado es otra preocupación importante en cuanto a la vulnerabilidad. Cada nueva actualización de seguridad (parche) que no se instala inmediatamente crea puertas traseras abiertas en la red. Esto sucede especialmente en el caso de los dispositivos más antiguos que no cuentan con soporte y que ya no reciben actualizaciones.

El software obsoleto puede presentar vulnerabilidades de día cero para las que las organizaciones pueden dudar si corregir por sí mismas. La creación de un parche personalizado a veces puede anular la garantía de un dispositivo, lo que conlleva costosas reparaciones cuando algo sale mal.

Aunque los dispositivos médicos tienen un ciclo de vida largo, si no se actualizan con diligencia con la última versión del sistema operativo o si ejecutan un sistema operativo obsoleto, los hackers pueden aprovechar las vulnerabilidades para robar datos, infiltrarse en la red de un hospital e interrumpir la atención sanitaria. De hecho, hasta el 83 % de los dispositivos de adquisición de imágenes médicas conectados a Internet (desde máquinas de mamografía hasta máquinas de resonancia magnética) son vulnerables, según informa Fortune.

Cuanto más antiguo sea un dispositivo, especialmente aquellos que se encuentran fuera del ciclo de vida de mantenimiento, más probable es que los delincuentes conozcan los puntos débiles que les permiten acceder a la red de su organización a través de un dispositivo de terceros.

Por ejemplo, Windows 95 lleva años sin mantenimiento y, sin embargo, muchas máquinas de resonancia magnética (entre otras) siguen dependiendo de ese sistema operativo, ya que fue el último en permitir la escritura directa. Los desarrolladores internos podrían corregir una vulnerabilidad, pero su parche podría anular la garantía de la máquina. La única opción segura es sustituir la máquina de resonancia magnética por completo, pero el coste es prohibitivo para muchos centros.

Los administradores de red intentan mantener los sistemas obsoletos fuera de la red, pero no siempre es posible, especialmente cuando son necesarios para la atención al paciente y deben proporcionar datos rápidamente a los médicos. El aislamiento también falla cuando hay un mapa incompleto de todos los dispositivos conectados a la red, lo que crea puertas traseras. Es difícil proteger lo que no se puede ver.

Cómo proteger dispositivos vulnerables no compatibles

Para evitar que estos dispositivos proporcionen acceso a la red de su organización, es fundamental adoptar una arquitectura de acceso de red Zero Trust (Zero Trust Network Access, ZTNA). ZTNA es un marco que trata cada solicitud entrante como una posible amenaza hasta que se demuestre que es segura, lo que detiene de forma eficaz a los atacantes antes de que tengan acceso al dispositivo, incluso si el software no está actualizado.

La adopción de la arquitectura ZTNA supone un cambio fundamental del enfoque casi medieval de los años anteriores a un modelo Zero Trust (comprobar la identidad en primer lugar y, a continuación, confiar). Si bien es probable que un enfoque Zero Trust no ofrezca protección total contra los ciberataques, limita el daño potencial de catastrófico a manejable. HealthITSecurity lo expresa mejor: "Si un atacante consigue obtener credenciales y manipular un dispositivo, es poco probable que llegue mucho más lejos con una arquitectura Zero Trust".

Akamai ofrece un plan sólido para ayudar a los proveedores a migrar a una arquitectura Zero Trust, sin tiempo de inactividad y con la flexibilidad de los flujos de trabajo actuales. Comience con la arquitectura ZTNA con esta guía de base.

Amenaza n.º 3: Proveedores que trabajan desde casa e iniciativa "traiga su propio dispositivo" (BYOD)

La continuidad de la atención en el siglo XXI está descentralizada. Los pacientes reciben atención desde la comodidad de sus hogares. Los proveedores prestan atención a través de su dispositivo móvil en lugar de en persona. Sin embargo, este aumento de la accesibilidad significa que los riesgos de ciberseguridad de los proveedores aumentan drásticamente a medida que los miembros del personal oscilan entre el acceso a las redes in situ y desde casa, e inician sesión desde dispositivos no gestionados.

Aunque es posible que los miembros de su equipo hayan iniciado sesión ocasionalmente en su sistema desde su red doméstica antes de la pandemia, el número de dispositivos personales que accedían a la red de su organización inevitablemente se disparó durante este periodo. Si esos portátiles, tablets o smartphones estuvieran infectados con malware, podrían convertirse en un punto de entrada para un ataque de ransomware.

Por ejemplo, si alguien de su equipo es víctima de un ataque de phishing al introducir accidentalmente sus credenciales de inicio de sesión en una página web falsa, los agentes maliciosos tendrán el mismo acceso que el usuario, lo que podría permitirles cifrar archivos, bloquear a su equipo o paralizar su organización y exigir un rescate cuantioso para descifrar los archivos.

