SOPHOS
Cybersecurity evolved.

Minimizar el riesgo de ataques a la cadena de suministro: directrices para las mejores prácticas

En diciembre de 2020, la noticia de un ciberataque contra la empresa de monitorización de TI SolarWinds puso en el punto de mira los ataques a la ciberseguridad de la cadena de suministro, pero están lejos de ser algo nuevo. De hecho, según la encuesta realizada por Sophos en 2020 a 5000 responsables de TI de 26 países[1], casi una de cada 10 víctimas de ransomware (9 %) afirmó que el ataque se produjo a través de un proveedor de confianza, lo cual resulta preocupante.

Pero, ¿qué es exactamente un ataque a la cadena de suministro y cómo funciona? Y lo que es más importante: ¿qué puede hacer para proteger su empresa de los efectos de un ataque a la cadena de suministro?

En este monográfico se responde a estas y otras preguntas.

1 El estado del ransomware 2020 – Sophos, 2020

Monográficos de Sophos. Abril de 2021

¿Qué es un ataque a la cadena de suministro?

Las empresas suelen depender de algún tipo de proveedor externo para gestionar toda o parte de una función empresarial concreta, como su infraestructura informática. Si bien permitir que los proveedores externos se conecten a su red tiene ventajas para la empresa (por ejemplo, liberar recursos internos), conlleva un riesgo inherente para la seguridad, concretamente la exposición a ataques a la cadena de suministro.

En un ataque a la cadena de suministro, en lugar de infiltrarse directamente en su empresa, los atacantes aprovechan el acceso que los proveedores externos de confianza tienen ya a sus sistemas para introducirse en su entorno. Una vez que entran, pueden realizar todo tipo de actividades maliciosas.

El hecho de tener un solo proveedor conectado a su red introduce el riesgo de un ataque a la cadena de suministro. Sin embargo, las pymes afirman tener, de media, al menos tres proveedores que pueden conectarse a sus sistemas[2]. Garantizar la protección de estos proveedores conectados supone un desafío importante y una mayor carga de trabajo para los equipos de TI. A este complicado reto hay que añadir que los ataques a la cadena de suministro son especialmente difíciles de detectar, y mucho más de defender, ya que pueden proceder de cualquier parte de la cadena de suministro.

Tipos de proveedores externos

Los servicios profesionales y los proveedores de servicios de TI son dos de los proveedores externos más comunes que pueden conectarse a la red de una empresa.

Servicios profesionales

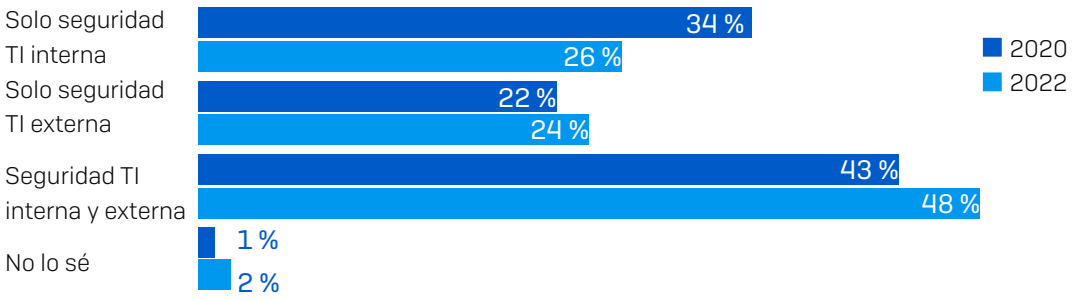
Las empresas suelen recurrir a los servicios profesionales para gestionar de forma independiente funciones empresariales (o parte de ellas) cuando no disponen de las habilidades o los conocimientos especializados necesarios a nivel interno. Por ejemplo, una empresa de contabilidad que necesita tener acceso a datos financieros confidenciales (a través de un software) para ofrecer al cliente el análisis y la información para los que ha sido contratada. Como es de imaginar, un ciberataque fructífero contra una empresa de este tipo podría ser devastador para su cartera de clientes.

Proveedores de servicios de TI

Los proveedores de servicios de TI son empresas externas a las que se confía la gestión de la infraestructura informática y/o la seguridad informática de una empresa. A menudo conocidos como proveedores de servicios administrados (MSP) o proveedores de servicios de seguridad administrados (MSSP), son el objetivo frecuente de los ataques a la cadena de suministro.

