UNIDOS POR LA CIBERSEGURIDAD JUNIO 2022

ATAQUE A LA CADENA DE SUMINISTRO EN AMÉRICA

Global Cyber

soluciones integrales en ciberseguridad

INTRODUCCIÓN

Un ataque a la cadena de suministro, también llamado ataque a la cadena de valor o ataque de terceros, ocurre cuando un actor de amenazas cibernéticas se infiltra en la red de un proveedor de servicios y emplea algún tipo de código malicioso para comprometer uno o más activos, como, por ejemplo, un servicio, un producto o un software contratado al proveedor.

Las consecuencias de un ataque a la cadena de suministro pueden ser severas. Primero, los actores maliciosos utilizan un proveedor comprometido para obtener privilegios y acceso persistente a una red de víctimas y con ello, llevar a cabo diversas actividades maliciosas que pueden incluir la realización de robo de datos personales o financieros, el seguimiento de organizaciones o individuos , así como la inhabilitación redes o sistemas, o incluso causar daños físicos o la muerte.

La consigna es que entre todos podemos crear una internet segura. Estamos llamados a crear esfuerzos comunes para prevenir incidentes, crear conciencia y estar preparados para enfrentar a los desafíos que nuestra hiperconectada realidad. Las tecnologías de la información están cambiando al mundo, y debemos adaptarnos a esos cambios con ciberseguridad.

¿Qué son los ataques a la cadena de suministro ?

En el caso de las empresas, uno de sus principales activos se encuentra en la información que poseen, y por eso resulta de gran interés para los ciberdelincuentes. De ahí que si las empresas protegen su información, protegen su negocio. Esta protección comienza por la concientización y sensibilización que permita hacer un uso adecuado de la tecnología, protegiendo el negocio y garantizando los derechos de los clientes o usuarios. Las empresas, sin importar su tamaño o su sector, deben

Pero la prevención no solo viene de la mano de la empresa, también de sus proveedores. En la actividad diaria, las empresas necesitan contratar determinados servicios especializados a proveedores externos para que les den soporte, y en este proceso resulta fundamental que gestionen con seguridad la información que manejan de los clientes, sobre todo si se trata de información sensible.

Un ataque a la cadena de suministro se produce cuando un atacante accede a la red de trabajo de una empresa a través de sus vendedores o proveedores o a través de la cadena de suministro. (1)

En el contexto de la transformación digital, esta amenaza se enfoca en comprometer proveedores de servicios digitales de manera externaliza o vía outsourcing, proveedores de telecomunicaciones, proveedores de software, proveedores de servicios externos, proveedores de hardware, proveedores de centros de operación de redes, proveedores de centros de operación de ciberseguridad, proveedores de servicios de medios de pago, proveedores de servicios de comercio electrónico como instrumento para infiltrarse desde allí en una organización objetivo.

(1) https://www.keepersecurity.com/es_ES/threats/supply-chain-attack.html

CONTACTO@GLOBALCYBER.CL

El activo afectado compromete entonces los datos o el sistema del o los clientes. Un servicio recién adquirido puede verse comprometido desde el principio, o puede ocurrir un compromiso a través de otros medios como un parche o revisión. En estos casos, el compromiso puede ocurrir antes de que el parche o la revisión ingresen a la red del cliente. Estos tipos de ataques afectan a todos los usuarios del activo comprometido y pueden tener consecuencias para el gobierno, la infraestructura crítica, empresas u organizaciones y los clientes.

El asegurarse de que los proveedores de servicios externalizados son confiables es extremadamente difícil. La ofuscación y anonimización dificultan la identificación del atacante.

Este tipo de ataques tienen un gran potencial debido a que un proveedor puede dar servicio a muchos clientes, estableciéndose una relación de confianza entre cliente-proveedor, los cuales a su vez pueden ser proveedores de otros. De esta forma, en una sola operación pueden infectarse o comprometerse todos los clientes o solo algunos muy específicos si esta vía la está utilizando, por ejemplo, un APT.

¿Cómo opera?

Una cadena de suministro comprende todo lo que se encuentra entre las materias primas y el producto final, lo cual abarca al proveedor de materias primas, los procesos de fabricación, la distribución y finalmente el consumidor, como le ocurrió al proveedor de soluciones de seguridad FireEye cuando fueron atacados recientemente. Cuando la empresa descubrió que había sido víctima de un ciberataque, una investigación más profunda descubrió que el atacante había introducido una actualización maliciosa en un producto de gestión de red llamado Orion, fabricado por SolarWinds; uno de los proveedores de software que utiliza la empresa

El backdoor, al que FireEye denominó SUNBURST y que ESET detecta como MSIL/SunBurst.A, fue implantado en Orion antes de que el código fuese entregado a FireEye, creando así un producto final contaminado para el consumidor. Pero en este caso, "el consumidor" se refería en realidad a unas 18.000 organizaciones comerciales y gubernamentales que instalaron la actualización maliciosa a través del mecanismo de actualización de Orion, convirtiéndose así en las víctimas finales del ataque. Al menos 100 de ellas fueron atacadas con la intención de realizar otras acciones maliciosas, y los actores de amenazas insertaron payloads adicionales y se adentraron más profundamente en las redes de las empresas. (1).

Cuando un grupo de cibercriminales se pone como objetivo realizar un ataque de cadena de suministro, buscará el eslabón más débil de dicha cadena, aquel que «menos esfuerzo» le requiera para instalar su método de ataque. Lo habitual es que busquen protocolos de red no seguros, servidores desprotegidos, y prácticas de codificación no seguras, así, Interrumpen, cambian los códigos fuente y ocultan malware en los procesos de compilación y actualización o cualquier vulnerabilidad que les permita insertar sus herramientas maliciosas.

Fuente:

(1) https://www.welivesecurity.com/la-es/2021/04/12/ataques-cadena-suministro-modalidad-que-crece-y-supone-gran-riesgo/
https://protecciondatos-lopd.com/empresas/ataques-cadena-de-suministro/

CONTACTO@GLOBALCYBER.CL

Y ahí es donde en realidad radica el potencial daño de los ataques de cadena de suministro: al comprometer a un solo proveedor, los cibercriminales pueden eventualmente obtener acceso sin restricciones y difícil de detectar a una gran franja de sus clientes.

Es prácticamente imposible que cualquier empresa tenga el control total de su cadena de suministro para garantizar que ningún componente en bruto que se ha incorporado en sus propios productos o que sus servicios no han sido contaminados o explotados en el camino hacia el eventual consumidor. Minimizar el riesgo de un ataque de cadena de suministro implica un ciclo interminable de gestión de riesgos y cumplimiento; en el ataque de SolarWinds, el profundo análisis posterior al ataque del producto del proveedor externo identificó el exploit enterrado muy profundamente en el código.

Tipos de ataques a la cadena de suministros

Los ataques a la cadena de suministro se pueden producir de muchas maneras, pues incluye los ataques mediante software, hardware y firmware.

Ataques a la cadena de suministro mediante software

Un ataque a la cadena de suministro mediante software tan solo requiere que una aplicación comprometida o una parte de un software envíe el malware por toda la cadena de suministro. Los ataques suelen dirigirse al código fuente de una aplicación, pues envían un código malicioso a una aplicación de confianza o al sistema del software.

El objetivo de los atacantes suelen ser las actualizaciones del software o de aplicaciones, que sirven como puntos de entrada. El problema de los ataques a la cadena de suministro mediante software es que son difíciles de rastrear, ya que los ciberdelincuentes suelen utilizar certificados robados para "firmar" el código y hacerlo parecer legítimo.

Ataques a la cadena de suministro mediante hardware

Los ataques mediante hardware dependen de dispositivos físicos, como el registrador de pulsaciones de teclas ubicado en una unidad USB mencionado anteriormente. Los atacantes se dirigirán al dispositivo que se abra camino a través de toda la cadena de suministro para maximizar su alcance y su daño.

CONTACTO@GLOBALCYBER.CL

Fuente: Crowdstrike

Ataques a la cadena de suministro mediante firmware

Insertar malware en el código de arranque de un ordenador es un ataque que solo tarda un segundo en desarrollarse. Cuando se inicia un ordenador, el malware se ejecuta y pone en riesgo todo el sistema. Los ataques con firmware son rápidos (e incluso indetectables si no se buscan) e extremadamente dañinos. (2)

(2) https://www.keepersecurity.com/es_ES/threats/supply-chain-attack.html

CONTACTO@GLOBALCYBER.CL

EJEMPLOS DE AMENAZAS EN EL CICLO DE VIDA DE LA CADENA DE SUMINISTRO DE LAS TIC

Fase de Diseño:

Vulnerabilidades introducidas durante el diseño a menudo no son intencionales y pueden potencialmente afectar a todos los usuarios de los componentes. Los actores maliciosos podrían integrar vulnerabilidades en componentes que puede instalarse en millones de piezas de equipos.

Dispositivos celulares secuestrados. 2016[1]: una empresa extranjera diseñó un software utilizado por un fabricante de teléfonos de EE. UU. Los teléfonos hicieron registros encriptados del historial de llamadas y mensajes de texto, detalles e información de contacto y transmitió esos datos a un servidor externo cada 72 horas.

Desarrollo y Producción:

Vulnerabilidades introducidas durante esta fase a menudo son inadvertidas y pueden ser costosas de corregir si no se identifican al realizar la prueba inicial de prototipos. Aún los productos bien diseñados pueden tener componentes maliciosos introducidos durante la fabricación o el montaje, siendo un forma que es potencialmente difícil de identificar.

SolarWinds 2020[2]: una empresa de gestión de TI fue infiltrada por un actor de amenazas extranjero que mantuvo la persistencia en su red durante meses. El actor de amenazas abandonó la red solo después de que había comprometido los servidores de compilación de la empresa y utilizó su proceso de actualización para infiltrarse en las redes de clientes estratégicos.

