Número 98 | Enero 2025

NTT DATA

Radar

El magazine de ciberseguridad

Fortaleciendo la cadena de suministro: Ciberseguridad para la gestión de riesgos de terceros

Por María Pilar Torres Bruna

Uno de los desafíos de una organización o un CISO a la hora de definir una estrategia de ciberseguridad es definir el perímetro a proteger. Migrar parte de la organización a la nube desdibujó un perímetro que estaba bien definido, y el teletrabajo incrementó esa percepción. Hay un tercer factor clave en la ciberseguridad de nuestras organizaciones, y son nuestros terceros. Algunos de ellos son críticos para poder realizar nuestro negocio y para ello, sus sistemas se integran en mayor o menor medida con los nuestros. ¿Cómo aseguramos que no suponen un nuevo vector de ataque para nosotros?

La "Seguridad en terceros" se refiere a la gestión de los riesgos asociados con los proveedores, socios y cualquier entidad externa que tenga acceso a los sistemas, datos o recursos críticos de una organización. Para conseguir una correcta gestión de estos riesgos, hay varios roles, además del CISO, que deben ser conscientes de su importancia y que tienen que definir controles o conocerlos para que estos se implanten. Los departamentos de compras, de negocio, u otros departamentos específicos, como jurídico, deben incorporar controles de seguridad en sus servicios y entenderlos como no negociables.

Los acuerdos contractuales permiten establecer las bases de seguridad que la compañía compradora de servicios necesita para proteger su información y su negocio, y ayudan a definir claramente las responsabilidades y expectativas de ambas partes en cuanto a la protección de datos y la gestión de riesgos. Además, los acuerdos contractuales facilitan la gestión de la relación con los proveedores, asegurando que se mantenga un nivel adecuado de seguridad de la información a lo largo del tiempo. Esto debe comprobarse mediante auditorías periódicas al tercero.

Finalmente, es importante establecer una revisión y actualización periódica de los contratos para adaptarse a nuevos riesgos y cambios en la normativa. Igualmente, que los proveedores entiendan los mínimos de seguridad que les van a exigir les permite dimensionar los servicios de una forma mucho más precisa.

¿Y por qué esto es importante en este momento? Se considera que los ataques a la cadena de suministro se convertirán en una de las principales amenazas en este año que comienza, el 2025.

Escalará el número de ataques identificados, sobre todo en infraestructura crítica y sectores industriales, así como a entornos en la nube mediante la implementación de gusanos nativos específicamente desarrollados para entornos de este tipo.

Actualmente, ya existe un gran número de ataques a organizaciones que se dan a través de los terceros. Las grandes compañías hacen una inversión grande en ciberseguridad, y ya es más difícil explotar un vector de ataque. Sin embargo, sus proveedores o partners pueden ser empresas más pequeñas y que quizá disponen de una menor inversión en ciberseguridad. En ese caso, un camino para los atacantes puede ser entrar a una de estas empresas y una vez dentro, escalar para llegar al objetivo.

Por estos motivos, hemos querido empezar este año hablando de la ciberseguridad en la cadena de suministro. El equipo de NTT DATA espera que sea de interés y deseamos a nuestros lectores un feliz 2025.

Maria Pilar Torres Bruna
Cybersecurity Director

La creciente amenaza de las filtraciones de datos en un mundo digitalizado

Cibercrónica por José Cianci

La evolución de las tecnologías ha convertido la información en el activo más valioso de la era digital, lo que la hace un objetivo atractivo para los cibercriminales. Estos atacantes emplean técnicas como el phishing, vishing y smishing, utilizando datos aparentemente legítimos, que a menudo provienen de filtraciones previamente liberadas o vendidas en la dark web, para engañar a las víctimas y obtener beneficios económicos o facilitar un vector de ataque en contra de la seguridad o reputación de su objetivo.

La protección de la confidencialidad, uno de los pilares de la seguridad de la información, es indispensable para prevenir incidentes de este tipo, los cuales no solo afectan a las organizaciones responsables, sino que también comprometen la privacidad individual de los usuarios. Estos eventos demuestran cómo los ataques cibernéticos pueden afectar la confianza en el tratamiento y la protección de los datos personales, así como en el cumplimiento de las políticas y leyes vigentes en cada país sobre la protección de datos. Este tipo de incidentes ponen en riesgo la seguridad económica de millones de personas y la reputación y estabilidad financiera de las organizaciones, que enfrentan posibles sanciones legales y daños a su imagen, por ello se destaca la importancia de reforzar las medidas de protección y garantizar el cumplimiento normativo para asegurar la confidencialidad de los datos.