Son blancos especialmente atractivos para los atacantes porque tienen acceso a muchos clientes diferentes. Dado que el número de empresas que subcontratan su seguridad TI está previsto que aumente hasta el 72 % en 2022[3], la posición de seguridad de estos proveedores es de suma importancia para la suya.

Cómo se presta la seguridad TI: 2020 frente a 2022



2,3 Ciberseguridad: El reto humano – Sophos, 2020

Tipos de ataques a la cadena de suministro

Si bien los ataques a la cadena de suministro difieren en cuanto a la forma en que se producen, los principios y el objetivo final de los atacantes suelen ser los mismos: infiltrarse en un proveedor de confianza externo y abusar del acceso del que goza para implantar malware, robar propiedad intelectual o espiar comunicaciones internas.

Ataques de phishing

Uno de los vectores de ataque más comunes utilizados por los atacantes de la cadena de suministro son los correos electrónicos de phishing. Los delincuentes atacan a proveedores externos de confianza con correos electrónicos de phishing para obtener acceso a sus redes y comprometerlas, y luego las utilizan como trampolín para penetrar en los sistemas de sus clientes.

Actualización de software comprometida

En ataques a la cadena de suministro más sofisticados, los hackers se infiltran en la infraestructura de una empresa o distribuidor de software e insertan código malicioso en los paquetes de actualización de software. El proveedor distribuye entonces esas actualizaciones a sus clientes, infectándolos en el proceso sin saberlo. Como podrá imaginar, las consecuencias pueden ser devastadoras, sobre todo si la empresa tiene una gran cartera de clientes. El ataque a SolarWinds de diciembre de 2020 es un claro ejemplo de este tipo de ataque.

Estudio de caso de ataque a la cadena de suministro: SolarWinds

A finales de 2020, se descubrió que la cadena de suministro de la empresa de gestión de TI SolarWinds se había visto comprometida. Este acontecimiento acaparó titulares en todo el mundo y puso de relieve la vulnerabilidad de la seguridad de la cadena de suministro. Se cree que afectó a más de 18 000 de sus clientes.

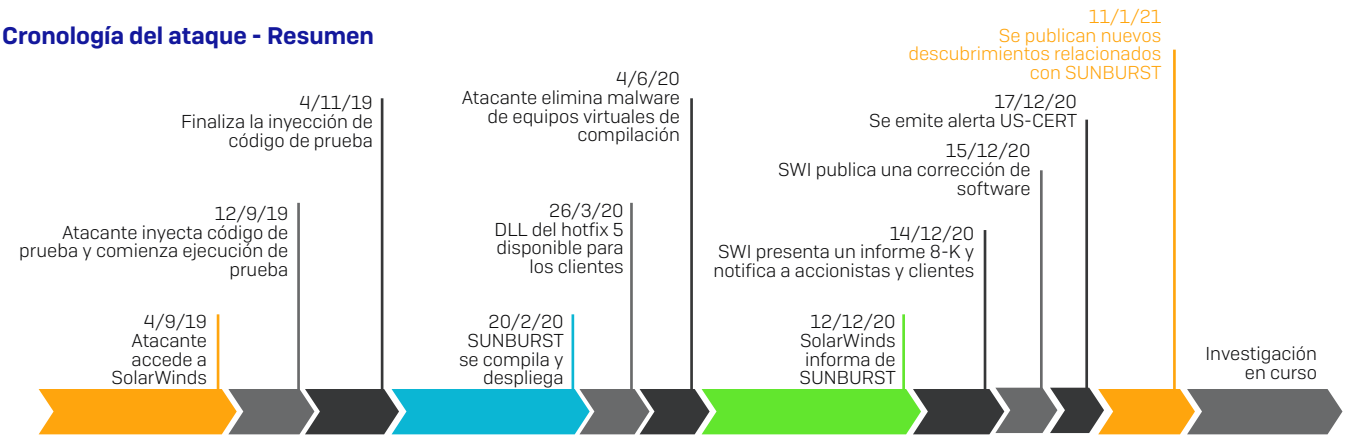
Es importante señalar que, a la fecha de publicación de este monográfico, abril de 2021, la investigación sobre el ataque a SolarWinds sigue en curso y podría cambiar.