[1] https://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html
[2] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Global Cyber
soluciones integrales en ciberseguridad

Fuente: Crowdstrike

CONTACTO@GLOBALCYBER.CL

Distribución:

Componentes transportados entre las instalaciones de producción y los clientes a menudo escapa del ámbito del personal responsable de su diseño o producción. Vulnerabilidades introducidas durante la distribución probablemente sean malintencionadas y afecten a un número limitado de componentes y clientes en comparación con fases anteriores.

Malware para dispositivos de usuario final. 2012[1]: Investigadores de una importante empresa de software de EE. UU., investigando software falsificado encontraron malware preinstalado en el 20 por ciento de los dispositivos que probaron. El malware se instaló en las computadoras de escritorio y portátiles nuevos después de su envío desde una fábrica a un distribuidor, transportista o revendedor. La pieza de software maliciosa más peligrosa que encontró se llama Nitol, un virus agresivo que se encuentra en computadoras en China, Estados Unidos, Rusia, Australia y Alemania, incluso se han identificado servidores en las Islas Caimán que controlan las máquinas infectadas con Nitol. Todas las computadoras afectadas se convierten en parte de una botnet, grupo de computadoras comprometidas, una de las formas más invasivas y persistentes de ciberdelito.

Adquisición y Despliegue:

Los "insiders" maliciosos pueden introducir vulnerabilidades o reemplazar el equipo con uno con componentes vulnerables durante la adquisición o instalación. Vulnerabilidades introducidas durante esta fase probablemente afecte solo a un número acotado de clientes.

Kaspersky Antivirus. 2017[2]: un proveedor de antivirus con sede en el extranjero estaba siendo utilizado por un servicio de inteligencia extranjera para el espionaje. Se instruyó a los clientes gubernamentales de EE. UU. A remover el producto de dicho proveedor de sus redes y no se le permitió adquirir productos a futuro de ese vendedor.

2015: un ciudadano de EE. UU. Importó miles de circuitos integrados falsificados desde China y Hong Kong, y los revendió a clientes de EE. UU., incluidos los contratistas de Defensa, suministrándolos a la Marina de los EE. UU. para uso en submarinos nucleares.

[1] https://www.theguardian.com/technology/2012/sep/14/malware-installed-computers-factories-microsoft
[2] https://www.theguardian.com/technology/2017/sep/13/us-government-bans-kaspersky-lab-russian-spying

Mantenimiento:

Componentes de TIC que reciben mantenimiento o actualizaciones son susceptibles a las vulnerabilidades introducidas a través de acceso físico o acceso vía la red, y de la explotación de vulnerabilidades previamente desconocidas o sin parchear. Las vulnerabilidades introducidas durante el mantenimiento generalmente están dirigidas contra entidades específicas, pero pueden afectar a muchos clientes en el caso de actualizaciones de software.

Backdoors integradas en actualizaciones de mantenimiento de rutina. 2020[1]: Miles de redes públicas privadas fueron infiltradas cuando un actor de amenazas usó una actualización rutinaria para entregar e ingresar una puerta trasera maliciosa.

Disposición (basura TIC):

Los componentes TIC que están incorrectamente desechados puede contener datos sensibles de la empresa o de los clientes. Actores maliciosos pueden intentar "refaccionar" componentes e intentar revenderlos como nuevos. Las piezas usadas pueden ser menos confiables y propensas a fallar o tener instalado malware.

Datos sensibles en la basura TIC. 2019[2]: Un investigador compró computadoras viejas, unidades flash, teléfonos y discos duros, encontrando solo dos dispositivos correctamente borrados de los 85 examinados. También se encontraron cientos de casos con información de identificación personal (PII), incluyendo números de seguridad social, números de pasaporte y números de tarjetas de crédito.

[1] https://www.npr.org/2020/12/15/946776718/u-s-scrambles-to-understand-major-computer-hack-but-says-little
[2] https://threatpost.com/second_hand_insecure_data/142948/

¿CÓMO PUEDO PROTEGERME?

Buenas practicas

- **Política de seguridad de la información para las relaciones con los proveedores**

Acordar los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso de los proveedores a los activos de la organización con el proveedor y se deberían documentar debidamente.
Identificar e imponer controles de seguridad de la información para abordar específicamente el acceso de los proveedores a la información de la organización en una política:

a) la identificación y la documentación de los tipos de proveedores, es decir, los servicios de TI, las utilidades de logística, los servicios financieros, los componentes de la infraestructura de TI y a quiénes autorizará la organización para acceder a su información;
b) un proceso y ciclo de vida estandarizado para administrar las relaciones con los proveedores;
c) la definición de los tipos de acceso a la información que se les permitirá a los distintos tipos de proveedores y el monitoreo y control del acceso;
d) requisitos mínimos de seguridad de la información para cada tipo de información y tipo de acceso para servir de base para los acuerdos individuales con los proveedores en base a las necesidades comerciales de la organización y los requisitos y su perfil de riesgo;
e) procesos y procedimientos para monitorear la adherencia a los requisitos de seguridad de información establecidos para cada tipo de proveedor y tipo de acceso, incluida la revisión de terceros y la validación de productos;
f) controles de precisión y nivel de detalles para garantizar la integridad de la información o el procesamiento de información que entrega cualquiera de las partes;
g) tipos de obligaciones aplicables a los proveedores para proteger la información de la información;

CONTACTO@GLOBALCYBER.CL

¿CÓMO PUEDO PROTEGERME?

h) manejo de incidentes y contingencias asociadas con el acceso a los proveedores, incluidas las responsabilidades de la organización y los proveedores;
i) resiliencia y, en caso de ser necesario, disposiciones de recuperación y contingencia para garantizar la disponibilidad de la información o el procesamiento de información proporcionado por cualquiera de las partes;
j) capacitación de concientización para el personal de la organización involucrado en las adquisiciones sobre políticas, procesos y procedimientos correspondientes;
k) capacitación de concientización para el personal de la organización que interactúa con el personal de los proveedores en cuanto a las reglas adecuadas sobre el compromiso y el comportamiento en base al tipo de proveedor y el nivel de acceso del proveedor a los sistemas y la información de la organización;
l) las condiciones sobre los controles y requisitos de seguridad de la información se documentarán en un acuerdo firmado por ambas partes;
m) administración de las transiciones necesarias de información, instalaciones de procesamiento de información y cualquier otra cosa que se deba mover y, garantizando que se mantiene la seguridad de la información a través de todo el período de transición.

- **Abordar la seguridad dentro de los acuerdos con los proveedores**

Establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización.
Establecer y documentar acuerdos con los proveedores para garantizar que no existen malos entendidos entre la organización y el proveedor en cuanto a las obligaciones de ambas partes para cumplir con los requisitos de seguridad de la información pertinentes.
Se deberían considerar los siguientes términos para incluir en los acuerdos y poder satisfacer los requisitos de seguridad de la información identificados:

a) descripción de la información que se debería proporcionar o a la que se debería acceder y los métodos para proporcionar o acceder a la información;

CONTACTO@GLOBALCYBER.CL

¿CÓMO PUEDO PROTEGERME?

b) clasificación de la información de acuerdo al esquema de clasificación de la organización; y si es necesario también realizar el mapeo entre el esquema propio de la organización y el esquema de clasificación del proveedor;
c) requisitos legales y normativos, incluida la protección de datos, los derechos de propiedad intelectual y derechos de autor y una descripción de sobre cómo se garantizará si se cumplen;
d) obligación de cada parte contractual de implementar un conjunto de controles acordados incluido el control de acceso, la revisión de desempeño, el monitoreo, los informes y la auditoría;
e) reglas de uso aceptable de la información, incluido en uso inaceptable en caso de ser necesario;
f) una lista explícita del personal autorizado para acceder a o recibir la información o los procedimientos o condiciones de la organización para su autorización y el retiro de la autorización, para el acceso a o la recepción de la información de la organización al personal del proveedor;
g) políticas de seguridad de la información pertinentes al contrato específico;
h) requisitos y procedimientos de la administración de incidentes (en especial la notificación y la colaboración durante la remediación de incidentes);
i) requisitos de capacitación y concientización para procedimientos específicos y requisitos de seguridad de la información, es decir, para la respuesta ante incidentes y procedimientos de autorización;
j) normativas pertinentes para la subcontratación, incluidos los controles que se deberían implementar;
k) socios de acuerdos pertinentes, incluida una persona de contacto para los asuntos de seguridad de la información;
l) requisitos de selección, si existe alguno, para el personal del proveedor para realizar los procedimientos de selección y notificación si no se ha completado la selección o si los resultados dan pie a dudas o inquietudes;
m) derecho a auditar los procesos y los controles del proveedor relacionados al acuerdo;
n) procesos de resolución de defectos y resolución de conflictos;
o) obligación del proveedor a entregar periódicamente un informe independiente sobre la efectividad de los controles y un acuerdo sobre la corrección oportuna de los asuntos pertinentes indicados en el informe;
p) obligaciones del proveedor para cumplir con los requisitos de seguridad de la organización.

CONTACTO@GLOBALCYBER.CL

¿CÓMO PUEDO PROTEGERME?

