SOPHOS
Cybersecurity delivered.

Prácticas recomendadas para proteger su red del ransomware

Refuerce su protección contra el ransomware y otros ataques de red

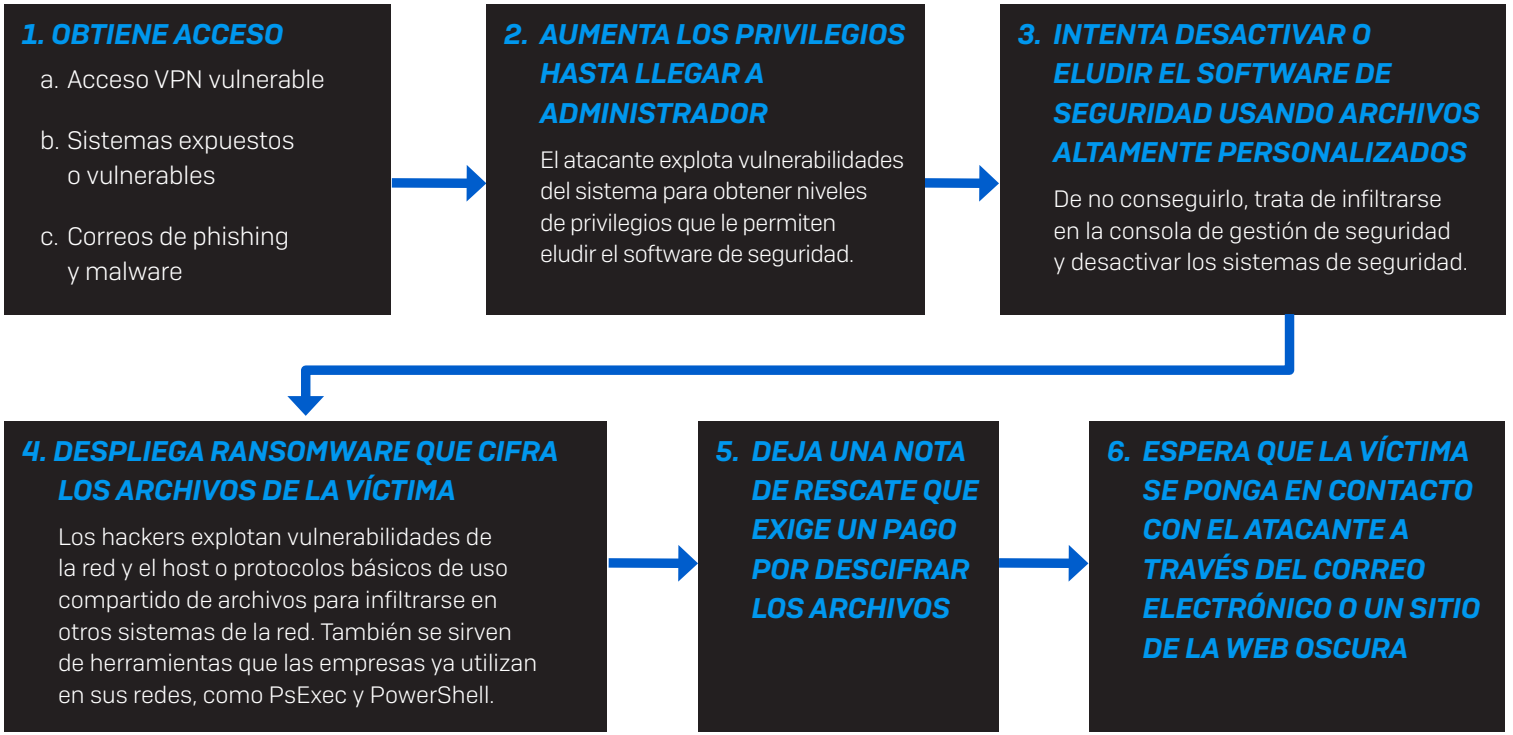
Monográficos de Sophos. Septiembre de 2022

Los ataques de ransomware están aumentando en volumen y gravedad

El 66 % de las organizaciones se vieron afectadas por el ransomware el año pasado, frente al 37 % en 2020.[1] Esto supone un aumento del 78 % con respecto al año anterior, lo que demuestra que los adversarios se han vuelto mucho más capaces de ejecutar ataques a escala que antes. El aumento del ransomware probablemente también refleje el creciente éxito del modelo de ransomware como servicio, que amplía el alcance del ransomware al requerir menos conocimientos para desplegar un ataque.

