Las cadenas de suministro, en el punto de mira: cinco medidas para protegerse del próximo gran ciberataque

Quien crea que el de SolarWinds será el último ataque de este tipo está muy equivocado

En menos de un año, organizaciones de todos los rincones del mundo han sido víctimas de varios ataques muy sonados, como los exploits de Microsoft Exchange Server y los ataques de ransomware contra Kaseya VSA, entre muchos otros. Ahora que el precio de las criptomonedas se ha disparado, atacantes como REvil (implicado en el ataque a Kaseya VSA) están decididos a lanzar campañas de ransomware que extienden sus ataques e infecciones a más objetivos secundarios. La interminable cadena de ciberataques que protagonizan los titulares de las noticias día tras día sugiere que, más temprano que tarde, las organizaciones van a tener que hacer todo lo que esté en sus manos para salvaguardar sus redes.

Este informe ofrece recomendaciones y consejos para ayudar a reducir las vulnerabilidades y la exposición a las amenazas en el seno de los entornos empresariales, al tiempo que se protegen las cadenas de suministro adyacentes.

Introducción

Como resultado de las transformaciones digitales, hemos sido testigos de cómo las empresas han engarzado su cadena de suministro a base de proveedores de tecnología y software con el fin, por un lado, de aumentar la productividad y, por otro, de poner las tecnologías emergentes al servicio del crecimiento y la eficiencia a gran escala. Aprovechándose de la confianza que las empresas depositan en sus proveedores y distribuidores de software —que tienen acceso a la red corporativa—, cada vez es más frecuente que los hackers ataquen las cadenas de suministro. Con este acceso, los ataques pueden incluso irrumpir en el proceso de firma de los certificados digitales de un proveedor dado para eludir las defensas de la víctima.

A la amenaza de un ataque a la cadena de suministro de software se suman los retos a los que tienen que enfrentarse hoy en día los equipos de seguridad, que incluyen un incesante goteo de alertas de seguridad sin ninguna conexión entre sí y que carecen del contexto necesario para decidir qué medidas tomar. Resulta fundamental que las empresas adopten herramientas de detección y respuesta con aprendizaje automático integrado que les permitan detectar cualquier comportamiento malicioso, aunque proceda de proveedores aprobados o de confianza.

Además, implementar un marco Zero Trust (confianza cero) para redefinir la arquitectura de red de la organización puede ser de gran ayuda a la hora de migrar desde un modelo de seguridad tradicional basado en el perímetro a otro basado en la verificación continua de la confianza.

La habilidad prodigiosa de la que hacen alarde los atacantes obliga al sector a replantearse varias cuestiones

En marzo de 2020, SolarWinds envió a sus 33 000 clientes de Orion® una actualización de software rutinaria que contenía, sin que nadie lo supiera, código hackeado. Unos 18 000 de ellos lo instalaron, lo cual causó un efecto dominó que terminó afectando a una gran cantidad de entidades estadounidenses públicas y privadas, como varias secciones del Pentágono, el Departamento de Estado, el de Energía, el de Seguridad Nacional y el del Tesoro, la Administración Nacional de Seguridad Nuclear y varios proveedores de soluciones de ciberseguridad. Ni que decir tiene que aún se van conociendo más repercusiones a medida que las empresas y los sectores federales siguen valorando los daños.

Estos ataques recientes que se aprovecharon de SolarWinds pusieron en evidencia la magnitud que puede llegar a tener un ataque sofisticado a la cadena de suministro. Las organizaciones dependen en gran medida del software y los servidores de SolarWinds para gestionar sus redes, sistemas e infraestructura de TI, y esto dio a los atacantes un nivel de acceso sin precedentes. Todo indica que el ataque pasó desapercibido durante diez meses aproximadamente.

SolarWinds anunció que un adversario había conseguido integrar código malicioso en una de sus actualizaciones de software con la correspondiente firma. Una vez que se aplicó la actualización, el código malicioso fue extraordinariamente sigiloso. En este ataque, el malware, conocido como SUNBURST, permaneció inactivo unas dos semanas para, después, contactar con un subdominio de avsvmcloud[.]com —el servidor de comando y control para la puerta trasera— y recibir más instrucciones y cargas que ejecutar. Algunas de las mayores y más innovadoras empresas y agencias gubernamentales de Estados Unidos identificaron SUNBURST en sus servidores de producción, cuando los datos confidenciales ya estaban en peligro y habían quedado expuestos.

Llama la atención que el atacante pudiera permanecer en la infraestructura durante tanto tiempo y acceder a los sistemas de terceras organizaciones sin que el tráfico diera señales de sospecha, pero hay que decir que los 72 proveedores de soluciones de detección de malware categorizaron el dominio avsvmcloud[.]com como benigno.