- **Cadena de suministro de la tecnología de información y comunicación**

Los acuerdos con los proveedores deberían incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.
Se deberían considerar los siguientes temas para incluirlos en los acuerdos con el proveedor sobre la seguridad de la cadena de suministro:

a) definir los requisitos de seguridad de la información que se aplicarán a la adquisición de tecnologías, productos o servicios de información y comunicación además de los requisitos de seguridad de la información para las relaciones con el proveedor;
b) para los servicios de tecnología de información y comunicación, que requieren que los usuarios propaguen los requisitos de seguridad de la organización en toda la cadena de suministro si los proveedores realizan subcontrataciones para partes del servicio de tecnología de información y comunicación proporcionados a la organización;
c) para los productos de tecnología de información y comunicación que requieren que los proveedores propaguen las prácticas de seguridad correspondientes a través de toda la cadena de suministro si estos productos incluyen componentes comprados a otros proveedores;
d) implementación de un proceso de monitoreo y métodos aceptables para validar que los productos y servicios de tecnología de información y comunicación se adhieren a los requisitos de seguridad establecidos;
e) implementación de un proceso para identificar los componentes de los productos o servicios que son fundamentales para mantener la funcionalidad y que, por lo tanto, requiere una mayor atención y escrutinio cuando se desarrollan fuera de la organización, especialmente si el proveedor del nivel superior externalice los aspectos de los componentes de productos o servicios a otros proveedores;
f) obtención de una garantía de que los componentes críticos y su origen se pueden rastrear en toda la cadena de suministrar;
g) obtener la garantía de que los productos de tecnología de información y comunicación entregados funcionan según lo esperado sin ninguna función inesperada o no deseada;
h) definición de las reglas para compartir la información en cuanto a la cadena de suministro y cualquier posible problema y compromiso entre la organización y los proveedores;

CONTACTO@GLOBALCYBER.CL

¿CÓMO PUEDO PROTEGERME?

i) implementación de procesos específicos para administrar el ciclo de vida de los componentes de tecnología de información y comunicación junto con la disponibilidad y los riesgos de seguridad asociados. Esto incluye los riesgos de los componentes que ya no están disponibles debido a que los proveedores ya no están en el negocio o a que ya no proporcionan estos componentes debido a los avances de la tecnología.

Las prácticas de administración de riesgos de la cadena de suministro de la tecnología de información y comunicación específicas se desarrollan sobre la seguridad de la información general, la calidad, la administración de proyectos y las prácticas de ingeniería del sistema, pero no las reemplazan. Se aconseja a las organizaciones a trabajar con los proveedores para comprender la cadena de suministro de la tecnología de información y comunicación y cualquier otro asunto que tenga un impacto importante en los productos y servicios que se proporcionan. Las organizaciones pueden influenciar las prácticas de seguridad de información de la cadena de suministro de la tecnología de información y comunicación aclarando en los acuerdos con sus proveedores los asuntos que deberían abordar proveedores en la cadena de suministro de tecnología de información y comunicación. La cadena de suministro de tecnología de información y comunicación según se aborda aquí incluye los servicios de computación en nube.

- **Monitoreo y revisión de los servicios del proveedor**

Deberían monitorear, revisar y auditar la presentación de servicios del proveedor de manera regular.
El monitoreo y revisión de los servicios del proveedor debería garantizar que los términos y condiciones de seguridad de la información de los acuerdos se respeten y que los incidentes y los problemas de seguridad de la información se gestionen correctamente.
Esto debería involucrar un proceso de relación administrativa de servicios entre la organización y el proveedor para:

a) monitorear los niveles de desempeño del servicio con el fin de verificar la adherencia a los acuerdos;
b) revisar los informes de servicio producidos por el proveedor y organizar reuniones de avance de manera regular según lo requieren los acuerdos;

CONTACTO@GLOBALCYBER.CL

¿CÓMO PUEDO PROTEGERME?

c) realizar auditorías de los proveedores, en conjunto con la revisión de informes de auditores independientes, en caso de estar disponibles y, un seguimiento de los problemas identificados;
d) proporcionar información sobre los incidentes de seguridad y revisar esta información según sea necesario conforme a los acuerdos y a cualquier pauta o procedimiento de apoyo;
e) revisar los seguimientos de auditoría del proveedor y los registros de eventos de seguridad de la información, los problemas operacionales, seguimiento de todas las fallas e interrupciones relacionadas con el servicio entregado;
f) resolver y gestionar cualquier problema identificado;
g) revisar los aspectos de seguridad de la información de las relaciones que tiene el proveedor con sus propios proveedores;
h) asegurarse de que el proveedor mantiene una capacidad de servicio suficiente junto con planes de trabajo diseñados para garantizar que se mantienen los niveles de continuidad en el servicio luego de grandes fallas o desastres en el servicio.

La responsabilidad de administrar las relaciones del proveedor se deberían asignar a una persona o equipo de administración de servicios asignado. Además, la organización se debería asegurar de que los proveedores asignen responsabilidades para revisar el cumplimiento y hacer cumplir los requisitos de los acuerdos. Se deberían tener las habilidades y recursos técnicos suficientes a disponibles para monitorear que se cumplen los requisitos del acuerdo, en particular los requisitos de seguridad de la información. Se deberían tomar las medidas necesarias cuando se observan deficiencias en la prestación de servicios. La organización debería retener el control y la visibilidad suficientes en todos los aspectos de seguridad para la información o las instalaciones de procesamiento de información sensible o crítica que evalúa, procesa o administra un proveedor. La organización debería retener la visibilidad en las actividades de seguridad como la administración del cambio, la identificación de vulnerabilidades y los informes y respuestas ante un incidente de seguridad de información a través de un proceso de informes definido.

CONTACTO@GLOBALCYBER.CL

¿CÓMO PUEDO PROTEGERME?

- **Administración de cambios en los servicios del proveedor**

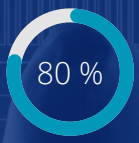
Deben administrar los cambios a la provisión de servicios de parte de los proveedores, manteniendo y mejorando las políticas de seguridad de la información, los procedimientos y controles específicos, considerando la criticidad de la información comercial, los sistemas y procesos involucrados y la reevaluación de riesgos.
Se deberían considerar los siguientes aspectos:
a) cambios a los acuerdos del proveedor;

b) los cambios realizados por la organización por implementar:
- mejoras a los servicios que se ofrecen actualmente;
- desarrollo de cualquier nueva aplicación y sistemas
- las modificaciones o actualizaciones de las políticas y procedimientos de la organización;
- controles nuevos o cambiados para resolver incidentes de seguridad de la información y mejorar la seguridad;
-

c) cambios en los servicios del proveedor a implementarse;
- cambios y mejoras en las redes;
- uso de nuevas tecnologías;
- adopción de nuevos productos o nuevas versiones;
- nuevas herramientas y entornos de desarrollo;
- cambios en la ubicación física de las instalaciones de servicios;
- cambio de proveedores;
- subcontratación a otro proveedor.

CONTACTO@GLOBALCYBER.CL

Cifras alarmantes



- el 80% de las organizaciones han tenido una infracción causada por uno de sus proveedores

- Las empresas tecnológicas con un 15%, se ven más afectadas por los ataques a la cadena de suministro de software

- Los ataques dirigidos a la cadena de suministro han tenido un crecimiento del 350% entre el primer trimestre del 2020 y el del 2021

- Los cibercriminales también han dirigido sus ataques a la cadena de suministro de las vacunascontra el covid-19 con un aumento de un 189% entre diciembre del 2020 y febrero del 2021

- Sólo en Estados Unidos, los ataques a la cadena de suministro aumentaron un 42% y afectaron a 7 millones de personas durante el cuarto trimestre de 2021

- Tres de cada cinco empresas fueron objeto de ataques a la cadena de suministro de software en 2021

Fuentes: BlueVoyant, Anchore, ISACA

Global Cyber
soluciones integrales en ciberseguridad

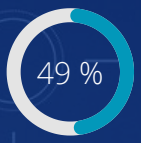
CONTACTO@GLOBALCYBER.CL

Cifras alarmantes

- SolarWinds en diciembre de 2020, impactó las cadenas de suministro de más de 18.000 organizaciones

- 1 de cada 5 proceso de evaluación de proveedores no incluye evaluaciones de ciberseguridad y privacidad.

- El 61% de las evaluaciones de riesgo no incluyen el riesgo de la cadena de suministro



- el 47 % de las organizaciones no realiza escaneo o pruebas de penetración en su cadena de suministro

- 39% de las organizaciones no ha desarrollado planes de respuesta a incidentes con proveedores en caso de un evento de ciberseguridad.

Fuentes: BlueVoyant, Anchore, ISACA

Global Cyber
soluciones integrales en ciberseguridad

CONTACTO@GLOBALCYBER.CL

ATAQUES A LA CADENA DE SUMINISTROS EN AMÉRICA

Este informe es un testimonio del trabajo que muchos países de América Latina están realizando para enfrentar los ataques a la cadena de suministro. Pero también es un manifiesto sobre la voluntad que tenemos para coordinar ese trabajo.
Las sociedades estamos avanzando en esa coordinación mucho más rápido de lo que nuestras legislaciones lo hacen.

Los equipos de seguridad TI en organizaciones y empresas están cada vez más abiertos a compartir información de inteligencia entre ellos. Lo que necesitamos es crear más instancias para fomentar ese intercambio y madurar nuestras estrategias de ciberseguridad con esos contenidos.
A ello debemos sumar los esfuerzos por crear concientización entre los usuarios y perspectivas ágiles de gestión en el trabajo de nuestros equipos, para que podamos hacer frente a las amenazas cibernéticas.

Los ataques a la cadena de sumintro, son una amenaza que trasciende a las sociedades y las iniciativas para enfrentarlos siempre serán insuficientes sino estamos unidos y bien coordinados.

Nuestro objetivo es fomentar una comunidad que madure para enfrentar a los ciberatacantes, atenuar su acción en América Latina y mitigar el impacto que pueda generar entre nuestras organizaciones.

Queremos agradecer a grandes amigos y profesionales que aceptaron la invitación ha colaborar en este trabajo.
Sus diferentes perspectivas y énfasis sobre el escenario del ransomware en cada uno de los países de América son un aporte muy relevante en el desafío que estamos enfrentando para mejorar nuestra ciberseguridad.