Cómo proteger el Edge de su red

Al supervisar de cerca quién accede a la red de su organización (dónde está, cuál es su dirección IP, qué dispositivo está utilizando, etc.), puede minimizar la probabilidad de que se produzca una situación como esta y actuar para detener un ataque antes de que ocurra.

Si su equipo utiliza dispositivos personales o trabaja desde casa, hágase estas preguntas:

- ¿Disponemos de un enfoque de acceso de red Zero Trust (ZTNA) para maximizar el escrutinio de las solicitudes entrantes y detener un ataque antes de que se produzca?
- ¿Hemos establecido la microsegmentación para limitar el acceso y evitar el movimiento lateral si un delincuente consigue entrar en la red de la organización?
- ¿Utilizamos un marco de acceso seguro a los servicios en el Edge (SASE) para proteger nuestra red al tiempo que minimizamos la latencia y mantenemos una experiencia de usuario rápida y agradable?
- ¿Utiliza nuestro equipo códigos de acceso, contraseñas seguras y únicas y autenticación multifactorial (MFA) para el acceso a cada dispositivo y cuenta?

Akamai facilita la gestión del acceso a la red con sus soluciones de seguridad para teletrabajadores.

Amenaza n.º 4: Asignación de flujo de datos deficiente

Con un pie en el entorno local y el otro en la nube, puede ser casi imposible comprender dónde residen los datos y cómo fluyen. Esto sucede por dos motivos diferentes.

En primer lugar, el volumen. Puede resultar abrumador mantenerse al día con el número de dispositivos y aplicaciones que se añaden y se eliminan de la red a diario (incluso cada hora), ya que los proveedores, contratistas y consultores parecen utilizar, cada uno, diferentes dispositivos, herramientas y soluciones.

En segundo lugar, el sistema de seguimiento de hardware y software ha dejado de ser preciso y fiable debido a la rotación de miembros del equipo, cambios en los procesos o prioridades contrapuestas.

Independientemente del motivo, es importante visualizar la red y los dispositivos conectados, ya que no se puede proteger lo que no se puede ver.

Cómo asignar el flujo de los dispositivos conectados

Es fundamental contar con una herramienta de visibilidad capaz de crear una hoja de ruta de los dispositivos conectados. Sobre todo, teniendo en cuenta, como cita un artículo de publicado en HIPAA Journal en 2019, que el 82 % de las organizaciones sanitarias sufrieron un ciberataque en sus dispositivos conectados en los 12 meses anteriores.

Elegir una solución que realice un seguimiento del flujo de datos a través de la red y le indique de dónde vienen y hacia dónde van (incluidos los dispositivos que no están conectados a la red) es el primer paso para asignar los dispositivos conectados. Esto le permite disponer de un diagrama de red en tiempo real de dónde fluye la información y le ayuda a detectar dispositivos con intenciones maliciosas que pueden estar en su red. Al poner anillos de microsegmentación definida por software alrededor de los sistemas, activos y datos principales (como la información sanitaria protegida), su organización puede limitar el movimiento lateral de los atacantes dentro de su red. Obtenga la visibilidad que necesita con las herramientas de microsegmentación de Akamai.

Amenaza n.º 5: Gestión de la complejidad de las redes, las aplicaciones y los sistemas

¿Sabe qué aplicaciones y software pueden leer sus datos? Algunas aplicaciones de software, como las plataformas de redes sociales, indican claramente su carácter invasivo en su declaración de privacidad o en los términos de servicio. Otros, como los proveedores de correo electrónico, son más encubiertos, pero siguen planteando un riesgo considerable (por ejemplo, al tener acceso a las fotos de un dispositivo cuando las imágenes contienen PHI).

También se puede permitir que las aplicaciones vean elementos copiados en el portapapeles, incluidos identificadores o contraseñas de pacientes. Si hay información del paciente en un dispositivo, existe la posibilidad de que un tercero (o un agente malintencionado) la vea (y la registre).

Forme a su equipo, vea toda su red y proteja su Edge

Es fundamental mentalizar a todos los miembros de la organización proveedora sobre los riesgos de utilizar dispositivos personales y sobre las medidas necesarias para proteger la información privada de los pacientes.

También es importante tener en cuenta la visión que tiene su organización de la superficie de ataque y los posibles vectores. ¿Su equipo de seguridad supervisa toda la red en torno a los diferentes proveedores de servicios en la nube y centros de datos locales? ¿O están aislados en varios grupos centrados en diferentes aspectos de la infraestructura de su organización? Es imprescindible mantener una visión integral de toda la red de la organización y de su actividad, especialmente durante un ataque.