Dada la importancia de SolarWinds para la automatización, se aprovecharon del posicionamiento estratégico y la conectividad de la solución para acceder a casi todos los demás componentes del entorno de los clientes y utilizaron la infraestructura y los certificados SAML atacados para moverse lateralmente y acceder a los datos confidenciales del correo electrónico. Un método de detección de eficacia probada se basaba en las desviaciones del comportamiento o las técnicas comúnmente empleadas en los kits de exploit y malware, que es justo lo que hacía Cortex XDR.

«Hace poco, vimos un intento de descargar Cobalt Strike en uno de nuestros servidores SolarWinds. Cortex XDR lo bloqueó enseguida con su función de protección contra amenazas basada en el comportamiento, y el centro de operaciones de seguridad aisló el servidor, investigó el incidente y protegió la infraestructura. Otra de las medidas que tomamos a consecuencia de este incidente fue implementar varios indicadores de riesgo en los productos de Palo Alto Networks destinados a nuestros clientes».

Nikesh Arora, director ejecutivo de Palo Alto Networks

El 17 de diciembre de 2020, el director ejecutivo de Palo Alto Networks, Nikesh Arora, desveló que su implementación interna de Cortex XDR había bloqueado una solicitud de DNS de uno de sus servidores SolarWinds Orion gracias al motor de protección contra amenazas basada en el comportamiento de Cortex XDR, lo que permitió al equipo del centro de operaciones de seguridad de Palo Alto Networks aislar el servidor y poner en marcha una investigación. Concluyeron que, gracias a Cortex XDR, el ataque no logró su objetivo, no se puso ningún dato en riesgo y la infraestructura siguió estando protegida.

Lo que les permitió detener este ataque sin precedentes fue, precisamente, esta integración crucial de las funciones de prevención, detección y respuesta a amenazas, unida al uso que hace Cortex XDR del aprendizaje automático y la inteligencia artificial para integrar automáticamente los datos del endpoint, la red y la nube.

Los ataques a la cadena de suministro siguen aumentando en términos de volumen y escala, y la ciberseguridad acaba de entrar de lleno en una nueva etapa poblada de adversarios estatales que, además de estar muy bien financiados, son muy disciplinados y tienen muy claro su objetivo: acceder a los entornos de sus víctimas, establecerse durante un tiempo y atacar con distintas finalidades (por ejemplo, para robar datos). Para frustrar estos tipos de campañas sofisticadas, habrá que echar mano de nuevas metodologías y tecnologías que permitan anticiparse a los adversarios, quienes están decididos a lanzar ataques aún más avanzados cada día que pasa gracias, en parte, a que la escala de la nube y la automatización abren la posibilidad de perpetrar ataques frente a los cuales la tecnología y las prácticas de gestión de riesgos obsoletas no tienen nada que hacer.

Cómo prepararse para el próximo ataque tipo SolarWinds: las empresas deben tomar medidas de inmediato

Es importante apuntar que, incluso antes de que se produjera este ataque, ya estaba claro que un buen porcentaje de los centros de operaciones de seguridad dependen demasiado de la intervención humana y del uso de varios productos de seguridad independientes entre sí. Ya entonces, los analistas trabajaban bajo mucha presión tratando de tener controladas todas las alertas generadas por la multitud de productos que tenían implementados. Muchos siguen confiando en la revisión manual de las decenas de miles de alertas que, cada semana, les llueven de docenas de productos de seguridad distintos y que muestran indicios de actividad sospechosa. Las prácticas manuales de investigación y respuesta suelen requerir una cantidad de tiempo excesiva para recopilar contexto (qué se sabe del endpoint, el usuario y el tiempo que llevan desarrollándose las actividades sospechosas) y analizar el incidente (qué otros eventos están relacionados con el nombre de host y la dirección IP, el tráfico, el dominio, la aplicación que se está utilizando, etc.). Todo esto da lugar a evaluaciones incompletas y a un sistema de seguridad ineficaz.

Según una encuesta realizada en 2019 a una serie de directores de seguridad de la información, «más del 41 % recibe más de 10 000 alertas al día y algunos incluso aseguran que se superan las 500 000».

Esta misma encuesta señalaba que solo el 24 % de las alertas investigadas se consideraban legítimas, mientras que un año antes la cifra ascendía al 34 %. También disminuyó de forma considerable la cantidad de alertas legítimas que se solucionaban: del 51 % en 2018 al 43 % en 2019.[1]

Y, por si no fuera suficiente, muchas organizaciones siguen empleando soluciones de seguridad obsoletas (antivirus, herramientas de detección y respuesta en el endpoint y otras tecnologías de seguridad), por lo que los riesgos son aún mayores. Además, los analistas reciben tantos datos de mala calidad que, muchas veces, terminan desajustando los sensores o, directamente, haciendo caso omiso de algunas alertas, lo que también aumenta el nivel de riesgo. A falta de contexto, muchas alertas quedan descartadas como falsos positivos porque no justifican una investigación. Sin embargo, si se contextualizan y se analizan en más profundidad con otras fuentes de datos, estos pueden resultar clave para entender actividades en apariencia benignas que, en realidad, son muy peligrosas.