Global Cyber
soluciones integrales en ciberseguridad

Ataque a la cadena de suministro en Chile

Katherina Canales
Especialista en estrategias
de Ciberseguridad
CoFundadora y COO en GlobalCyber
r

La pandemia de COVID-19 impuso nuevas formas de gestión de los negocios y transformó las infraestructuras del trabajo, creando nuevos y positivos flujos de negocio en la cadena de suministros, pero con un importante costo en la ciberseguridad.

La digitalización y la virtualización de procesos aumentó la agilidad y capacidad de respuesta de las organizaciones y empresas para responder a las demandas en una circunstancia compleja, creando -o consolidando- una nueva cultura de intercambio electrónica.

El comercio en línea permitió la continuidad de los negocios y servicios, y hoy representan casi un cuarto del intercambio comercial global. Por un lado, este comercio electrónico simboliza el triunfo de las tecnologías de la información en medio de un contexto de adversidad pocas veces visto en la historia, pero por otro lado, también representa el enorme y universal desafío de ciberseguridad al que se exponen las organizaciones.

En los últimos 3 años las empresas y organizaciones han multiplicado su exposición a los riesgos y vulnerabilidades cibernéticas. Y si bien muchas de estas organizaciones cuentan con capacidades para enfrentar, contener y mitigar un incidente, estas no pueden declararse inmune ante los riesgos y vulnerabilidades, especialmente porque todas dependen en algún grado de proveedores de componentes y servicios de los que se desconoce su estrategia de ciberseguridad.

CONTACTO@GLOBALCYBER.CL

Esta ampliación y flexibilización de la cadena de suministros -forzada por la necesidad de los tiempos y justificada por sus beneficios de corto y mediano plazo- aumentan la superficie de ciberataques integrando vulnerabilidades en los flujos de negocio.

Pese al desafío de ciberseguridad, las empresas siguen confiando en las tecnologías blockchain para administrar sus bases de datos por la facilidad para registrar, seguir y comerciar de forma transparente y eficiente sus activos informáticos.

El debate sobre este punto adquiere una mayor intensidad porque se debe poner en la balanza el costo de adoptar e implementar las medidas de ciberseguridad. En ese sentido, la adopción de regulaciones aparece como un beneficio, pero también como una piedra de tope que retrasa la innovación y la inversión. A esto se suma que el mercado actual sufre una alta fragmentación, donde diferentes empresas, consorcios y productos operan bajo diferentes reglas y protocolos. Esto significa que los desarrolladores no pueden aprender de los errores y vulnerabilidades de otros, sin importar los riesgos en la integración en la cadena.

A ello se suma una serie de complejidades en la cadena que tienen relación con la corrupción, el incumplimiento de contratos, la falsificación de componentes, entornos regulatorios confusos, entre otros, que afectan a la ciberseguridad.

Pero otro factor que compromete la cadena de suministros es la poca comprensión de ésta. No todas las cadenas son iguales, o mejor dicho, todas son diferentes o únicas, y es necesario comprender el desafío en la dimensión específica de los negocios.

Eso también exige que las organizaciones cuenten con talentos y tecnologías que sean adaptables a necesidades, realidades y regulaciones en contextos específicos, capaces de adaptarse en la medida que cambia el desafío y del riesgo.

Eso también nos lleva al otro problema evidente, la amenaza. Las tácticas y técnicas de explotación en una cadena de suministro cambian con cada nueva tecnología.

No solo se trata de evaluar los problemas de agentes externos a una red, también de los internos y el ineludible factor humano de riesgo.

El intercambio con proveedores en cada una de las partes de la cadena de suministros representa un riesgo que se refleja en cifras. en el último tiempo el 40% de los ciberataques en las empresas tiene su origen entidades de la cadena de suministros.

las organizaciones y empresas deben avanzar en fortalecer sus equipos de seguridad informática que puedan comprender las amenazas cibernéticas de forma holística, así como en invertir en tecnologías que les permitan obtener una mayor visibilidad e implementar los protocolos decir seguridad cada uno de los intercambios.

Para chile y américa latina el desafío es doblemente importante. por un lado, nuestras economías son el sustento de muchos componentes y servicios que son necesarios en otros mercados, especialmente en materias primas. por el otro lado nuestro consumo tecnológico es cada vez más abundante y nuestras infraestructuras dependen del desarrollo tecnológico en otras latitudes, además de la comprensión de esas tecnologías por parte de nuestros especialistas. por eso es que la creación de equipos de coordinación de ciberseguridad local -pública y privada- Y la cooperación internacional son relevantes para comprender cómo se están enfrentando estos desafíos para adaptar las lecciones aprendidas y pre visualizar escenarios de amenazas futuras.

CONTACTO@GLOBALCYBER.CL

Ataque a la cadena de suministro en Brasil

Vagner Nunes
Cybersecurity Advisor
gtechne.com

Los ataques a la cadena de suministro han sido uno de los principales objetivos de los hackers en los últimos años. Pero el mayor ataque sufrido por una empresa brasileña, se hizo mundialmente conocido como el ataque a JBS en los Estados Unidos. El ataque pudo interrumpir la producción y la cadena de suministro de carne en Estados Unidos, Canadá y Australia.

El ataque de ransomware que afectó a la empresa se atribuyó al grupo ruso REvil, que según fuentes oficiales, JBS en Brasil pagó un rescate de 11 millones de dólares por el desbloqueo de la información de producción que el ataque secuestró.

También, según JBS USA, el atentado sigue siendo investigado por el FBI y la Casa Blanca afirma que el ataque se originó en Rusia. El presidente John Biden dijo que intercederá ante el presidente Vladimir Putin para que se lleve a cabo la investigación y se culpe a los responsables.

REvil es conocido como un tipo de empresa de ransomware como servicio (RAAS) por su forma de operar. Esto implica que los desarrolladores de ransomware reclutan a afiliados o socios para difundir su malware malicioso.

Un tipo común de ataque a la cadena de suministro son los proveedores de servicios gestionados (MSP). Tienen un amplio acceso a las redes de sus clientes, lo que es muy valioso para un atacante. Después de explotar el MSP, el cybercriminal puede expandirse fácilmente a las redes de sus clientes.

Además, según Check Point Software Technologies, en 2021 las organizaciones sufrieron un 50% más de ciberataques por semana en las redes corporativas en comparación con 2020, en todo el mundo. Las estadísticas sobre Brasil, por su parte, señalaron que, en promedio, las organizaciones del país fueron atacadas 1.046 veces por semana, un aumento del 77% comparando los períodos de 2020 a 2021.

Conclusión: Hoy en día, las plagas digitales como el malware y ransomware han traspasado el territorio económico y están en el centro del tablero político de todo el mundo, incluso entre los países que conforman el G7. La ciberseguridad es ahora una cuestión de soberanía nacional, y ya no es un tema meramente técnico o académico.

CONTACTO@GLOBALCYBER.CL

Ataque a la cadena de suministro en Ecuador

Mariam López
Especialista en ciberseguridad

Los ataques a la cadena de suministro están tomando relevancia dado que en la actualidad un ataque informático pone en riesgo a toda la infraestructura de una organización teniendo un gran impacto en la entrega de productos o servicios hacia sus usuarios finales, es un fenómeno que se ha incrementado a nivel global y en este escenario el Ecuador no se ha quedado fuera.

Es importante como en todo proceso productivo realizando una analogía al entorno de ciberseguridad que se tomen en cuenta todas las medidas que sean necesarias para garantizar la seguridad de los productos y servicios que son entregados que inciden en la provisión de productos o servicios de las organizaciones tal cual lo indican las mejores prácticas y normas ISO.

En lo que va del 2022, se han detectado ataques de ransomware que aprovechando la falta de actualización de sistemas operativos, utilizando formato binario ejecutable PE lograron afectar a infraestructuras críticas. Otro tipo de ataque se dio a través de un sistema que se encuentra distribuido en varias organizaciones para el control de accesos del personal con lo que los atacantes lograron tener acceso a información sensible a través de una escalada de privilegios.

Un punto de interés a analizar es el tipo de ataques que se dan por la integración de IT con OT, que permite a los atacantes tener acceso a equipos que no deberían estar expuestos por ser considerados críticos para las organizaciones se han identificado casos relacionados con generadores eléctricos, sistemas de control entre otros; y en un escenario similar la integración de equipos IoT con IT en los que a través de pantallas utilizadas para publicidad se han perpetrado accesos no deseados a sistemas críticos de organizaciones.

Con las afectaciones analizadas, es imperante que las organizaciones adopten esquemas de trabajo para validar las responsabilidades y dominios en cuanto a ciberseguridad en los procesos de contratación que deben cumplir los proveedores, se implementen mecanismos para la valoración del riesgo que se tiene al utilizar un producto o servicio de un proveedor y que se asuma como actividad la evaluación periódica tomando en consideración que siempre estará evolucionando. El tener políticas claras en las organizaciones para gestionar accesos e identidades, gestión de indicadores de compromiso en la red partiendo de una política de cero confianza que contemple el análisis del tráfico bajo un enfoque que toda actividad es maliciosa y que solamente las conexiones que pasen todas las validaciones se consideren como viables para que tengan acceso.

Finalmente siempre existirá la brecha generada por la carencia de estrategias de sensibilización en los usuarios finales, al no brindar la importancia que estas tienen se pueden generar por la falta de conocimiento libre acceso a datos sensibles sin controles, aceptación de conexión de equipos de usuario final sin registro lo que hace imperante que se fomente el desarrollo de habilidades en seguridad de la información.