¿Cómo lo consiguieron los atacantes?

De manera resumida, los hackers lograron insertar código malicioso en Orion, la plataforma de monitorización y gestión de infraestructuras de SolarWinds. Luego, este código malicioso se envió sin querer a los clientes a través de una actualización de software estándar. Se calcula que alrededor de 18 000 clientes (entre ellos muchas empresas Fortune 500 y agencias gubernamentales de EE. UU.) instalaron las actualizaciones, lo que los dejó expuestos.

Lo que resulta preocupante es que, ya en septiembre de 2019, SolarWinds empezó a sospechar de indicios de juego sucio, como se puede ver en la siguiente tabla cronológica. Esto sugiere que la maniobra fue calculada y que los responsables del ataque extremaron las precauciones, tratando de hacer saltar el menor número posible de alarmas en su infiltración. Puede leer el análisis detallado de Sophos sobre cómo la variante de malware Sunburst burló las defensas.

Cronología del ataque - Resumen



Todos los eventos, fechas y horas son aproximados y están sujetos a cambios, a la espera de que finalice la investigación.

SolarWinds: https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

¿Qué impacto ha tenido el ataque?

El éxito del ataque, bautizado como Sunburst, dio a los delincuentes un amplio acceso a sistemas de información corporativos y gubernamentales. Ya ha dado lugar a volúmenes aún sin calcular de datos robados y ha suscitado preocupación por que los atacantes hayan utilizado esta posición para introducir otras puertas traseras en redes empresariales que todavía no se han descubierto.

Y lo que es más importante, la escala global del ataque ha puesto de manifiesto lo poco preparadas que están muchas empresas a la hora de defenderse de los ataques a la cadena de suministro.

Paquetes envenenados

Un tipo menos común de ataque a la cadena de suministro, pero que previsiblemente será más frecuente en el futuro, es lo que hemos llamado "paquetes envenenados". A medida que crece el uso de la nube, Docker y las metodologías de desarrollo ágil, también lo hace el uso de componentes estándar para acortar el ciclo de vida del desarrollo. Los delincuentes han comenzado a cargar código malicioso en contenedores, bibliotecas y otros recursos de uso común, con la esperanza de que se incluyan en el producto final.

Directrices para defenderse contra los ataques a la cadena de suministro

Dada la complejidad y la naturaleza de los ataques a la cadena de suministro, la tecnología por sí sola no puede evitarlos. Estas directrices para las mejores prácticas pretenden ayudarle a minimizar el riesgo asociado a un ataque a la cadena de suministro.

1. Cambie de un enfoque reactivo a proactivo a la ciberseguridad

SolarWinds fue la señal de alarma para muchas empresas de todo el mundo. Una vez que un ataque resulta obvio, a menudo es demasiado tarde: para cuando un delincuente distribuye una carga, puede haber robado ya datos críticos y, a menudo, haber tenido acceso a su red durante días. Hay que adoptar una nueva mentalidad: asumir que siempre se está en peligro y buscar las amenazas antes de que sea demasiado tarde. Hay tecnologías y servicios que pueden respaldar este enfoque, que ampliaremos más adelante en este monográfico.

2. Monitorice las primeras señales de peligro

Durante las investigaciones llevadas a cabo por el equipo de Sophos Managed Threat Response (MTR), hay dos cosas que destacan como indicadores tempranos de peligro: por un lado, el uso de credenciales para el acceso remoto y con fines administrativos durante las horas no laborables y, por otro, el abuso de las herramientas de administración del sistema para realizar tareas de vigilancia y robar datos de la red.

El uso de cuentas legítimas y de sus propias herramientas para conseguir persistencia y mantenerla se suele denominar "vivir de la tierra" (LOL). Detectar estos comportamientos requiere vigilancia y pericia; sin embargo, saltan a la vista para un analista de operaciones de seguridad preparado, quien le alertará del ataque antes de que se haya producido la mayor parte del daño. Conviene invertir en la tecnología y la formación necesarias para supervisar estos indicadores internamente o contratar a un proveedor de servicios de detección y respuesta gestionadas (MDR) para que los supervise en su nombre.