Para garantizar la eficiencia de las operaciones de seguridad en el futuro, es preciso sustituir las herramientas de seguridad obsoletas y fragmentadas por otras que se integren bien y ofrezcan funciones avanzadas de análisis, aprendizaje automático y detección automatizada que permitan acelerar la respuesta y, al mismo tiempo, mejoren la precisión. Cuando se integran las herramientas adecuadas con los datos pertinentes —previamente consolidados—, las organizaciones pueden reducir los tiempos de respuesta y obtener una visión global de todos los incidentes que les permita documentar mejor las investigaciones.

Teniendo en cuenta todo esto, ¿en qué dirección debemos avanzar? ¿Cómo pueden prepararse las empresas y las organizaciones para enfrentarse, no ya al próximo ataque a la cadena de suministro, sino a todas las demás amenazas que están por llegar y que no dejan de evolucionar?

Lea las siguientes cinco medidas para descubrir cómo puede contribuir cada una de ellas a mejorar las actividades relativas a la seguridad, ya sea la evaluación de riesgos cibernéticos o la elaboración de una estrategia de operaciones de seguridad más completa.

1. *Anticipating the Unknowns* (disponible en inglés), Cisco, marzo de 2019, https://ebooks.cisco.com/story/anticipating-unknowns/page/6/6.

1. Conozca su superficie de ataque

Ahora que los empleados, socios y proveedores trabajan fuera del perímetro de la red de la empresa, el riesgo de que los sistemas internos y los datos de las organizaciones queden expuestos y sufran un ataque es mayor que nunca. Algunas posibles soluciones consistirían en realizar pruebas de penetración, buscar vulnerabilidades y utilizar una tecnología emergente conocida como «gestión de la superficie de ataque».

¿Qué es la gestión de la superficie de ataque (ASM)?

Según la definición del SANS Technology Institute, la gestión de la superficie de ataque (ASM, por sus siglas en inglés) es:

> «Una categoría de soluciones emergente que se propone ayudar a las organizaciones a afrontar este reto proporcionando un punto de vista externo de la superficie de ataque de una organización, que está formada por todos los activos de hardware, software, software como servicio y en la nube a los que se puede acceder a través de Internet y que puede detectar un atacante. En pocas palabras, la superficie de ataque es cualquier activo externo que pueda detectar, atacar y utilizar un ciberdelincuente para infiltrarse en el entorno».[2]

SANS enumera una serie de casos de uso habituales para la adopción de una solución ASM, entre los que se encuentran los siguientes:

- Identificación de lagunas externas en la visibilidad
- Detección de activos desconocidos y de casos de informática en la sombra
- Gestión de riesgos en la superficie de ataque
- Priorización de vulnerabilidades según el riesgo
- Evaluación del riesgo de las filiales y el derivado de las fusiones y adquisiciones

Independientemente de que se decida implementar soluciones ASM o llevar a cabo pruebas de penetración o búsqueda de vulnerabilidades, lo que está claro es que hay que identificar los requisitos tanto en lo que se refiere a los productos como a las operaciones, para determinar cuál es la mejor opción según criterios de funcionalidad, prestaciones, capacidad y evaluación.

2. Prevenga todos los peligros que pueda

Aunque en el mercado abundan las soluciones de seguridad, se siguen produciendo ciberataques y su nivel de sofisticación —tanto en términos de complejidad como de financiación— es cada vez mayor.

Dicho esto, se ha constatado que muchos de los ataques más destacados utilizan vectores de ataque bastante recurrentes, como el malware integrado, los correos electrónicos de *phishing* y la escalada de privilegios. Por todo ello, conviene utilizar la tecnología y seguir las prácticas recomendadas para prevenir todo tipo de ataques y poder centrarse en lo importante.

Medidas de prevención básicas

- **Invierta en proteger los endpoints. Las plataformas de protección del endpoint (EPP, por sus siglas en inglés) emplean diversas técnicas de prevención, como análisis estáticos para detectar malware basándose en la inspección de archivos, reglas heurísticas para bloquear los exploits y análisis del comportamiento para evaluar cuán maliciosos son los archivos según las funciones que ejecuten.**
- **Con independencia del tipo de entorno en el que trabaje (desarrollo, control de calidad o producción), asegúrese de tener una solución de seguridad integrada que siempre le permita enviar datos sobre vulnerabilidades a las herramientas que ya utiliza, como rastreadores de errores para la aplicación rápida de correcciones.**
- **Utilice contraseñas complejas. Su seguridad se verá reforzada solo con que su contraseña tenga al menos diez caracteres. Aunque el sistema no se lo pida, cambie la contraseña dos o tres veces al año.**
- **Procure que el software esté siempre actualizado. Instale las actualizaciones de seguridad conforme vayan estando disponibles.**
- **Restrinja el acceso de la red a los hosts y las redes de confianza. Permita acceder a Internet únicamente a los servicios de red que lo necesiten. A menos que sea absolutamente necesario, no implemente sistemas a los que se pueda acceder directamente desde Internet. Si se necesita habilitar el acceso remoto, utilice un método de acceso seguro, como las redes privadas virtuales (VPN, por sus siglas en inglés) o el protocolo SSH.**
- **Prevenga el *phishing* y otras infecciones que se transmiten a través del correo electrónico formando a los empleados en las prácticas recomendadas y políticas más recientes, como el borrado de archivos adjuntos sospechosos.**
- **Utilice la autenticación multifactor (MFA, por sus siglas en inglés) siempre que sea posible.**
- **Configure los filtros de correo no deseado para optimizar su cobertura.**