Al igual que con la amenaza n.º 4, las mejores opciones de defensa para proteger el Edge de su red son una arquitectura Zero Trust combinada con microsegmentación y MFA para el inicio de sesión en las cuentas. Emplear un único proveedor para proteger todos los sistemas, independientemente de a quién pertenezcan y de si se encuentran en la nube o en el entorno local, le permitirá proteger su red sin dificultar la experiencia del usuario.

¿Cuál es el coste de la inacción?

Los costes pueden adoptar muchas formas. La más obvia es la financiera, ya que las empresas del sector sanitario de EE. UU. tienen de media 9,23 millones de dólares en costes totales asociados a una sola filtración de datos, según el informe Cost of a Data Breach 2021 de IBM. Otros costes son más cualitativos, como la seguridad y la confianza de los pacientes, que pueden tener una repercusión igual, si no mayor, en las organizaciones sanitarias.

Reducción de la seguridad de los pacientes

La seguridad de los pacientes es el objetivo más importante en lo que respecta a la ciberseguridad. Cuando los sistemas de TI se ven obligados a apagarse por un ataque, la atención a los pacientes se ve interrumpida. Los tratamientos y las citas se posponen y esto puede tener consecuencias negativas en la salud de los pacientes. De hecho, una demanda reciente marcó la primera denuncia de la muerte de un paciente como resultado directo de un ataque de ransomware.

Por otra parte, los dispositivos médicos conectados que se utilizan para la monitorización remota de pacientes (por ejemplo, la frecuencia cardíaca o los niveles de glucosa) suponen una amenaza más directa para la atención sanitaria. Por ejemplo, la interrupción de las mediciones de la presión arterial de un paciente puede provocar que enfermedades peligrosas pasen desapercibidas y no se traten, lo que podría causar un evento centinela.

Pérdida de la confianza de los pacientes

La incapacidad de proporcionar una atención médica fiable y de proteger la información de los pacientes lleva a una pérdida de la confianza de estos últimos. Más del 90 % de los pacientes afirma que cambiaría de proveedor si su información privada se viera comprometida como consecuencia de una filtración de datos. El número real puede ser inferior llegado el momento, pero haga los cálculos: incluso si solo la mitad de esos pacientes se fueran, o una décima parte, ¿qué repercusión tendría en su base de pacientes? ¿Y cuánto tiempo incurriría en pérdidas continuas mientras consigue gradualmente nuevos pacientes?

Pérdida de ingresos

Con un 38 %, la pérdida de negocio es el mayor factor de coste asociado a una filtración de datos. Cuando los sistemas principales de los proveedores dejan de funcionar (como los historiales médicos, los servidores de correo electrónico, etc.), los negocios entrantes se detienen de forma brusca. Esto supone que no haya citas, visitas, encuentros ni ingresos (por no mencionar el impacto que tiene en la atención a los pacientes).

Scripps Health, con sede en San Diego, sufrió un importante ciberataque en mayo de 2020 que provocó una pérdida de ingresos de 91,6 millones de dólares, principalmente por la reducción del volumen de atención en el departamento de urgencias y en las cirugías electivas.

Incluso si algunas partes de la red del sistema sanitario siguen funcionando, no se puede estar seguro de que todo esté a salvo hasta que se haya localizado el vector, se haya aplicado un parche para la vulnerabilidad y se haya completado el análisis forense.

Aumento de los gastos generales

Contratar y retener a los codiciados ingenieros de ciberseguridad es costoso, pero los costes reales van mucho más allá. El empleo de un equipo de ciberseguridad propio en su organización puede dejarle con costosas deficiencias en la cobertura.

En términos generales, cuanto más tiempo tarde su organización en identificar y exfiltrar a un atacante de su red, mayores serán los costes. Un informe de Ponemon Institute afirma que la detección de un ciberataque en los primeros 200 días puede ahorrar a una organización más de 1,26 millones de dólares. Lamentablemente, según el mismo informe, se tarda, por término medio, 287 días en identificar y contener un ataque. *¡287 días!* Esto significa que los atacantes a menudo pasan más de nueve meses dentro de la infraestructura de la red tramando y planificando su ataque para causar el máximo daño a la reputación y los resultados de su hospital.

Es esencial cuantificar la cantidad de tiempo que su equipo de seguridad necesita para identificar y tomar medidas contra un ataque. Consolidar los proveedores de seguridad en aquellos que ofrecen servicios gestionados y asistencia técnica en situaciones en las que aumenta el personal puede suponer un ahorro significativo de costes.