Es relevante indicar que en el Ecuador se tiene el Código Orgánico de la Economía Social de los Conocimientos que se definen las tecnologías libres y formatos abiertos aplicando estos conceptos a software y hardware fomentando la migración a software de fuente abierta para las instituciones del sector público y el libre acceso en caso de contratación de software del código fuente. Lo que genera retos en la implementación de los controles para garantizar que los desarrollos sean seguros y no sean brechas de seguridad a futuro para las organizaciones que decidan tomar como base los códigos fuente de aplicaciones como base para desarrollos propios. También se cuenta con el Esquema Gubernamental de la Información en su versión 2.0 para aplicación en el sector público en la Administración Pública Central e Institucional, este esquema tiene como base los controles definidos en la norma ISO 27002 y gestión de riesgos.

CONTACTO@GLOBALCYBER.CL

Por otro lado para el sector financiero se cuenta con Normas Generales para las Instituciones del Sistema Financiero emitidas por la Superintendencia de Bancos y Seguros para la gestión y administración de riesgos, que contemplan a la gestión del riesgo operativo; y para el sector de economía popular y solidaria la Resolución No. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 emitida por la Superintendencia de Economía Popular y Solidaria que sobre la base de las normas ISO 27000 define la implementación del SGSI para ese sector.

"Los seres humanos somos confiados por naturaleza por lo que las organizaciones deben ser proactivas en lugar de reactivas mantener el monitoreo para no dejar ninguna parte de su infraestructura sin proteger y con esto prevenir ser las próximas víctimas de ataques cibernéticos"

CONTACTO@GLOBALCYBER.CL

Ataque a la cadena de suministro en México

Radamés Hernández Alemán
Incident Response Team Leader

Muchas personas en México aún recuerdan el 30 de abril de 2018, no sólo por haber sido un día de pago salarial para millones de personas, sino además se daba la oportunidad de pasar un fin de semana largo al haberse otorgado descanso junto al día 1° de mayo que se festeja el Día del Trabajo; ese día sin embargo, múltiples usuarios en redes sociales empezaron a preguntar qué estaba pasando con las transferencias bancarias, ya que varias de las aplicaciones estaban presentando ralentización en las operaciones, ya que no había forma de confirmar las transferencias interbancarias que por un lado generaba descuento y por otro, no se actualizaba el saldo.

Miles de llamadas de preocupación realizaban los usuarios a sus destinatarios: familiares, amigos, empresas, incluyendo a los propios bancos esperando una respuesta positiva; el Banco de México, autoridad central del país, había anunciado en marzo de 2018 que en virtud de algunos problemas con algunas aplicaciones de distintos bancos, había optado por habilitar los mecanismos alternos al Sistema de Pagos Electrónicos Interbancarios (SPEI) para asegurar las operaciones.[1]

Más de 300 millones de pesos estimó el Banco Central de México el importe de las transacciones (más de 14 millones de dólares americanos) que fueron sustraídas de cuentas concentradoras de bancos y casas de bolsa mexicanas, que significó un periodo de contingencia para las operaciones y derivó en un incremento a la regulación para las instituciones financiera.

[1] Fuente Banco de México publicación oficial https://www.banxico.org.mx/publicaciones-y-prensa/informes-trimestrales/recuadros/%7B86A498AE-5F8A-57CE-2C11-B5059AB9EB20%7D.pdf

Pocos días después del suceso, el Banco de México crea una nueva Dirección de Ciberseguridad para fortalecer, entre otros, los mecanismos de seguridad en el ámbito digital.[2]

En el informe enviado al H. Congreso de la Unión, el Banco Central explicó que de manera reciente al evento "...algunos participantes del SPEI experimentaron incidentes en sus aplicativos que utilizan para preparar sus órdenes de transferencia y conectarse al SPEI...", dejando que en claro que el SPEI no había sido blanco del ataque y que los aplicativos vulnerados forman parte de las operaciones de los bancos y casas de bolsa afectados.

Uno de los aspectos reveladores del citado informe es el hecho de que "personas no autorizadas" lograron crear transacciones válidas en el sistema, las cuales tuvieron éxito debido al acceso de información privilegiada en aplicaciones desarrolladas quizás por terceros afectando la cadena de suministro de software en torno al SPEI. Si bien no es un caso único, si fue emblemático debido al impacto mediático que suscitó.

Los cibereataques a la cadena de suministro se han posicionado entre las principales amenazas en 2022; las tendencias publicadas por la firma de consultoría e investigación tecnológica Gartner, Inc., las ubica en la tercera posición con una predicción que asegura que más del 45% de las organizaciones habrán sufrido un ataque de esta naturaleza, alcanzando el triple de lo observado en 2021.[3]

TOP TRENDS IN CYBERSECURITY, 2022
DE GARTNER

[2] Fuente: Medio Digital Expansión https://expansion.mx/economia/2018/05/18/caso-spei-la-cronologia-del-hackeo-al-sistema-financiero-mexicano

3] Fuente Sitio web oficial de Gartner, Inc. https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022

Ciberataques de alta escala como el de Solarwinds en 2020, que afectó a cientos de entidades de gobierno y empresas (incluyendo globales), provocaron consternación en la industria de software considerado como un evento de alerta de máxima seguridad; el incidente se originó debido a la supuesta actualización de Orión (un producto de Solarwinds) que después se identificó como un código malicioso (malware) de tipo troyano, dejando huecos de seguridad que aún se resienten en la comunidad.[4]

Ante estos eventos, las organizaciones han venido impulsando mejores prácticas a fin de evitar que la cadena de suministro se vea afectada, por una parte, las exigencias a los prestadores de servicios que provisionan software se han incrementado para que logren demostrar que operan con estrictas medidas que permitan alcanzar altos estándares de cumplimiento; sin embargo, si considera que la complejidad de su organización requiere de un mecanismo estandarizado basado en experiencias con buenos resultados; por otra parte, el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST por sus siglas en inglés) publicó una serie de conceptos, principios y estructuras que permiten minimizar los riesgos asociados ante eventos de esta naturaleza en el denominado "NIST Special Publication 800-207, Zero Trust Architecture"[5] una buena base sin duda si se busca fortalecer las capacidades de ciberseguridad de cualquier organización.

[4] Fuente CNN medio digital https://edition.cnn.com/2020/12/19/tech/solarwinds-hack-companies/index.html
[5] Fuente Instituto Nacional de Estándares y Tecnología (NIST) sitio web oficial. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

CONTACTO@GLOBALCYBER.CL

Ataque a la cadena de suministro en Colombia

Angela Cortés Hernández
Especialista en Seguridad Digital,
Coordinadora del COLCERT.

En Colombia hemos implementado estrategias con el objetivo de mitigar los riesgos del entorno digital definiendo lineamientos orientados hacia la gestión de los riesgos con un enfoque económico y social, para la implementación de la Política Nacional de Seguridad Digital, de esta forma, cobra mayor relevancia pensar en cómo se puede ver afectada la sociedad frente a la correcta prestación de los servicios esenciales en el país. Si bien es cierto hasta ahora venimos revisando el abordaje de la gestión de los riesgos desde el punto de vista de la cadena de suministros, hemos generado un trabajo que ha sido guiado por las recomendaciones de la OECD, siendo esto muy útil, para desarrollar o fortalecer los protocolos y guías relacionados con la adquisición de productos y servicios digitales en los diferentes sectores de la economía.

Por otro lado, entendiendo que en cualquier elemento de la cadena de suministro hay vulnerabilidades de diferente naturaleza que se deben mitigar, hemos generado actividades que se vienen adelantando desde los diferentes frentes de trabajo, además de esto, hemos desarrollado algunas iniciativas para mitigar los riesgos de seguridad digital relacionados con el uso de las tecnologías emergentes en el sector público, en donde, si bien no se abordan problemas puntuales frente a los productos, sí se han generado una serie de guías para gestionar la implementación de nuevas tecnologías revisando y adoptando estas recomendaciones, buscando mitigar fallas de seguridad que pueden estar presentes en el mercado.

Lo anterior cobra mayor relevancia, teniendo en cuenta casos como el del INVIMA[1], el cual nos hace generar una retrospectiva sobre la forma en que estamos identificando y protegiendo los servicios, esto teniendo en cuenta que, elementos que se vieron afectados en este caso no se tenían identificados mediante una correlación con la operación de la entidad y se generaron impactos a nivel de diferentes sectores productivos tales como represamiento de carga, demoras en el ingreso de elementos esenciales, retrasos en la expedición de permisos, posible desabastecimiento de productos, entre otros.

Finalmente, es importante reconocer los retos que trae la evolución en la transformación digital para fortalecer la visión de impacto de los riesgos de seguridad digital, teniendo en cuenta que se complejiza la prestación de los servicios; en este escenario se ve un número cada vez mayor de actores involucrados en la seguridad de la red lo cual deriva en la necesidad de definir de manera clara la distribución de responsabilidades, por otro lado, se van incluyendo más servicios que dependen de proveedores externos, aumentando así la superficie de ataque e impactando la cadena de suministro, entendiendo que aunque muchos de los riesgos tecnológicos pueden gestionarse de manera efectiva, las interacciones que se crean por el efecto de este nuevo relacionamiento, pueden abrir brechas con el aumento en la confianza en proveedores y vendedores externos, convirtiéndose en un elemento que aumenta las amenazas internas.

[1] Instituto Nacional de Vigilancia de Medicamentos y Alimentos - INVIMA

CONTACTO@GLOBALCYBER.CL

Ataque a la cadena de suministro Bolivia

Henry Hoyos Z.
Co Fundador de Computer Security Conference 8.8 Andina y Director Comercial del Holding Siscotec.

El mundo entero se encuentra sumergido en una crisis en la cadena de suministros, algo nunca antes visto desde la segunda guerra mundial. Pasando por la escases de chips, la gran crisis del transporte marítimo, la pandemia por el covid a lo que ahora se suma la guerra entre Rusia y Ucrania traen nubarrones de las cuales los especialistas en cadena de suministros deben tomar una especial atención.

Demos un rápido resumen sobre el concepto de cadena de suministros, la cual se define como; todo lo que se encuentra entre las materias primas y el producto final, lo cual abarca al proveedor de materias primas, los procesos de fabricación, la distribución y finalmente el consumidor.