Cómo funcionan los ataques de ransomware

Para entender cómo protegerse de los ataques de ransomware, primero debemos analizar cómo funcionan. El ataque de ransomware dirigido típico funciona del siguiente modo:



Los ataques de ransomware modernos suelen utilizar herramientas legítimas de TI y de usuario final, como una VPN o el protocolo de escritorio remoto (RDP), para obtener acceso. Estas herramientas las utiliza el personal autorizado en el ejercicio de su trabajo, lo que dificulta la detección inicial de estos ataques. La raíz del problema es la excesiva confianza implícita en el uso de estas herramientas: se supone que cualquiera que pueda acceder a una VPN o al RDP es de confianza, una práctica que ha demostrado una y otra vez ser imprudente.

1 El estado del ransomware 2022, Sophos - Encuesta independiente a 5600 profesionales de TI de 31 países.

Cómo prevenir los ataques de ransomware

Hay tres medidas de seguridad de red que pueden ayudar a mitigar el riesgo de un ataque de ransomware.

1. Elimine la exposición del acceso remoto

Muchos creen que una red privada virtual (VPN) protege de los ataques de ransomware. Este mito es falso, y es que las VPN son un vector de ataque fácil de usar para los ciberdelincuentes. Por supuesto, en los últimos tiempos este vector de ataque se ha vuelto aún más atractivo debido a la enorme proliferación del uso de VPN de acceso remoto a raíz de que millones de empleados hayan pasado a teletrabajar en los últimos dos años. Los atacantes se han dado cuenta de que estas redes domésticas están mal protegidas y son vulnerables, lo que las convierte en blancos fáciles.

Uno de los ataques de ransomware de mayor repercusión en 2021 afectó a una organización estadounidense de oleoductos que vio interrumpido el suministro de combustible para la mayoría de sus clientes en las zonas este y sur de EE. UU. Durante el ataque, los ciberdelincuentes explotaron una VPN de acceso remoto.

La mayoría de los clientes VPN obsoletos también contienen vulnerabilidades que pueden ser explotadas, lo que complica aún más el reto de proteger la red de las amenazas externas. Esto ha llevado a organizaciones policiales como el FBI, el Departamento de Seguridad Nacional de los EE. UU. y la CISA (Agencia de Ciberseguridad y Seguridad de las Infraestructuras) a emitir advertencias sobre la posibilidad de ataques a la infraestructura de VPN de acceso remoto.

Práctica recomendada: sustituir la VPN de acceso remoto por ZTNA

Zero Trust Network Access (ZTNA) es el sustituto moderno de las VPN de acceso remoto. Elimina la confianza inherente y el amplio acceso que brinda la VPN, y en su lugar utiliza los principios de Zero Trust: no confiar en nada y verificarlo todo. ZTNA ofrece una mayor seguridad, una gestión más sencilla, una mejor visibilidad y una mejor experiencia de usuario en comparación con las VPN de acceso remoto.

ZTNA elimina los clientes VPN vulnerables, utiliza la autenticación multifactor (MFA) y el estado de seguridad de los dispositivos para controlar el acceso, y solo proporciona acceso a aplicaciones de red específicas, microsegmentando eficazmente su red. Es una cuestión tan importante que la Casa Blanca ha creado un mandato de arquitectura Zero Trust que todas las agencias federales deben cumplir para 2024.