2. Pierre Lidome, *The SANS Guide to Evaluating Attack Surface Management* (disponible en inglés), SANS Institute, 26 de octubre de 2020, https://www.sans.org/reading-room/whitepapers/analyst/guide-evaluating-attack-surface-management-39905.

Muchas brechas se producen debido a una combinación de errores humanos, sistemas sin actualizar y la gran persistencia de atacantes modernos que utilizan la transformación digital en su propio beneficio.

Siga las siguientes recomendaciones si sospecha que ha sido víctima de un ataque:

- Si solo se han infectado unos cuantos sistemas, desconéctelos (físicamente) de su red interna de inmediato para contener la infección y evitar que se propague. Si no puede hacerlo con prontitud o el número de sistemas infectados es mayor, y no tiene implementado ningún servidor proxy ni un sistema avanzado de filtrado de los datos de salida del cortafuegos, bloquee de inmediato TODO el tráfico saliente a las redes externas.
- Implemente filtros en los enrutadores, cortafuegos y demás dispositivos de red internos pertinentes para aislar los segmentos infectados y supervisar el tráfico de red. Así, se asegurará de contener la infección o, cuando menos, podrá identificar cómo se está propagando y a qué hosts ha alcanzado ya.
- Supervise todo el tráfico de la red para bloquear posibles ataques polifacéticos.
- Revise los archivos de log pertinentes para intentar identificar qué sistema fue el primero en infectarse y, si es posible, cuál fue el vector de ataque.
- Resulta fundamental determinar si alguno de los sistemas infectados consiguió conectarse a algún sitio de Internet y, dado el caso, qué información quedó expuesta.

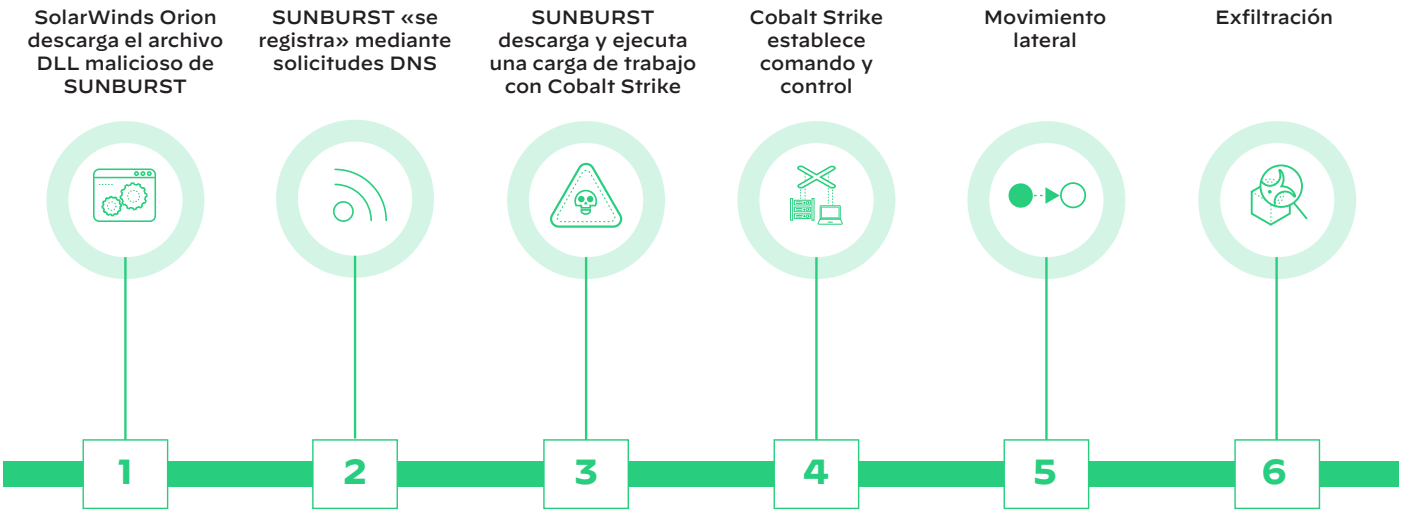

Figura 1: Cortex XDR bloqueó el ataque de SolarStorm durante la tercera fase

Con Cortex XDR, se ahorra el tiempo y el coste de crear su propia infraestructura general de seguridad del endpoint. Esta implementación simplificada, que no requiere licencias de servidor, bases de datos ni ninguna otra infraestructura para empezar a funcionar, permite a las organizaciones proteger sus endpoints sin demora.