Multas normativas

Con tanta información personal valiosa a su cargo, una filtración de datos podría acarrear grandes multas por parte de los organismos reguladores. A 30 de noviembre de 2021, la Oficina de Derechos Civiles del Departamento de Salud y Servicios Humanos de EE. UU. ha establecido o impuesto sanciones contra 106 entidades cubiertas por la HIPAA por un total de más de 131 millones de dólares. Eso es una media de más de 1,2 millones por multa (además de los costes adicionales mencionados aquí).

Cómo preparar mejor a su organización sanitaria para un ciberataque

Las ciberamenazas actuales requieren que las organizaciones proveedoras cuenten con una seguridad líder en el sector. Sus pacientes y su negocio dependen de ello: el coste de la inacción es demasiado alto.

Limitaciones financieras, prioridades contrapuestas o incertidumbre en lo referente a los posibles peligros pueden empujarle a asumir demasiado riesgo. Sin embargo, sus iniciativas de seguridad deben ser exhaustivas, estratégicas, vigilantes y ágiles.

Un ecosistema que está protegido adecuadamente hoy no necesariamente estará protegido mañana. Las amenazas evolucionan rápidamente. Un día (o menos) puede bastar para que los atacantes aprovechen una nueva vulnerabilidad.

Los proveedores que desean reducir esa zona de amenaza y seguir el consejo del enfoque de copia de seguridad descrito en el aviso federal (guardar tres copias en al menos dos formatos diferentes, con uno fuera de línea), buscan cada vez más un enfoque híbrido. El almacenamiento de datos en el entorno local les proporciona un mayor control sobre la seguridad, pero puede resultar costoso y difícil de ampliar al ritmo necesario, especialmente con la explosión actual de datos sanitarios y la transformación digital en el sector de la salud, ambas impulsadas por la pandemia. El almacenamiento de datos en la nube pública es más rentable, pero las organizaciones corren el riesgo de sufrir interrupciones y de que no haya transparencia en la protección de los datos.

Un enfoque híbrido permite que los datos confidenciales se conserven en el entorno local, mientras que los menos confidenciales se almacenan en la nube. Incluso esto no es perfecto, ya que se debe establecer seguridad para proteger la transferencia de datos entre los dos tipos de almacenamiento y garantizar que el acceso se limita a aquellos que están autorizados a realizar las transferencias y ver los datos. Avanzar hacia los siete requisitos clave para implementar una arquitectura ZTNA ayuda a las instituciones a proteger sus datos, al otorgar a los usuarios acceso únicamente a las aplicaciones que necesitan para su función, con una mayor seguridad ofrecida por la MFA.

Akamai está aquí para ayudarle a prepararse para cuando se produzca un ataque, no por si se produce. Trabajemos juntos para crear una visión coherente de la red para detectar rápidamente un ataque y mitigar eficazmente los daños. Nuestra misión se centra en proteger las redes frente a ataques distribuidos de denegación de servicio y ataques de ransomware para ofrecer experiencias web seguras y fluidas (incluidas aplicaciones y API).

Reforzamos el Edge de su red para limitar las posibilidades de que se produzca una infracción, así como para reducir el radio de efecto cuando se produce una. Y lo hacemos manteniendo la flexibilidad para el acceso de los usuarios, de modo que su organización pueda centrarse en proporcionar resultados sanitarios óptimos ante las cambiantes exigencias operativas y de atención.

Proteger la información de sus pacientes de la creciente sofisticación de los ciberdelincuentes y de una superficie de ataque en expansión basada en la nube nunca ha sido tan importante. Las organizaciones y entidades gubernamentales centradas en el paciente confían en la plataforma en el Edge de Akamai para acercar las experiencias digitales a los pacientes y mantener las amenazas a raya.

Confíe en Akamai, el partner que hará que la ciberseguridad deje de ser una carga perpetua para convertirse en una ventaja competitiva de su organización.

Póngase en contacto con nosotros para obtener más información o llámenos al +1-877-425-2624.

Akamai potencia y protege la vida online. Las empresas líderes de todo el mundo eligen Akamai para crear, proteger y ofrecer sus experiencias digitales, ayudando así a millones de personas a vivir, trabajar y jugar cada día. Gracias a la mayor y más fiable plataforma en el Edge, Akamai acerca las aplicaciones, el código y las experiencias a los usuarios, y mantiene alejadas las amenazas. Obtenga más información sobre los productos y servicios de seguridad, distribución de contenido y Edge Computing de Akamai en www.akamai.com y blogs.akamai.com, o siga a Akamai Technologies en X y LinkedIn. Publicado el 22 de febrero.