Elimine la exposición a través de sistemas de escritorio remoto (RDP) y otros sistemas

Las herramientas de administración remota, como el RDP, la computación virtual en red (VNC) y otras soluciones de gestión remota, permiten al personal remoto acceder a los sistemas y administrarlos. Por desgracia, si no se aplican las medidas de seguridad adecuadas, estas herramientas también ofrecen a los atacantes la posibilidad de lanzar ataques de ransomware.

No proteger el RDP y otras soluciones de administración remota puede dejar los sistemas expuestos a ataques de ransomware. Los ciberdelincuentes utilizan a menudo herramientas de escaneado masivo y de hacking por fuerza bruta que prueban cientos de miles de combinaciones de nombres de usuario y contraseñas hasta que dan con la correcta. A veces, utilizarán esas credenciales para lanzar inmediatamente un ataque. Otras, pueden venderlas a otro grupo de delincuentes.

"Teníais una vieja vulnerabilidad Log4j crítica no parcheada en Horizon; así es como pudimos acceder en un principio. Fue un escaneado masivo, no estábamos dirigiéndonos intencionadamente contra vosotros. Ya dentro de vuestro equipo virtual de Horizon, volcamos credenciales, nos hicimos con los derechos de un administrador de dominio, descifamos el hash y logramos movernos lateralmente".

Declaraciones de unos atacantes de ransomware sobre cómo obtuvieron acceso

La cita anterior es de un grupo de ciberdelincuentes que extorsionó a una organización después de obtener acceso a sus sistemas a través de una vulnerabilidad no parcheada en VMware Horizon que descubrió gracias a un escaneado masivo. Esto subraya la importancia de mantener el firmware y el software del sistema parcheados y actualizados.

Práctica recomendada: eliminar el acceso externo directo

Proteja los sistemas remotos bloqueando todos los accesos a través de un firewall y autorizando únicamente el acceso a través de ZTNA. De este modo, se elimina la posibilidad de acceso directo desde el exterior.

Revise todas las reglas del firewall para asegurarse de que ningún sistema RDP o de administración remota esté expuesto a través de reglas de enrutamiento de puertos o NAT. Asimismo, asegúrese de que el acceso protegido está rigurosamente controlado a través de una solución ZTNA. Esta verifica que solo los usuarios y dispositivos autorizados que hayan superado las comprobaciones de identidad mediante MFA y de estado de seguridad tendrán acceso a sus sistemas.

Por otro lado, podría considerar el uso de nuevas tecnologías de autenticación segura, como Windows Hello para empresas. Y, por supuesto, mantenga su infraestructura parcheada y actualizada para evitar que viejas vulnerabilidades se conviertan en un blanco fácil.

2. Bloquee la entrada de malware y ransomware a través de phishing y descargas

Otro antiguo vector de ataque es el uso de tácticas que inducen a los usuarios a responder a correos electrónicos de phishing o a abrir mensajes maliciosos. Hoy en día, se necesitan soluciones modernas de protección para firewalls, endpoints y correo electrónico que trabajen conjuntamente con la tecnología de Machine Learning y de espacios seguros más reciente para identificar las amenazas selectivas en constante evolución que intentan acceder a la red. Lo ideal es detener estas amenazas antes de que entren en la red o aislarlas para evitar que avancen si consiguen afianzarse en ella.

Práctica recomendada: utilizar protección contra amenazas de día cero

Asegúrese de contar con la última protección de correo electrónico contra los mensajes maliciosos y de phishing para mantener estas amenazas fuera de las bandejas de entrada de los usuarios. También es aconsejable que su firewall disponga de tecnología de inspección detallada de paquetes (DPI), incluido el descifrado con TLS 1.3, para inspeccionar las cargas cifradas, análisis de Machine Learning para detectar amenazas de día cero y espacios seguros para evaluar los archivos entrantes en tiempo de ejecución. Enseñe a sus usuarios a identificar posibles amenazas de phishing. Y asegúrese de que sus endpoints tienen la mejor protección disponible contra el robo de credenciales, los exploits y el ransomware.

Para aislar las amenazas que entran en la red y limitar su capacidad de movimiento, se pueden seguir varias prácticas recomendadas, que analizaremos en la siguiente sección.