Siguiendo los incidentes recientes, el 1 de diciembre de 2024, la Agencia Tributaria de España fue aparentemente víctima de un ataque de ransomware perpetrado por un grupo de hackers autoclamados Trinity. Los ciberdelincuentes afirman haber robado 560 gigabytes de datos privados y confidenciales; amenazan con 38 millones de dólares de extorsión, que se debe pagar como cripta para evitar la publicación de la información. A pesar de que la Agencia Tributaria ha declarado que no se han producido fugas de seguridad ni irregularidades en sus sistemas, la preocupación por la seguridad de los datos de los contribuyentes se ha intensificado y las capacidades de las instituciones públicas para resistir los ciberataques se han cuestionado.

Los ataques de doble extorsión, es decir, el cifrado y la publicación de datos sensibles, demuestran una tendencia ascendente en España. Las autoridades están investigando el caso y las medidas de seguridad cibernética se incrementarán para evitar ataques futuros.

A finales de octubre de 2024, Interbank, una de las principales entidades bancarias de Perú, enfrentó una grave filtración de datos que expuso la información de tres millones de clientes. Este incidente, originado por un acceso indebido a datos sensibles como saldos, números de tarjetas de crédito y credenciales API, desató una ola de pánico entre los usuarios, generando temores sobre la seguridad de sus ahorros y provocando un pánico bancario sin precedentes. Mientras las investigaciones apuntan a posibles fallos internos y la intervención de ciberdelincuentes extranjeros exponiendo la falta de una infraestructura robusta de ciberseguridad.

Para el mes mayo de 2024, Landmark Admin, una compañía que brinda servicios administrativos a importantes aseguradoras en Estados Unidos sufrió un ciberataque que expuso la información personal de más de 800.000 personas. Los atacantes accedieron a datos sensibles, como números de Seguro Social, licencias de conducir, pasaportes, información bancaria, médica y detalles de pólizas de seguro. Aunque la compañía detectó actividad sospechosa el 13 de mayo y tomó medidas para proteger sus sistemas, los atacantes lograron infiltrarse nuevamente el 17 de junio. Como respuesta, Landmark Admin ha implementado protocolos de cifrado de datos más fuertes y otras mejoras de seguridad en su infraestructura, restaurando los sistemas comprometidos y colaborando con las autoridades para investigar el ataque.

Adicionalmente, ofreció a las personas afectadas 12 meses de monitorización de crédito gratuito y servicios de protección contra el robo de identidad, junto con orientación adicional para prevenir fraudes. Aunque la compañía no ha identificado al grupo responsable del ataque ni ha sido atribuida por ningún colectivo de ransomware conocido, este incidente evidencia los riesgos y desafíos a los que se enfrentan las empresas que gestionan información sensible.

Iniciando el año 2024, Telefónica ha investigado un posible caso de filtración de datos que afectaría a 120.000 clientes y empleados. Según las investigaciones preliminares, la información comprometida incluye nombres, direcciones, correos electrónicos y números de teléfono, aunque no se han identificado datos sensibles como cuentas bancarias o contraseñas. La empresa detectó la supuesta brecha en marzo de 2024, y los datos habrían sido ofrecidos en foros en línea por ciberdelincuentes, quienes afirmaron que no tenían uso para ellos y decidieron ponerlos a la venta. La filtración podría estar relacionada con vulnerabilidades en un proveedor externo.

Telefónica trabaja para confirmar la autenticidad de la información y tomar medidas correctivas. Este incidente se suma a antecedentes de ciberseguridad en la compañía, incluyendo un ataque global en 2017 y otro en 2022 que afectaron partes de su infraestructura y configuraciones de routers.

Finalmente, un incidente masivo ocurrió el año pasado, cuando más de 760.000 registros de empleados de importantes empresas como Bank of America, Koch, Nokia, JLL, Xerox, Morgan Stanley y Bridgewater fueron filtrados en línea, exponiendo información sensible que podría tener graves consecuencias. Los datos, que incluyen nombres, correos electrónicos, números telefónicos, cargos laborales e incluso los nombres de altos directivos de las compañías, provienen de un hackeo masivo ocurrido el año anterior. En ese hackeo, un grupo de ciberdelincuentes, vinculado a la banda rusa Cl0p, aprovechó una vulnerabilidad de zero-day en el software de transferencia de archivos MOVEit para robar información de miles de organizaciones.

El ataque afectó a casi 100 millones de personas y 2.800 empresas, y la información ahora filtrada es considerada valiosa por los ciberdelincuentes, ya que permite realizar ataques de ingeniería social, como el phishing o el robo de identidad, al tener acceso a datos organizacionales detallados.

Cada uno de estos casos pone en evidencia no solo la creciente amenaza de las filtraciones de datos, sino también la vulnerabilidad ante ataques cada vez más sofisticados. Los ciberdelincuentes, al aprovechar las fallas en la seguridad de las organizaciones, no solo roban información, sino que afectan la confianza pública y comprometen la estabilidad económica de las víctimas.

Este panorama muestra la necesidad urgente de reforzar las políticas de ciberseguridad, adoptar tecnologías más avanzadas y fomentar la educación de clientes y empleados acerca de los riesgos cibernéticos. La protección de datos no es solo una obligación legal, sino una necesidad estratégica para mitigar riesgos y asegurar que la confianza y la seguridad no se vean comprometidas.