¿Bolivia está preparada para ataques a la cadena de suministros?
Desde una perspectiva logística, Bolivia al ser un país mediterráneo depende en gran medida de este tipo de transporte a lo que se suma que sólo contamos con la autorización de una sola aerolínea carguera, a todo esto se suman los constantes bloqueos carreteros que ahondan la crisis de transporte la cual se ha elevado en un 328% en costos de transporte marítimo.

Desde un punto de vista de ciberseguridad cabe recalcar que Bolivia adolece de una ley de ciberseguridad de estado y un plan de DRP, lo que sumado a la falta de establecer pilares para un marco común de colaboración entre los estados de Sudamérica ante un posible ataque a la cadena de suministro pone en total indefensión al aparato de desarrollo productivo del país.

No menos importante, es que adolecemos de profesionales con experiencia y empresas locales especializadas en ciberseguridad industrial y seguridad OT con mención en Documentación Operativa OD-2061, normas ISO/IEC 27000, así mismo adolecemos de un laboratorio de pruebas de un organismo de certificación nacional (NCB), dichas certificaciones se definen para las siguientes evaluaciones, cada una de las cuales se aplica a una o más normas de la serie IEC-62443:

- Capacidad productiva
- Capacidad de procesamiento
- Aplicación de capacidades en el producto
- Aplicación de capacidades en el proceso
- Aplicación de capacidades en la solución.

Hoy en día los profesionales en ciberseguridad industrial deben estar especializados en la complejidad de la cadena de suministros la cual fue segmentada originalmente en tres elementos:

- Complejidad del producto
- Complejidad del proceso
- Complejidad de la red

Debemos tomar en cuenta que un ataque a la cadena de suministro también conocido como ataque a terceros o ataque a la cadena de valor, se produce cuando un atacante accede a la red de trabajo o de una empresa a través de sus vendedores o proveedores a través de la cadena de suministros por lo que algunos ataques son muy difíciles de rastrear, estos pueden producirse de muchas maneras tales como;

- Ataques mediante software, en Bolivia pocas organizaciones están incorporando listas de materiales de software (SBOM).
- Ataques mediante hardware, gran parte de la tecnología están basada en stateful siendo una minoría las basadas en stateless, así mismo es escaso encontrar tecnologías BDS (Bridge Detection Systems).
- Ataques mediante firmware, los más comunes son los bootkits para los cuales se requiere que las empresas migren de los EDR a los XDR y desde luego, siempre usar el sentido común.

Ataque a la cadena de suministro en Honduras

Dr. Denis Aguilar
Director de la facultad de Ingeniería de la Universidad Tecnológica de Honduras

Honduras es un país con un sinnúmero de desaciertos a lo largo de su historia, desde la independencia hace 200 años, pesan más las decisiones erradas que las correctas tomadas a lo largo de la historia.

Las Pymes representan el 90% de las empresas privadas y recién están haciendo relevo a la tercera generación gerencial (Si consideramos un promedio de vida por generación de 65 años. En estos dos siglos, los nietos de empresas longevas fundadas son dirigidas por los nietos milenian en algunos casos).

Tomando de referencia lo anterior, los migrantes a la era tecnológica (segunda generación de hondureños emprendedores o los hijos de fundadores), desconocen o no le prestan la atención debida a su mayor bien "la información digital", sus decisiones se basan en mecanismo administrativos tradicionales, basados en papel (Hardcopy). Al tecnificarse sus empresas, no invierten en proteger sus datos, su información histórica ahora digitalizada en bases de datos o Eres (Enterprise Resource Planning), en los improvisados datacenters. Sus sistemas informáticos son producto de una necesidad de sobrevivir en un mundo globalizado.

La idea de delito informático para estos gerentes que muchos de ellos son referentes y exitosos empresarios es básica, no ven lo inminente y peligroso para sus negocios.

CONTACTO@GLOBALCYBER.CL

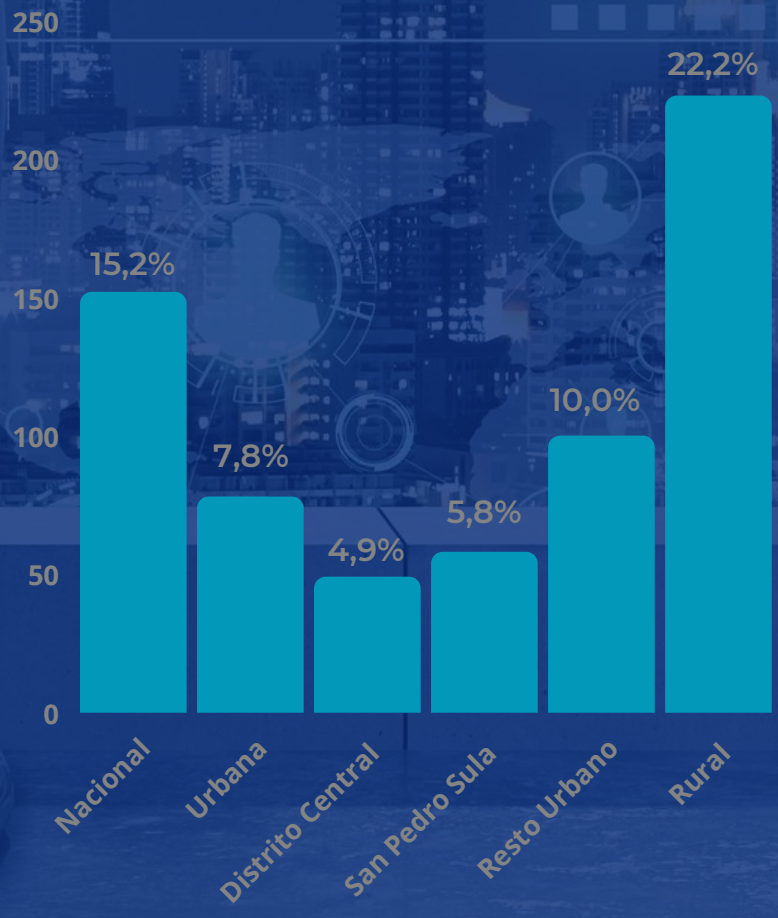
El sector público, corre la misma suerte el gobierno y sus instituciones usan deficientes sistemas informáticos y no presupuestan fondos para modernización y entrenamiento del personal. Salvo instituciones como el registro nacional de las personas RNP, el Banco Central, la Secretaria de Finanzas entre otras. Invierten en programas de ciberseguridad.

Educación en ciberseguridad.

Existe un gran número de empresas que desconocen sobre ciberseguridad y tampoco desean invertir recursos, más que los indispensables. Si bien es cierto un sector en el país que si lleva la vanguardia en ciberseguridad es el financiero y por la naturaleza de la banca siendo vulnerable si no se protege. Implementan infraestructura de vanguardia y planes de contingencia en ciberataques para proteger sus activos digitales bajo los estándares actuales.

La raíz de muchas situaciones adversas en Honduras en la falta de educación e inversión para adecuar a sus ciudadanos lo mismo sucede en las empresas público y privadas, no se destinan recursos para entrenar a sus colaboradores, la ciberseguridad es un riesgo de toman para ahorrar costos a expensas del peligro que representa. En los últimos años ya se han suscitado ataques ransomware proveniente de Rusia y Europa del este.

TASA DE ALFABETISMO POR DOMINIOS



FUENTE: HTTP://PROYECTOHONDURAS.ORG/ARCHIVOS/120

Global Cyber
soluciones integrales en ciberseguridad

CONTACTO@GLOBALCYBER.CL

Ataque a la cadena de suministro en Panamá

Silvia Batista
Coordinadora de CSIRT Panamá

También conocidos como "Ataques a terceros", son un tipo de ataque específico que tiene por objetivo afectar a todos aquellos vendedores y proveedores de un servicio en la cadena de suministro para afectar el ciclo de producción u operación de un servicio.

Sabemos que, aun teniendo la mejor postura de ciberseguridad, esta no es infalible, los actores maliciosos van a intentar entrar a la organización. Aun cuando las organizaciones realicen estrategias para defenderse de este tipo de ataques, los representantes de los terceros no realizan los mismos esfuerzos en sus empresas, dejando que los atacantes puedan entrar a las redes de la organización comprometiendo los sistemas y llegar al usuario final.

Panamá, en busca de fortalecer el marco legislativo ha presentado anteproyectos de ley en diferentes ocasiones. En el trascurso de los últimos 10 años, estos anteproyectos de ley se han presentado para modificar el código penal, que busca incluir otros tipos de delitos que van acorde a las nuevas tecnologías, y a su vez homologar con lo establecido en la convención de Budapest.

BlueVoyant, empresa de servicios de ciberseguridad, publicó a finales del 2021 los hallazgos de su segunda encuesta global anual sobre la gestión de riesgos cibernéticos de terceros. La encuesta reveló que el 93% admitió que ha sufrido una brecha de seguridad cibernética directa debida a vulnerabilidades en su cadena de suministro.

Comprendemos que, en nuestro país, cada día digitalizamos más procesos y llevamos hacia adelante más iniciativas de impacto nacional, involucrando a los ciudadanos. El incremento de diversos proveedores que brindan los servicios con múltiples beneficios que hacen muy valiosos su contratación, confiando una vez más en un tercero que puede ser elemento clave para mantener a salvo a nuestra organización como también puede poner en riesgo nuestra operación.

Debemos evaluar las empresas que forman parte de nuestra cadena de suministro y revisar continuamente los contratos y planes de trabajo de estas empresas, en búsqueda de mantener una relación contractual que proteja los intereses de nuestra organización.