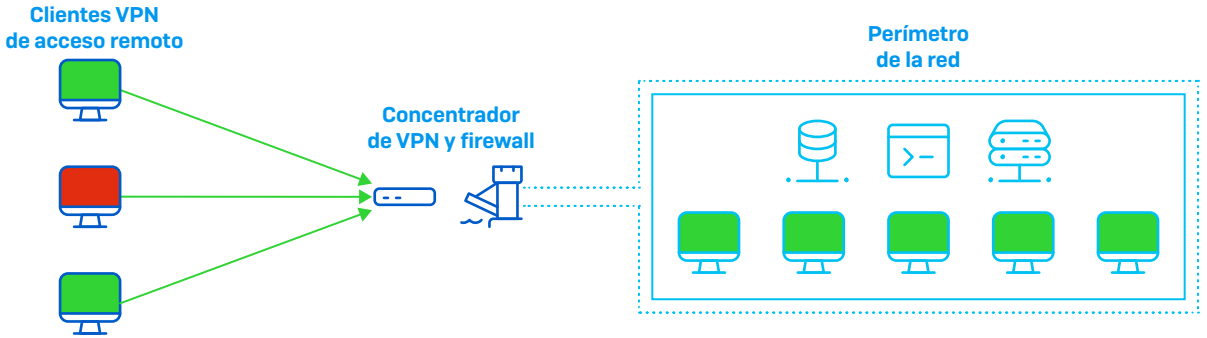
5 Manual de estrategias del adversario activo 2022 - Sophos.

Limite el movimiento lateral

Durante un ataque a la red, es absolutamente imprescindible que su solución de seguridad para redes limite su capacidad de moverse por la red o moverse lateralmente.

Por desgracia, la mayoría de las redes se asemejan a una fortificación medieval, con la proverbial muralla del castillo y el foso formando un perímetro seguro alrededor de los recursos de la red. Una VPN proporciona el equivalente a una casa del guarda para que los usuarios autorizados entren en un perímetro seguro. Pero, una vez que los ciberdelincuentes se infiltran en una red, tienen pleno acceso a todo lo que está dentro de su perímetro. Esta misma libertad de movimiento dentro de una red se aplica también a amenazas como el ransomware.

Los ciberdelincuentes utilizan el RDP y otros sistemas de gestión, así como los dispositivos no administrados, como puntos de entrada. También utilizan estos puntos de entrada para moverse lateralmente por una red.



Práctica recomendada: microsegmentar la red

Esta práctica es fundamental en las redes modernas, junto con Zero Trust. Para diseñar la red, recomendamos seguir estas tres mejores prácticas:

1. **Segmente su red.** Cree pequeñas áreas o VLAN y conéctelas mediante switches gestionados y un firewall para aplicar la protección antimalware e IPS entre segmentos. Esto le permite identificar y bloquear las amenazas que intenten propagarse lateralmente por la red.
2. **Utilice ZTNA.** Microsegmente sus aplicaciones de red y permita que solo los usuarios autorizados accedan a los recursos que necesitan. De esta manera, si un dispositivo de usuario se ve comprometido y una amenaza no es detectada, la amenaza puede eliminarse rápidamente. Sophos ZTNA va un paso más allá al eliminar completamente el acceso si un dispositivo se ve comprometido.
3. **Utilice tecnologías como la Seguridad Sincronizada de Sophos.** La Seguridad Sincronizada le permite responder automáticamente a una amenaza activa en la red, aislarla y evitar que se desplace lateralmente. Puede identificar inmediatamente una amenaza y avisar a los dispositivos con buen estado de seguridad para que ignoren cualquier tráfico procedente de un host comprometido; al mismo tiempo, los dispositivos Sophos Switch descartan automáticamente los paquetes de un dispositivo afectado y Sophos Firewall limita aún más el acceso del host comprometido a otras áreas de la red.