3. Obtenga la máxima visibilidad

La visibilidad empresarial, con una estrategia de datos unificada que abarque toda la cadena de suministro, puede proporcionar una visión de conjunto de todas las aplicaciones y de la infraestructura. La visibilidad también puede incluir los datos de telemetría procedentes de los endpoints, las redes y los entornos en la nube. Además, debe establecer correlaciones entre esas fuentes de datos para entender cómo están relacionados los distintos eventos y si, por contexto, un comportamiento es o no sospechoso.

Los datos de telemetría y la investigación forense, combinados con el aprendizaje automático, pueden ofrecer una fotografía nítida de una cadena de ataque dada para analizarla en profundidad durante la fase de clasificación y verificación de una alerta, lo que simplifica y agiliza la investigación y la respuesta.

En el caso concreto del ataque a SolarWinds, aunque el software del proveedor ya contenía código malicioso no autorizado, Cortex XDR de Palo Alto Networks fue capaz de bloquear un intento de descarga de Cobalt Strike en uno de sus servidores SolarWinds gracias al motor de protección contra amenazas basada en el comportamiento (véase la figura 1).

Por tanto, en este tipo de ataques avanzados, contar con plena visibilidad puede ayudar a las organizaciones a detectar y detener cualquier fase del ciclo de vida de un ataque (aunque el host ya se haya visto afectado). Si un ataque es tan avanzado que consigue eludir sus medidas preventivas, tendrá que contar con un sistema capaz de detectar la actividad posterior a la intrusión que el atacante necesita desarrollar para alcanzar sus objetivos.

4. Tome medidas cuanto antes

Si bien los hackers consiguieron entrar en el sistema de SolarWinds allá por enero de 2019, parece ser que el acceso a su infraestructura ya se vendía en la *dark web* a fecha de 13 de octubre de 2017 —concretamente en el foro de ciberdelincuencia Exploit—, lo que viene a corroborar que existe un incentivo económico en el lanzamiento de campañas de amenazas avanzadas persistentes (APT, por sus siglas en inglés).

Para marzo de 2021, tanto Microsoft como FireEye ya habían informado de la presencia de nuevos indicadores de riesgo que incluían implantes de puerta trasera y de malware para establecer acceso continuo a las redes afectadas. Según el propio gigante tecnológico:

> «Microsoft detectó estas nuevas herramientas y funciones de ataque en ciertas redes de clientes atacadas y constató que se habían estado utilizando entre agosto y septiembre de 2020. Los análisis posteriores apuntaron a que podían haber estado presentes en los equipos atacados desde bastante antes (concretamente, junio de 2020). Estas herramientas son nuevos componentes de malware que solo utiliza este actor. Están pensadas específicamente para ciertos tipos de redes y se cree que se introducen después de que el atacante haya conseguido acceder mediante el uso de credenciales robadas o del binario de SolarWinds y después de moverse lateralmente con TEARDROP y de otras actividades *hands-on keyboard* (intrusiones en que los ciberdelincuentes exploran los sistemas atacados ellos mismos, sin esperar a que la máquina lo haga de forma automatizada)».[3]

Una vez que un atacante ha conseguido entrar, el éxito de una campaña dependerá de su capacidad de evadir la detección inicial y ser persistente. SolarStorm, el atacante responsable de la brecha de SolarWinds, utilizó credenciales robadas para acceder a los servicios en la nube y explotar las identidades atacadas para obtener y conservar el acceso a las redes a través de VPN y herramientas de acceso remoto.

De ahí que reducir el tiempo de permanencia (o el tiempo que transcurre hasta que se descubre la brecha) y el consiguiente movimiento lateral resulte indispensable para contener un ataque, eliminarlo y recuperarse de él. Las consecuencias van más allá de posibles daños a la reputación de la organización, multas por infringir la normativa y pérdidas de datos cruciales para la empresa: cuanto más se tarde en detectar y contener una brecha, mayor será su impacto económico.

En su informe *Quantifying the Value of Time in Cyber-Threat Detection and Response*, Aberdeen Group apuntaba que, si el tiempo de permanencia se limita a siete días, el impacto es un 77 % inferior y, si se acorta a un solo día, el impacto puede llegar a reducirse en un 96 % (véase la figura 2).[4]