Fuente: https://www.bluevoyant.com/resources/managing-cyber-risk-across-the-extended-vendor-ecosystem

CONTACTO@GLOBALCYBER.CL

Ataque a la cadena de suministro en Costa Rica

Ing. Alexander Vargas Céspedes, MSc
Decano de Ingenierías & TICs
Universidad Latina de Costa Rica

Hoy en día, todas las organizaciones, independientemente de su tamaño, reciben todo tipo de ciberataques, desde robo de información, encriptación de datos, bloqueo de accesos, corrupción de aplicaciones, borrado de información, sobrecarga de sistemas hasta la suplantación de identidad, cualquiera de ellos y otros más pueden afectar las cadenas internas y de suministros de las organizaciones provocando que el negocio quede paralizado o con una afectación mayor.

En el caso de Cosa Rica, esto ha sido evidente cada año, pues con base al informe de Fortiguard Labs de la empresa Fortinet vemos como en el 2019 el país tuvo 32 millones de intentos de ciberataques, para el 2020 alcanzaron los 201 millones de ciberataques, mientras que para el 2021 superaron los 2,500 millones de intentos de ciberataques, siendo el ransomware, fusión de los términos en inglés ransom (rescate) y software, el principal de estos.

El 18 de abril de este año, el grupo de ciberdelincuentes conocido como Conti dirigió a organismos e instituciones de Costa Rica un ciberataque masivo en forma de ransomware, el cual es un software malicioso que secuestra la información de un sistema (como datos, archivos o claves) para pedir un rescate.

El grupo ha atacado desde entonces a 30 instituciones costarricenses como el Ministerio de Trabajo, el de Ciencia, Tecnología y Telecomunicaciones, el Seguro Social o el Instituto Meteorológico Nacional, solicitando en principio un rescate de US$10 millones y luego por US$20 millones a cambio de cesar el ataque y devolver la información robada. El gobierno de Costa Rica se negó a pagar.

De estas instituciones del estado, la más afectada fue el Ministerio de Hacienda, donde los ciberdelincuentes entraron a los servidores afectando los sistemas de declaración de impuestos y de comercio exterior del país pertenecientes al Ministerio de Hacienda.

Así, las aduanas se paralizaron, dejaron de procesar los impuestos de las importaciones y exportaciones, se paralizaron los sistemas de recaudación y se suspendieron pagos de salarios de empleados del sector público. Un ejemplo claro de esto, fueron los pequeños comerciantes que no alcanzaron a emitir facturas porque los sistemas no respondieron de la forma adecuada y sin ese documento no consiguieron despachar o entregar sus productos.

Otra de las instituciones más afectadas por los ciberataques fue la Caja Costarricense del Seguro Social (CCSS), la cual se vio obligada a apagar todos sus sistemas informáticos para evitar el secuestro de sus bases de datos, lo que impactó los diversos servicios que brinda la entidad, por ejemplo, en el otorgamiento de citas, entrega de medicamentos, el uso de expedientes médicos y el registro adecuado de los nuevos casos del coronavirus COVID-19, justo en momentos en que Costa Rica enfrenta un repunte de infecciones.

De esta afectación nacional, surge la oportunidad de colaboración conjunta entre sectores para repelar los ciberataques, los gobiernos no pueden actuar solos y la participación de la comunidad académica y el sector privado son esenciales para desarrollar capacidades efectivas de resiliencia. Por otra parte, es importante incrementar la cooperación internacional con países de mayor experiencia y desarrollo en temas de ciberseguridad, y por último, debe existir un trabajo conjunto entre el sector público y privado en la generación de programas de sensibilización de cero confianza, donde tanto la ciudadanía como los colaboradores de estos sectores se encuentren alfabetizados y formen esa primera barrera de protección ante una amenaza de ciberataque.

Ataque a la cadena de suministro en el Perú

Aldo Villaseca Hernández
Cyber Security Consultant Base4 Security

Los ataques a la cadena de suministro son en la actualidad de una de las mayores amenazas que las organizaciones en el mundo deben afrontar.
Este tema no es nuevo y si revisamos un poco los antecedentes desde el año 2017:

- Shadow Pad (infectaron software de un proveedor usado para gestión de servidores).
- NotPetya (infectaron software de contabilidad).
- CCBkdr (software CCleaner infectado en la misma página web del fabricante).
- ShadowHammer (actualizaciones de BIOS, UEFI y software de fabricante de Laptops).
- Sunburst o Solorigate (vulnerabilidad explotada de Orion Platform de SolarWinds).

Es interesante al identificar las técnicas y posibles vectores de ataque las publicaciones de MITRE actualizadas que datan de abril 2018 al presente año. El compromiso de la cadena de suministro puede tener lugar en cualquier etapa de la cadena de suministro, incluyendo:

- Manipulación de las herramientas de desarrollo.
- Manipulación de un entorno de desarrollo.
- Manipulación de repositorios de código fuente (públicos o privados).
- Manipulación del código fuente en dependencias de código abierto.
- Manipulación de los mecanismos de actualización/distribución del software.
- Imágenes del sistema comprometidas/infectadas (múltiples casos de medios extraíbles infectados de fábrica).
- Sustitución de software legítimo por versiones modificadas.
- Venta de productos modificados/falsificados a distribuidores legítimos.
- Interdicción de envíos.

CONTACTO@GLOBALCYBER.CL

Global Cyber
soluciones integrales en ciberseguridad

A su vez en el informe de ISACA Supply Chain Security Gaps: A 2022 Global Research Report nos presenta un ranking de los riesgos mas relevantes a la cadena de suministros:

Top Supply Chain Risks

Quienes respondieron indicaron que estaban muy preocupados sobre los siguientes riesgos en su cadena de suministro:

1. Ransomware **73%**
2. Poor information security practices by suppliers **66%**
3. Software security vulnerabilities **65%**
4. Third-party data storage **61%**
5. Third-party service providers or vendors with physical or virtual access to information systems, software code or IP **55%**

Teniendo en cuenta todo lo anterior nos queda la reflexión de que el desarrollo de una Estrategia de Ciberseguridad para la Cadena de Suministros nos ayuda a estar mejor preparados para esta amenaza.

CONTACTO@GLOBALCYBER.CL

Medidas Organizativas sobre aspecto Contractual con el Proveedor	Medidas Organizativas y Técnicas en relación con proveedores
Revisar que el Nivel de Acuerdo de Servicio (SLA) propuesto por el proveedor esta alineado a necesidades del negocio (disponibilidad del servicio).	Tener un inventario actualizado de proveedores, identificando puntos de contacto y su criticidad en base al servicio ofrecido.
Confirmar que el proveedor cuenta con informes de auditoria independientes sobre el cumplimiento de certificaciones de seguridad de información, continuidad de negocio, gestión de servicios, gestión de riesgos y/o buenas prácticas aceptadas por la industria que presenta y/o dice cumplir.	Establecer criterios de evaluación que nos permitan garantizar que los terceros cumplen con las responsabilidades de ciberseguridad definidas en los contratos y acuerdos de confidencialidad.
Solicitar que el proveedor tenga un Plan de Continuidad de Negocio (PCN) y Plan de Recuperación de Recuperación de Desastres (DRP).	Realizar ejercicios de ciberseguridad probando los procedimientos sobre respuesta a incidentes con la participación de los proveedores y demás partes interesadas para asegurarse que conocen y cumplen sus roles e incorporar lecciones aprendidas como parte de la mejora continua.
Validar que el proveedor ofrece garantía por el producto o servicio en caso de fallas alineado a los requisitos de disponibilidad (cadena de suministros).	En caso de necesidad de acceso remoto por parte del proveedor, solo otorgarlo después de analizar los riegos y firmar un acuerdo de confidencialidad y aceptación de condiciones mínimas de conexión (por IP fija, con cliente VPN, lista de usuarios y aplicaciones autorizadas).
Incluir en el contrato se debe que se van a considerar medidas técnicas.	La actividad de los proveedores de servicios externos se debe supervisar para detectar posibles eventos de ciberseguridad.

CONTACTO@GLOBALCYBER.CL

Ataque a la cadena de suministro en Paraguay

Gabriela Ratti
Directora General de Ciberseguridad y Protección de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones de Paraguay

La cadena de suministro y las vulnerabilidades y/o oportunidades de explotación intrínsecos que están presentes en los diferentes componentes, procesos y actores de la cadena, hoy no son un riesgo sino una realidad: la cadena de suministro existe y no podemos evitarla, no existe ninguna organización que pueda afirmar ser 100% autosuficiente, ni en cuestiones tecnológicas ni en ningún aspecto.

Cada vez tenemos mas ejemplos de casos donde el vector de entrada de un ataque fue un tercero de la cadena, un actor de confianza, desde ataques genéricos y oportunistas, hasta ataques avanzados y sumamente dirigidos (APT).

Podemos hacer todo el esfuerzo para proteger al máximo nuestra organización, pero qué control tenemos sobre nuestros proveedores, incluso, aquellos que no somos conscientes que son nuestros proveedores, como por ejemplo los colaboradores voluntarios de librerías open source gratuitas.

En Paraguay venimos siguiendo de cerca los debates acerca de las posibles soluciones: exigir certificaciones a todo el mundo? Excluir a marcas/fabricantes poco confiables? Modelos zero-trust? Revisión de todos los códigos, exigencia de open source 100%?. La realidad es que probablemente no exista una solución única ni que resuelva completamente la problemática, ya que en gran parte se trata de cuestiones subjetivas y de confianza.

Debemos basarnos en algo para construir un sistema de información: un framework, una librería, un sistema operativo. Si ese "algo" ya se introdujo estando comprometido, como podríamos saberlo?.