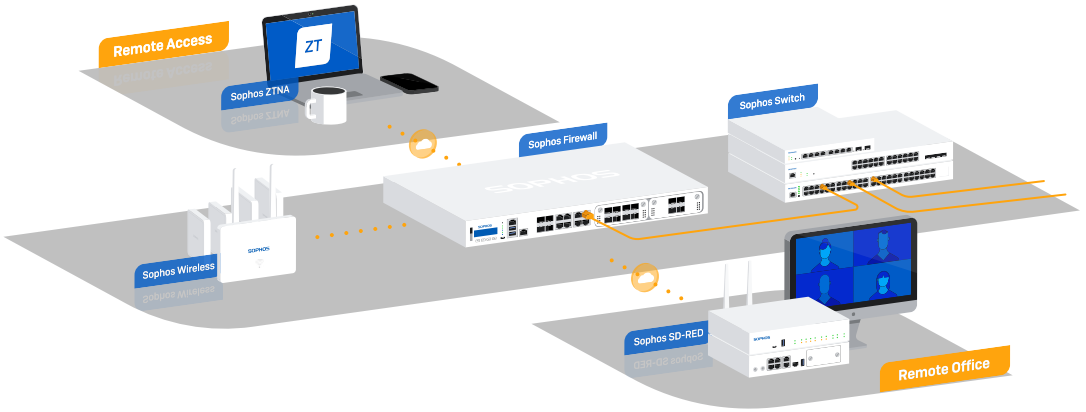
Prácticas recomendadas de la seguridad de redes para protegerse del ransomware

En resumen, estas son las prácticas recomendadas que puede utilizar para proteger su red frente al ransomware y otras ciberamenazas:

- **Microsegmente su red.** Esto permite limitar la propagación lateral de las amenazas. Utilice Sophos ZTNA para microsegmentar el acceso a sus aplicaciones de red. Use también Sophos Firewall y Sophos Switch para microsegmentar los recursos de su red interna. Además, recurra a Sophos SD-RED para segmentar y conectar de forma segura dispositivos y emplazamientos remotos.
- **Sustituya la VPN de acceso remoto por ZTNA.** Elimine un vector de ataque común eliminando clientes VPN antiguos potencialmente vulnerables. Pásese a una solución ZTNA moderna como Sophos ZTNA, que se integra con la protección para endpoints next-gen de Sophos para proteger adecuadamente los dispositivos y las identidades de sus usuarios y el acceso a sus aplicaciones y datos, además de su red, todo ello desde una única consola, con un único agente y a través de un solo proveedor.
- **Implemente la protección más sólida posible.** Recomendamos aplicar los niveles más altos de protección en sus firewalls, endpoints, servidores y dispositivos móviles, así como en el acceso remoto.
  - Asegúrese de que su firewall cuenta con inspección TLS 1.3, IPS de última generación y DPI de transmisión con Machine Learning y espacios seguros para protegerse de las amenazas de día cero más recientes. Sophos Firewall incluye todas estas tecnologías y las integra estrechamente para ofrecer una protección y un rendimiento potentes, de modo que saque el máximo partido de su inversión de firewall.
  - Asegúrese además de que sus endpoints tienen funciones modernas de protección next-gen contra el robo de credenciales, los exploits y el ransomware. Sophos es considerado sistemáticamente como el mejor proveedor de soluciones de protección para endpoints next-gen. Cubrimos sus endpoints, dispositivos móviles y servidores y le permitimos gestionarlos desde la misma consola de administración en la nube que el resto de sus productos de Sophos.
- **Reduzca el área de la superficie de ciberataque.** Revise las reglas del firewall y elimine cualquier acceso remoto o acceso al sistema RDP a través de VPN, NAT o enrutamiento de puertos. Asimismo, asegúrese de que los flujos de tráfico estén debidamente protegidos. Sophos Firewall le facilita esta tarea gracias a una visibilidad superior, paneles de control, informes y funciones de gestión de reglas.
- **Mantenga el firmware y el software parcheados y actualizados.** Esto es especialmente importante para cualquier infraestructura de red, como un firewall o software o clientes de acceso remoto, pero igual de importante para todos sus sistemas, ya que cada actualización incluye parches de seguridad esenciales para vulnerabilidades previamente identificadas. Sophos le permite mantener todos sus productos de ciberseguridad actualizados automáticamente.
- **Utilice la MFA.** Asegúrese de que se adopta un modelo Zero Trust en su red, según el cual cada usuario y dispositivo debe ganarse continuamente la confianza verificando su identidad. Además, le recomendamos que aplique una política de contraseñas seguras y que se plantee adoptar soluciones de autenticación como Windows Hello para empresas. Todos los productos de Sophos admiten la MFA con el proveedor de autenticación que prefiera.