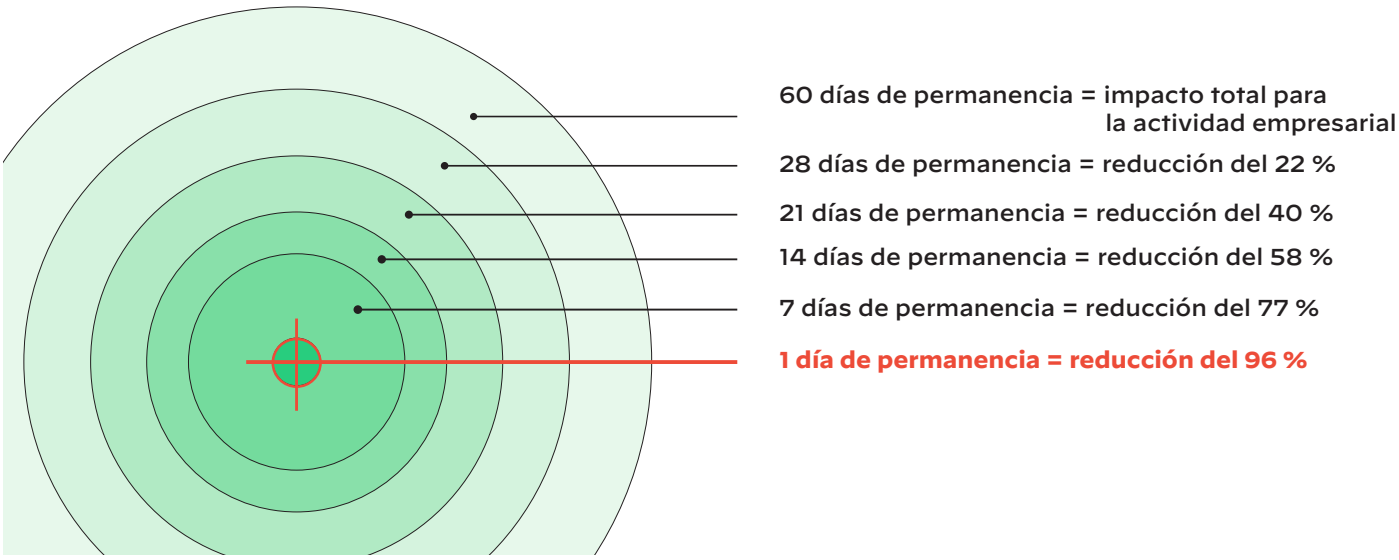

Figura 2: *Quantifying the Value of Time in Cyber-Threat Detection and Response* (disponible en inglés), Aberdeen Group, febrero de 2016

3. Ramin Nafisi et al., *GoldMax, GoldFinger, and Sibot: Analyzing NOBELIUM's Layered Persistence* (disponible en inglés), 4 de marzo de 2021, https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/4.
4. Aberdeen Group, *Quantifying the Value of Time in Cyber-Threat Detection and Response* (disponible en inglés), febrero de 2016.

Más allá de la importancia de responder a los ataques de inmediato, hay que considerar la rapidez y frecuencia con que los adversarios analizan y localizan posibles vectores de amenaza. Los avances en las tecnologías de análisis permiten a los ciberdelincuentes encontrar vectores de ataque fácil y rápidamente, pues revelan activos abandonados, irregulares o mal configurados que pueden convertirse en la puerta trasera necesaria para lanzar el ataque.

En su *Informe de Cortex Xpanse sobre amenazas a la superficie de ataque (2021): conclusiones de las principales multinacionales sobre la gestión de la superficie de ataque*, Palo Alto Networks detalla las conclusiones clave de su estudio sobre las superficies de ataque públicas de algunas de las empresas más grandes del mundo. Entre enero y marzo, el equipo supervisó los análisis de 50 millones de direcciones IP asociadas con 50 multinacionales con el objetivo de conocer la rapidez con la que los atacantes pueden identificar sistemas vulnerables que explotar.

Estas son algunas de las conclusiones más interesantes del informe:

- **Los ciberdelincuentes no descansan**. Como el perro y el gato: los atacantes realizan un análisis nuevo cada hora, cosa que a las multinacionales puede llevarles semanas.
- **Los ciberdelincuentes no dejan escapar las nuevas vulnerabilidades**. Los atacantes no tardaron ni 15 minutos en realizar sus análisis desde que se anunciaron vulnerabilidades y exposiciones comunes (CVE, por sus siglas en inglés) entre enero y marzo, y no esperaron ni cinco minutos desde la actualización de seguridad de día cero de Microsoft Exchange Server.
- **Lo que más preocupa es la seguridad de la nube**. El 79 % de los problemas de seguridad más graves detectados en las multinacionales se encontraban en los ecosistemas en la nube, y solo un 21 % en los entornos locales, lo cual subraya una vez más el riesgo inherente de los servicios alojados en la nube.

MTTD (tiempo medio de detección): cantidad de tiempo que tarda una empresa en identificar un posible incidente de seguridad.

MTTF (tiempo medio hasta el fallo): tiempo durante el cual un sistema defectuoso puede ejecutarse hasta dejar de funcionar.

MTTR (tiempo medio de respuesta): tiempo que tarda un equipo en controlar, corregir o eliminar una amenaza tras haberla identificado.

MTBF (tiempo medio entre fallos): refleja la fiabilidad y disponibilidad de un sistema. Sirve para evaluar el rendimiento del sistema bajo unas condiciones predeterminadas durante un período de tiempo dado.