3. Realice una auditoría de su cadena de suministro

Puede parecer obvio, pero dedicar algo de tiempo a elaborar una lista de todas las empresas con las que está conectado puede ser muy valioso. Probablemente haya más de las que cree. Al realizar este ejercicio, podrá identificar rápidamente los eslabones débiles (por ejemplo, las empresas más susceptibles a la ciberdelincuencia) y tomar nuevas medidas para mitigar los riesgos asociados. Es de esperar que esté conectado con proveedores externos como:

- **Proveedores de servicios de TI**
  - MSP / MSSP
  - Proveedores de la nube
- **Servicios profesionales**
  - Finanzas
  - Jurídicos
  - Seguridad
  - Conserjería
- **Proveedores**
  - Materiales
  - Servicios
  - Mano de obra
  - Logística

Una vez que haya identificado con qué proveedores está conectado, podrá evaluar el tipo de acceso a la red que tienen y a qué información podrían acceder utilizando esas credenciales. Si supera el mínimo, es el momento de bloquear ese acceso y limitarlo solo a la información necesaria. Comience con los proveedores con mayor acceso innecesario y vaya bajando.

4. Evalúe la posición de seguridad de sus proveedores y partners comerciales

Hay muchos enfoques para realizar una evaluación, pero uno frecuente para los grandes proveedores de servicios, operadores en la nube y procesadores de pagos es determinar a qué tipos de certificaciones y auditorías están sujetos.

Por ejemplo, un procesador de pagos deberá cumplir el estándar PCI DSS. Si está sujeto al nivel 1 o 2 de PCI DSS, debe solicitarle el informe de cumplimiento (RoC) emitido por su QSA/ISA. Deberá revisar estos RoC trimestralmente para asegurarse de que cumplen sus expectativas.

Otra certificación habitual para confirmar auditorías son los informes SOC 2/2+/3 para sus proveedores de servicios en la nube. Las auditorías SOC evalúan los controles y mitigaciones de seguridad que abarcan cinco principios de servicios de confianza: privacidad, seguridad, disponibilidad, integridad del procesamiento y confidencialidad.

Al igual que con su propia seguridad, el número de auditorías no es garantía de nada, pero sin duda es una indicación de que el proveedor se toma en serio la seguridad y el cumplimiento. Otras cosas que puede considerar o pedir son los informes de pruebas de penetración, el cumplimiento del RGPD o la frecuencia de fallos de seguridad o filtraciones de datos anteriores.

5. Revise constantemente su propia higiene de las operaciones de seguridad TI

Si bien la posición de seguridad de sus proveedores es fundamental para protegerse de los ataques a la cadena de suministro, no debe descuidar su propia higiene de ciberseguridad. Muchas empresas la pasan por alto, ya sea porque no saben por dónde empezar o no se creen lo suficientemente importantes como para ser el blanco de delincuentes a través del ataque a un partner de confianza. Sus prácticas de ciberseguridad podrían significar la diferencia entre una pequeña molestia y una filtración de datos catastrófica.

Active la autenticación multifactor (MFA)

La forma más habitual en que vemos que las empresas son víctimas de ataques a la cadena de suministro es mediante el uso de accesos robados pero autorizados. Los proveedores de servicios reciben con demasiada frecuencia credenciales con los mismos derechos y privilegios que los empleados internos.

En otras palabras, no están obligados a utilizar la MFA, lo que permite a los atacantes explotar tanto las credenciales robadas mediante ataques de phishing como la reutilización no autorizada de credenciales por parte de su personal. Dado que la mayoría de las empresas emplean el inicio de sesión único (SSO), se puede abusar de estas credenciales para acceder a todo tipo de sistemas que son innecesarios para la tarea asignada, lo que aumenta el riesgo de usuarios maliciosos tanto internos como externos.

Revise el acceso de los proveedores y los privilegios de las aplicaciones

Otro error común es ofrecer VPN, RDP u otra tecnología de acceso remoto sin restricciones a terceros para que puedan gestionar las soluciones. Por "sin restricciones" nos referimos a dar acceso a toda la red en lugar de segmentar y endurecer cuidadosamente las herramientas de acceso remoto necesarias.