- **Responda al instante a los ciberataques.** Utilice las tecnologías de automatización y la experiencia humana para acelerar la respuesta a los ciberincidentes y su remediación.
  - Asegúrese de que su infraestructura de seguridad de red le ayuda a responder automáticamente a los ataques activos para poder aislar un host comprometido antes de que pueda causar daños graves. Solo la Seguridad Sincronizada de Sophos puede garantizarle los niveles de respuesta que realmente necesita, justo cuando los necesita.
  - Despliegue un servicio de detección y respuesta gestionadas (MDR) como Sophos MDR. Con Sophos MDR, un equipo de expertos en amenazas supervisa y responde constantemente a los incidentes antes de que se conviertan en problemas para que no tenga que preocuparse.

Proteja su red con Sophos



Sophos ofrece todo lo que necesita para proteger íntegramente su red de los ataques, incluyendo firewalls, ZTNA, switches, redes inalámbricas, dispositivos perimetrales remotos, protección de correo electrónico, MDR y protección para endpoints next-gen para todos sus dispositivos y servidores. Y lo mejor es que todo se gestiona desde una única consola de administración en la nube, Sophos Central, con soluciones perfectamente integradas que permiten servirse de la Seguridad Sincronizada de Sophos y la detección y respuesta a amenazas entre productos o la detección y respuesta ampliadas (XDR).

La Seguridad Sincronizada garantiza que sus productos de Sophos comparten constantemente datos de telemetría y estados de seguridad para que pueda responder rápidamente a los ciberataques. Cuando se detecta un host comprometido, los endpoints con buen estado de seguridad ignoran automáticamente el tráfico, los switches descartan los paquetes del host comprometido y el firewall bloquea el acceso a otras áreas de la red hasta que se resuelva el problema. Ningún otro sistema de seguridad puede ofrecer esto: con Sophos, la ciberseguridad es más sencilla y eficaz.

Sophos XDR es la única solución XDR del sector que sincroniza la seguridad nativa de firewalls, endpoints, servidores, correo electrónico, la nube y Microsoft 365 para ofrecerle una visión integral del entorno de su organización. Ofrece información completa y análisis en profundidad para la detección, investigación y respuesta a las amenazas, tanto para los equipos de los centros de operaciones de seguridad dedicados como para los administradores de TI.

Si le parece que la ciberseguridad es demasiado compleja y cambia demasiado rápido como para gestionarla eficazmente por su cuenta, tenemos la solución para usted. Sophos MDR protege más de 11 000 organizaciones de todo el mundo, con búsqueda y neutralización de amenazas 24/7 a cargo de un equipo global de expertos en amenazas.

En definitiva, Sophos ofrece una cartera de productos y servicios de ciberseguridad que le permiten proteger fácilmente su red contra el ransomware.

Descubra cómo Sophos puede proteger su red en es.sophos.com

Sophos ofrece soluciones de ciberseguridad líderes en el sector a empresas de todos los tamaños, protegiéndolas en tiempo real de amenazas avanzadas como el malware, el ransomware y el phishing. Gracias a nuestras funcionalidades next-gen probadas, los datos de su organización estarán protegidos de forma eficiente por productos con tecnologías de inteligencia artificial y Machine Learning.

2022-09-12 ES-WP (DD)

SOPHOS