5. Apueste por el modelo Zero Trust

Aunque ya llevamos un tiempo hablando del concepto de «Zero Trust» (confianza cero), no acabó de asentarse hasta 2009, cuando Forrester Research formalizó el «Modelo Zero Trust (confianza cero)» de la ciberseguridad.[5] En resumidas cuentas, se trata tanto de un modelo arquitectónico para redes como de un marco para establecer políticas de seguridad.

Zero Trust confía en la verificación y validación estrictas de cada persona, dispositivo o entidad que intente acceder a los recursos de la red. El objetivo primordial es evitar que se produzcan brechas y proteger los datos, las aplicaciones y los sistemas empresariales críticos de ataques y exploits.

Los principios del modelo Zero Trust están diseñados para reducir la exposición y el acceso no autorizado en todo el espectro de amenazas. Se han desarrollado cuidadosamente para cubrir la seguridad de las aplicaciones críticas y los datos confidenciales de una organización empresarial dada. Estos principios pueden integrarse fácilmente en cualquier estrategia de seguridad y entre ellos se incluyen los siguientes:

- **Política del mínimo privilegio (PoLP, por sus siglas en inglés):** una política según la cual los usuarios finales reciben la cantidad mínima de acceso que necesitan para llevar a cabo su trabajo. Esto ayuda a reducir las probabilidades de exposición al malware, las vías de entrada de los atacantes y el riesgo de exfiltraciones de datos.
- **Microsegmentación:** en los centros de datos e implementaciones en la nube que requieren distintas credenciales de acceso, las redes se dividen en segmentos independientes o «zonas seguras» para ayudar a aislar las cargas de trabajo. Esto permite, además, limitar el movimiento lateral (o en dirección este-oeste) en las redes internas en caso de brecha.
- **Autenticación multifactor:** un protocolo de seguridad que obliga a que las personas se autentiquen con más de un procedimiento de seguridad. Normalmente, es una combinación de cosas que uno sabe (p. ej., contraseñas o claves PIN), cosas que uno tiene (una llave electrónica, una tarjeta de identificación, etc.) y marcadores físicos (algún dato biométrico, la voz o la huella dactilar).

5. John Kindervag et al., *No More Chewy Centers: The Zero Trust Model of Information Security* (disponible en inglés), 23 de marzo de 2016, https://www.forrester.com/report/No+More+Chewy+Centers+The+Zero+Trust+Model+Of+Information+Security/-/E-RES56682?objectid=RES56682.

Estos son algunos de los pasos que se recomienda seguir para que las funciones Zero Trust (confianza cero) alcancen un buen nivel de madurez:

- Supervisar toda la actividad y recopilar todos los datos, no solo los eventos que resulten sospechosos.
- Detectar el comportamiento anómalo con los análisis y el aprendizaje automático.
- Detectar y bloquear el comportamiento malicioso en el endpoint.
- Segmentar el acceso con el cortafuegos del host.
- Supervisar y restringir el acceso a dispositivos USB no autorizados mediante el control de dispositivos. Los usuarios no pueden conectar ningún dispositivo a la máquina, excepto cuando el uso y el dispositivo estén autorizados y durante un tiempo limitado.
- Bloquear los hosts remotos maliciosos.
- Orquestar los controles de seguridad. La automatización y la orquestación pueden ayudar a identificar lagunas en las arquitecturas Zero Trust (confianza cero) y resolverlas automáticamente o activar flujos de trabajo que ayuden a los analistas a corregirlas. Tal y como recomienda el informe de Forrester *The Zero Trust eXtended (ZTX) Ecosystem* (disponible en inglés), «evite las soluciones que funcionan de manera aislada y opte por aquellas que se integran para dar lugar a un ecosistema que favorezca la visibilidad y el control en todo el ecosistema y refuerce la orquestación de los mecanismos de defensa».

A continuación encontrará más información para ayudarle a diseñar su estrategia Zero Trust (toda ella disponible en inglés):

- Instituto Nacional de Normas y Tecnología estadounidense: *Zero Trust Architecture: NIST Publishes SP 800-207*
- Centro Nacional de Ciberseguridad estadounidense: *Zero Trust principles - beta release*
- Organismo Nacional de Seguridad estadounidense: *Embracing a Zero Trust Security Model*
- Forrester Research: *Five Steps To A Zero Trust Network**, donde recomiendan lo siguiente para implementar una estrategia Zero Trust (confianza cero) eficaz:

1. Identificar los datos confidenciales.
2. Trazar un mapa de los flujos de datos confidenciales.
3. Diseñar un microperímetro Zero Trust.
4. Supervisar el entorno Zero Trust en detalle con análisis de seguridad.
5. Automatizar y orquestar la seguridad.

** El informe está a disposición de los suscriptores de Forrester y también es posible comprarlo.*

Un arma no tan secreta: Cortex XDR

Afortunadamente, existe una forma eficiente de aplicar todos esos principios a cualquier estrategia de seguridad. Las plataformas modernas de detección y respuesta ampliadas (XDR, por sus siglas en inglés) recopilan y correlacionan los datos procedentes de múltiples fuentes —red, endpoint, servidor y cargas de trabajo en la nube— de manera automática para detectar antes las amenazas y que los analistas tarden menos en investigarlas y responder a ellas.