Todas las herramientas dirigidas a usuarios externos deben requerir la autenticación multifactor, y deben limitarse a hosts o sistemas únicos. Cuando se desee un acceso adicional, se recomienda el uso de "hosts de salto" para reducir el riesgo y ofrecer más oportunidades de supervisión y registro.

Permitir por defecto todas las aplicaciones firmadas por el certificado de software de un proveedor también expone a las empresas a ataques a la cadena de suministro. En repetidas ocasiones hemos visto cómo se robaban certificados y se empleaban para firmar malware. Las herramientas de seguridad deben inspeccionar todo lo posible.

Supervise de forma proactiva los boletines de seguridad de los proveedores
Monitorice los boletines de seguridad de todos los proveedores para poder desplegar rápidamente parches y mitigaciones cuando se detecten vulnerabilidades, y esté atento a las noticias relacionadas con sus proveedores. Cuando se está en medio de una crisis respondiendo a un incidente, es posible que usted no figure muy alto en la lista de empresas a las que notificar. Esto puede permitirle bloquear el acceso y empezar a investigar si se ve afectado por su situación.

Revise su póliza de seguro de ciberseguridad (si la tiene)
Por último, si dispone de un seguro de ciberseguridad, determine si cubre las pérdidas de terceros y cómo activar la póliza, si es necesario. Coordínese con sus proveedores para asegurarse de que su cobertura se solapa con la que ellos tengan.

Habilitadores de tecnología y servicios

Como se ha mencionado anteriormente, la defensa contra los ataques a la cadena de suministro es compleja por naturaleza. Más bien se trata de gestionar el riesgo asociado a ellos y amortiguar el golpe. Por suerte, existen tecnologías y servicios que son ideales para ayudar a mitigar este riesgo.

Búsqueda de amenazas

Hemos mencionado la necesidad de pasarse a un enfoque proactivo a la ciberseguridad para protegerse de los ataques a la cadena de suministro. La búsqueda de amenazas es una práctica clave que las empresas deben adoptar para materializar esta mentalidad.

Detección y respuesta para endpoints (EDR)
Un elemento clave en la búsqueda de amenazas es la tecnología EDR. La EDR, que suele estar integrada en las plataformas de protección de endpoints, combina datos de endpoints y supervisión continua en tiempo real con funciones de respuesta y análisis automatizadas. Esto permite a los equipos de seguridad identificar y remediar rápidamente las amenazas.

Sophos Intercept X Endpoint incluye una potente funcionalidad EDR. Sophos EDR es la primera EDR diseñada tanto para analistas de seguridad como para administradores de TI, y le ofrece las herramientas necesarias para formular preguntas detalladas a la hora de buscar amenazas y reforzar la higiene de sus operaciones de seguridad TI. Podrá utilizar potentes consultas SQL predefinidas y personalizables que le proporcionan la información que necesita para tomar decisiones informadas.

Además, la función de identificación de amenazas automatizada de Sophos EDR le permite identificar automáticamente actividad sospechosa, priorizar los indicadores de amenazas y buscar rápidamente las posibles amenazas en endpoints y servidores.

Más información sobre las funciones de Sophos EDR

Servicios de detección y respuesta gestionadas (MDR)
Las ciberamenazas más devastadoras, como el ataque a SolarWinds, suelen ser ataques perpetrados por humanos. Si bien la tecnología, en particular las herramientas de búsqueda de amenazas como la EDR, desempeña un papel importante, sigue siendo necesario contar con operadores expertos. Detener los ataques llevados a cabo por humanos requiere una búsqueda de amenazas realizada por humanos, y los responsables de TI lo saben, ya que el 48 % de ellos tiene previsto incorporar estas prácticas durante el próximo año[4].

4 Ciberseguridad: El reto humano – Sophos, 2020

Uno de estos enfoques a la búsqueda de amenazas a cargo de humanos es la contratación de un servicio MDR. El galardonado servicio MDR de Sophos, Sophos Managed Threat Response (MTR), va más allá de la mera notificación de amenazas: dota a su personal de TI de un equipo dedicado de expertos en ciberseguridad que trabajan 24/7 para buscar, validar y remediar de forma proactiva posibles amenazas e incidentes en su nombre.