Certificaciones como la TIA SCS 9001 son muy nuevas y podrían ayudar en estos procesos, sin embargo es muy probable que los tiempos de adopción sean todavía lentos. En el Paraguay, si bien no tenemos una respuesta definitiva, estamos evaluando qué tipo de controles o exigencias incluir, especialmente en los proyectos de infraestructuras críticas, para asegurar que éstas sean confiables también a lo largo de la cadena de suministro, buscando un balance entre la seguridad, la confiabilidad, los costos y la realidad de la madurez de las organizaciones.

Ataque a la cadena de suministro en la República Dominicana

Carlos Leonardo
Director CSIRT Nacional
República Dominicana

Los ataques a la cadena de suministro han sido una preocupación para los expertos en seguridad cibernética durante muchos años porque la reacción en cadena provocada por un ataque a un solo proveedor puede comprometer una red de proveedores. Según las investigaciones, el malware es la técnica de ataque a la que recurren los atacantes en el 62% de los ataques.

Las ciberamenazas han pasado a ocupar un lugar destacado en las preocupaciones sobre la seguridad de la cadena de suministro. Estas amenazas se refieren a vulnerabilidades en los sistemas de TI y software, como ataques de malware, piratería, acceso no autorizado, suplantación de certificados y puertas traseras inyectadas de manera intencional o maliciosa en el software propietario, de código abierto o adquirido que utilizan las organizaciones.

La seguridad de la cadena de suministro implica principalmente minimizar los riesgos del uso de software desarrollado por otra organización y asegurar los datos de la organización a los que accede otra en su cadena de suministro. Las organizaciones no pueden dar por sentado que el software que utilizan o adquieran es seguro.

Debido a que a menudo se requiere una estrecha colaboración entre empresas, proveedores y revendedores, las redes informáticas pueden entrelazarse o compartirse datos confidenciales. Esto puede resultar en una violación de una organización que afecta a muchas. En lugar de atacar al objetivo directamente, un ciberdelincuente puede atacar a una organización más débil en la cadena de suministro del objetivo y utilizar ese acceso para cumplir sus objetivos.

Uno de los casos de mayor impacto ha sido el de SolarWinds: en 2020, un grupo de hackers obtuvo acceso al entorno de producción de SolarWinds e incorporó una puerta trasera en las actualizaciones de su producto de monitoreo de red Orion. Los clientes que ejecutaron la actualización maliciosa sufrieron filtraciones de datos y otros incidentes de seguridad.

Esto tuvo repercusiones en todo el mundo, principalmente en América, donde es más utilizado esta plataforma de monitoreo de las redes. Al darse a conocer este evento, las organizaciones de la República Dominicana que la utilizan, realizaron escaneos y búsqueda de indicadores de compromiso, afortunadamente no se identificaros hallazgos de impacto.

En el país, desde el Centro Nacional de Ciberseguridad realizamos esfuerzos para que las organizaciones establezcan controles y mejores practicas para mitigar los impactos de las amenazas a la cadena de suministro.

- Mapear el panorama de amenazas

El primer paso es trazar un mapa completo de la cadena de suministro de software. En una organización grande, puede estar compuesta por una gran cantidad de proveedores de software, proyectos de código abierto, TI y servicios en la nube.

Utilizar herramientas automatizadas descubrir qué dependencias de software se esconden dentro de los proyectos de software de una organización y escanearlos en busca de problemas de seguridad y licencias validas. Así como realizar un inventario completo de todas las herramientas y servicios de terceros utilizados en los proyectos de software.

- Políticas y Gobernanza

Asegurarse de que los proveedores tengan políticas y procedimientos de seguridad estructurados, validados y certificados.

CONTACTO@GLOBALCYBER.CL

Los contratos entre la empresa y los proveedores deben establecer claramente los estándares y requisitos para el acceso y uso de datos para que la responsabilidad pueda asignarse con precisión en caso de violaciones. Los acuerdos deben exigir a los proveedores que notifiquen a la organización si se incumplen. También debe haber disposiciones claras para mitigar el riesgo cuando finaliza la relación con un proveedor.

- Privilegios de información de control

Es común que las empresas pongan datos a disposición de terceros, pero esto debe hacerse con la debida consideración. Cuantas más personas tengan acceso a los datos, más difícil será controlar y mitigar las amenazas.

- Reducir el riesgo en los ambientes de desarrollo

Muchos ataques a la cadena de suministro se centran en comprometer las estaciones de trabajo de los desarrolladores o los entornos de desarrollo. Una estación de trabajo de desarrollador, que tiene permiso para enviar código a la canalización es un "gran premio" para los atacantes.

Al final de día, es imprescindible implementar controles y auditoria de seguridad en todo el ciclo de vida de desarrollo de la organización.

CONTACTO@GLOBALCYBER.CL

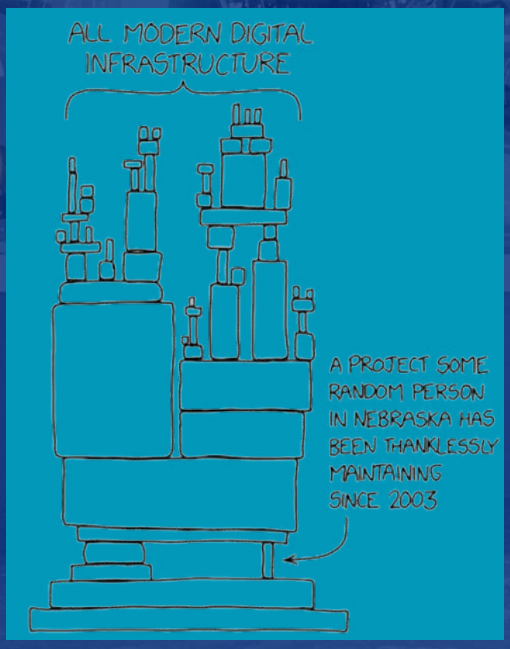
Ataque a la cadena de suministro en Uruguay

Mateo Martínez
Master en Seguridad Informática
Gerente de Krav Maga Hacking

Los ataques a la cadena de suministro se han vuelto cada vez más comunes en materia de ciberseguridad. Muchas veces se vuelve la forma más simple para los atacantes ya que se tienen menos controles, muchas veces sin aplicabilidad de regulaciones y menor nivel de auditoría. El enfoque es muy amplio, pero me gustaría fortalecer el concepto con los aspectos vinculados al desarrollo de software seguro.

Vulnerabilidades como Log4Shell nos han hecho repensar en todo el proceso de desarrollo de software, reflotando el concepto de Software Bill of Materials (SBoM). De hecho, muchas de las métricas centrales por las que se evalúa a un desarrollador de aplicaciones se benefician de la reutilización del código existente y las bibliotecas externas.

Está presente en alrededor del 96% de las aplicaciones y en promedio, el 79% de todo el código en uso proviene de bibliotecas de código abierto. 85% con componentes out-of-date de más de 4 años!



CONTACTO@GLOBALCYBER.CL

Global Cyber
soluciones integrales en ciberseguridad

Y tal como se muestra en el gráfico en forma graciosa, la realidad nos afirma que muchos de los componentes y tecnologías utilizados se basan en piezas de software mantenidas por individuos o grupos de individuos de confianza, que hoy en día son objetivos de ataques y engaños para que los atacantes pueda incluir piezas de código maliciosas en millones de descargas.
En promedio, una vulnerabilidad en un proyecto de código abierto tarda 54 días en agregarse a la Base de datos nacional de vulnerabilidades (NVD) después de ser divulgada públicamente.

Un atacante puede desarrollar un exploit para la vulnerabilidad un par de semanas después de la divulgación pública. Esto significa que los desarrolladores pueden continuar usando código vulnerable durante un mes después de que los ciberdelincuentes comiencen a explotarlo antes de que una entrada en el NVD indique que es necesaria una actualización.

¿Qué es la confusión de dependencia? (Dependency Confusion)

El problema de confusión de dependencias es una falla de diseño inherente en las herramientas de instalación nativas y los flujos de trabajo de DevOps que atraen las dependencias a su cadena de suministro de software. En este contexto, la confusión de dependencias se refiere a la incapacidad de su entorno de desarrollo para distinguir entre un paquete actual privado creado internamente en su compilación de software y un paquete con el mismo nombre disponible en un repositorio de software público.

¿Qué es typosquatting?

Los atacantes crean paquetes maliciosos que se parecen mucho a los de los paquetes legítimos y luego los cargan, por ejemplo, en el repositorio de descargas de NPM. Por ejemplo, si hay un componente de código abierto llamado "set-var" que se utiliza para configurar el entorno operativo de una aplicación creada para un marco específico, un equipo malintencionado podría crear un clon de ese proyecto llamado "setvar" que incluye su código malicioso.

SCA (Software composition Analysis) implica escanear una aplicación en busca de componentes de código abierto que contengan vulnerabilidades conocidas. Sin embargo, el 40% de los desarrolladores nunca realizan SCA o insisten en que nunca usan código de fuentes abiertas.

CONTACTO@GLOBALCYBER.CL

Recomendaciones

- Listar y analizar componentes del software
- Borrar código que no se utiliza (tenemos versionadores)
- Medir tiempo utilizado de las herramientas de seguridad en el pipeline
- Analizar los beneficios y el impacto de cada incorporación de herramientas
- Analizar la capacidad de filtrado de falsos positivos
- Más importante aún, ser muy crítico con la capacidad de detección de riesgos
- Incorporar métricas y dashboards ejecutivos de control y gestión SAST, DAST, SCA
- Establecer modelos de madurez y definir una hoja de ruta
- Analizar si los controles implementados son eficaces y eficientes periódicamente
- Los test automatizados NO sustituyen las actividades pruebas manuales
- DevOps suma muchos beneficios al negocio, pero es necesario pensar en DevSecOps
- Generar una cultura de DevSecOps integral

CONTACTO@GLOBALCYBER.CL

UNIDOS POR LA CIBERSEGURIDAD JUNIO 2022

Global Cyber

soluciones integrales en ciberseguridad