Cortex® XDR™ de Palo Alto Networks es la primera plataforma de detección y respuesta ampliadas del sector que integra de forma nativa los datos de los endpoints, la red y la nube para detener amenazas sofisticadas, lo que permite al usuario eliminar las amenazas de la red, el endpoint y la nube al instante desde una única consola.

Cortex XDR es la única solución con la que los equipos de seguridad pueden hacer todo esto:

- **Detectar automáticamente ataques sigilosos** en todo tipo de vectores de amenaza, gracias al análisis del comportamiento de los datos de la red, el endpoint y la nube. La misión de la tecnología principal de Cortex XDR es aprender el comportamiento de cada dispositivo y usuario para compararlo con el de otros dispositivos y usuarios de la red de la organización en cuestión. A continuación, utiliza estos perfiles de comportamiento para detectar desviaciones con respecto al comportamiento anterior, al de sus homólogos o al que se espera de esa entidad.
- **Acortar las investigaciones** relacionando los datos de telemetría de seguridad, por una parte, y las alertas de cada endpoint y demás fuentes de datos, por la otra, y dándoles sentido para mostrarlos como un solo incidente que revele la causa principal. La visibilidad de todas las fuentes de datos permite eliminar los ángulos muertos de la seguridad, mejora la precisión de la detección identificando los ataques sofisticados que se producen en las distintas capas de datos y proporciona contexto adicional para simplificar las investigaciones. Además, al consolidar los datos, se reduce el número de productos de detección y respuesta que tienen que gestionar los clientes.
- **Adaptar los mecanismos de defensa continuamente** mediante la aplicación del conocimiento obtenido a partir de las investigaciones con el objetivo de prevenir futuras amenazas. Sus analistas pueden detener rápidamente la propagación del malware, aislar los endpoints, analizarlos todos para eliminar el malware en tiempo real e incluso acceder a ellos directamente e investigar las amenazas sin que los usuarios lo noten siquiera.

Conclusión

Los ataques como el que sufrió SolarWinds representan una llamada de atención a los distintos profesionales de la ciberseguridad de todos los sectores, que no pueden bajar la guardia a la hora de proteger sus redes de las amenazas persistentes y sofisticadas. Aunque el sector se esté tomando una especie de «respiro» colectivo mientras se llevan a cabo las correspondientes evaluaciones a posteriori y se reparan los daños que ha dejado tras de sí el ataque a SolarWinds, las organizaciones tienen que darse cuenta de que reforzar sus sistemas de seguridad es algo que no puede esperar, porque el próximo gran ataque podría producirse mañana mismo.

Los atacantes siempre están ideando técnicas que desafían los límites de lo posible y buscando nuevas formas de lanzar campañas discretas sin que nadie se entere ni les impida ocasionar el mayor daño posible.

Es el momento de recurrir al sinfín de soluciones de seguridad y prácticas recomendadas modernas que le ayudarán a reforzar su estrategia de seguridad. Se pueden tomar medidas de forma gradual para garantizar que los equipos de seguridad avancen por el buen camino, empezando por visibilizar la superficie de ataque, prevenir lo más posible y aplicar los principios Zero Trust (confianza cero).

Seguramente lo ideal sea considerar la opción de adoptar soluciones de nueva generación como la tecnología XDR, que son la evolución lógica de otras herramientas de eficacia demostrada como las de detección y respuesta en el endpoint (EDR, por sus siglas en inglés). La tecnología XDR ofrece la visibilidad y el control necesarios de los componentes adyacentes a la empresa mediante integraciones que relacionan los datos de EDR con otros tipos de telemetría.

La capacidad de esta tecnología de utilizar los flujos de datos relativos a la seguridad para mejorar los modelos de aprendizaje automático —así como para facilitar la coordinación entre la detección y la respuesta— tiene el gran poder de mantener a los adversarios a raya durante largo tiempo.

¿Le interesaría obtener más información sobre las nuevas funciones de búsqueda de amenazas o sobre cómo puede defender su entorno Cortex XDR? Programe un taller práctico con nuestros expertos o solicite una demostración de Cortex XDR.

Recursos adicionales para entender la tecnología XDR

Descargue nuestro libro electrónico *XDR: guía esencial*.

Descargue nuestra ficha técnica sobre *Cortex XDR*.

Visite nuestra página de la Ciberpedia What is XDR? (disponible en inglés).

Para obtener información sobre la tercera ronda de evaluaciones MITRE ATT&CK®, *descargue nuestro libro electrónico* (disponible en inglés).

Somos líderes en el informe de Forrester Research *The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q3 2020* (disponible en inglés). Haga clic en el enlace para descargar el informe.

paloalto NETWORKS

Oval Tower, De Entrée 99 - 197
1101HE Ámsterdam
Países Bajos

Tel.: +31 20 888 1883

www.paloaltonetworks.es

cortex_wp_supply-chains-in-the-crosshairs_071221-es