El equipo de Sophos MTR de cazadores de amenazas y expertos en respuesta se dedican a:

- Buscar y validar de forma proactiva posibles amenazas e incidentes.
- Utilizar toda la información disponible para determinar el alcance y la gravedad de las amenazas.
- Aplicar el contexto empresarial adecuado para las amenazas reales.
- Iniciar acciones para interrumpir, contener y neutralizar amenazas de forma remota.
- Brindar asesoramiento práctico para abordar la causa raíz de los incidentes recurrentes.

Más información sobre Sophos MTR

La evolución hacia un enfoque de confianza cero a la ciberseguridad

Antes hemos hablado de revisar su propia posición de seguridad; en particular, de habilitar la MFA y verificar constantemente tanto los privilegios de acceso como los de las aplicaciones. Todo esto puede lograrse adoptando un enfoque de confianza cero a la ciberseguridad.

La confianza cero se basa en el principio de que no se debe confiar en nada y que se debe comprobar todo, y en que hay que centrarse en proteger los recursos independientemente de dónde estén física o digitalmente. No existe un único proveedor, producto o tecnología que pueda hacerle llegar a la confianza cero. Lo que se necesita es un cambio cultural y numerosas soluciones distintas para modificar los paradigmas por los que protegemos nuestros recursos. Sin embargo, un paso hacia este modelo es la adopción de una solución Zero Trust Network Access (ZTNA).

ZTNA, como su nombre indica, se basa en el principio de la confianza cero. Permite a los usuarios acceder de forma segura a los datos desde cualquier lugar, al tiempo que ofrece a los administradores controles muy granulares.

ZTNA se centra en verificar al usuario, normalmente con la autenticación multifactor y un proveedor de identidad, validar el estado de seguridad y el cumplimiento del dispositivo (comprobando si está inscrito, actualizado, debidamente protegido, con cifrado habilitado, etc.) y luego utilizar esa información para tomar decisiones basadas en políticas para determinar los privilegios y el acceso a las aplicaciones en red importantes. ZTNA constituye una gran alternativa a las VPN de acceso remoto, ya que puede ofrecer controles muy granulares sobre quién puede acceder a qué, algo fundamental para protegerse de los ataques a la cadena de suministro que dependen del acceso de los proveedores a sus sistemas.

Sophos ZTNA, nuestra nueva solución de acceso a la red gestionada e implementada en la nube, se incluye actualmente en el programa de acceso temprano (EAP) y estará disponible para el público general a partir de mediados de 2021. Ofrece protección para cualquier aplicación en red alojada en su red local, en la nube pública o en cualquier otro sitio de alojamiento. Cubre todo, desde el acceso RDP a los recursos compartidos de archivos en red hasta aplicaciones como Jira, Wikis, repositorios de código fuente, aplicaciones de soporte y emisión de incidencias, y mucho más.

Más información sobre Sophos ZTNA

Conclusión

Dada su complejidad, es casi imposible evitar que se produzca un ataque basado en la cadena de suministro. Sin embargo, si sigue las directrices de este monográfico, puede reducir el riesgo de ser víctima de un ataque y evitar que éste afecte significativamente a su empresa. En resumen:

1. Cambie de un enfoque reactivo a proactivo a la ciberseguridad
2. Monitorice las primeras señales de peligro
3. Realice una auditoría de su cadena de suministro
4. Evalúe la posición de seguridad de sus proveedores y partners comerciales
5. Revise constantemente su propia higiene de las operaciones de seguridad TI

Además, plantéese adoptar tecnologías y servicios como EDR, MTR y ZTNA para apoyar sus objetivos de seguridad de la cadena de suministro.

El panorama de las amenazas ha evolucionado, y que la cadena de suministro se vea comprometida es un problema para las empresas de todos los tamaños. Todos somos objetivos en la cadena de suministro de alguien, y nunca ha sido tan importante minimizar el riesgo de la cadena de suministro de terceros.

Obtenga más información sobre las soluciones de ciberseguridad líderes del sector y la experiencia de Sophos en es.sophos.com

Sophos ofrece soluciones de ciberseguridad líderes en la industria a empresas de todos los tamaños a fin de protegerlas 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 empresa estarán protegidos de forma eficiente por productos con tecnologías de inteligencia artificial y Machine Learning.

14-04-2021 (SB-NP)

SOPHOS