José Cianci Pacheco
Cybersecurity Junior Engineer

La importancia de los proveedores y la cadena de suministro en la ciberseguridad

Artículo por Julissa Calderón

La ciberseguridad en los proveedores y la cadena de suministro es un aspecto que cobra relevancia en las compañías en el ámbito de la ciberdefensa y ciber resiliencia. En los últimos años los ataques provocados por la exposición de información en terceros se han incrementado. Los ciberdelincuentes hoy en día ven a los proveedores de confianza como un medio importante para llegar al objetivo final y buscan vectores de ataque que permitan vulnerar datos o poner en riesgo la organización. Por ello es crucial que las compañías se encuentren preparadas mediante la seguridad en las relaciones con sus proveedores.

¿Existirá alguna compañía que no cuente con servicios subcontratados con terceros?

Si bien las compañías soportan los procesos core de sus negocios, muchas veces necesitan de proveedores especializados en determinados servicios/productos para soportarse en ellos y engranarlos como parte de su cadena de valor. Por supuesto, no todos los proveedores soportan procesos críticos de las compañías, pero se tienen algunos que sí, y que incluso por ello se convierten en socios estratégicos.

¿Qué compañía no comparte información de su negocio en el marco del contrato con sus proveedores?

Los proveedores pueden otorgar bienes o servicios, sobre lo cual, según el marco de su contrato y alcance, necesitan conocer información de la compañía. En ciertos casos además de conocerla, deben trabajar con ella, lo que supone tener un acceso diferente. En el ámbito tecnológico, algunos terceros para efectuar sus labores necesitan acceder a la red de la compañía e incluso a sistemas de información, por lo que es importante que las medidas de seguridad en proveedores estén establecidas, se cumplan y sean monitorizadas por la organización asegurándose que las medidas aplicadas son las similares o incluso mejores a las que se determinan en la misma empresa.

¿Todas las compañías cuentan con políticas de seguridad establecidas y compartidos con sus proveedores, en los cuales se cuide la información y el entorno en el cual se comparte?

No todas las organizaciones efectúan esfuerzos en establecer condiciones de seguridad y ciberseguridad en sus acuerdos con los proveedores, en algunos casos sólo determinan cláusulas generales en los contratos a fin de cuidar la confidencialidad, integridad y continuidad de información en el marco del producto o servicio, sin embargo, vemos que a pesar del riesgo que representa, numerosas compañías carecen de medidas adecuadas de ciberseguridad las cuales se controles y monitoricen.

¿Qué consideraciones se deben tener respecto a las medidas de ciberseguridad?

1. Respecto a la arista de ciberseguridad es importante que se puedan determinar aquellos proveedores que, por el servicio brindado, cumplen con alguno de los siguientes aspectos:

    - Proveedores que soportan procesos críticos del negocio.
    - Proveedores que acceden a activos de información de la compañía.
    - Proveedores que son custodios de activos de información.

    El tener identificados a estos proveedores es un primer paso para establecer y aplicar medidas de seguridad según su participación e implicancia en la seguridad y ciberseguridad de la compañía.

2. Establecer medidas de seguridad de información y ciberseguridad que deben cumplir los proveedores en todo el ciclo de vida: en la contratación, en el despliegue del servicio u operación y en el cierre del contrato.

Para esto es importante engranar estas especificaciones con los procesos de adquisición y compras, así como con aspectos legales que se analizan como parte de los contratos. Es relevante tomar en cuenta los siguientes aspectos principales:

- Límites de acceso.
- Establecer canales de comunicación seguros.
- Seguridad de dispositivos de conexión.
- Planes de respuesta a ciber incidentes.

3. Aplicar análisis de riesgos de seguridad de información y ciberseguridad a aquellos proveedores que se requiera. Aquí se recomienda que se inicie con proveedores que soporten procesos críticos y/o que se relacionen con activos de información de mayor relevancia para la compañía.
4. Monitorizar el cumplimiento de las medidas aplicadas por los proveedores, sean medidas técnicas, legales u organizativas en relación a la ciberseguridad, a fin de tener claridad de su cumplimiento y efectuar recomendaciones en caso de que amerite.
5. Concientizar a los proveedores respecto a su participación e importancia de su labor en el cuidado de la ciberseguridad y seguridad de información.

Existen varios frameworks y/o normativas internacionales que establecen estándares que se pueden tomar en cuenta para mejorar la protección en las relaciones con los proveedores, por ejemplo, la norma ISO 27001:2022 incorpora ciertos aspectos de control para garantizar la seguridad en las diferentes capas de las Tecnologías de Información y comunicaciones. Asimismo, la NIST SP 800-161r1, contiene especificaciones para la gestión de riesgos en la cadena de suministro de ciberseguridad.

Las amenazas cibernéticas se encuentran en constante evolución, por lo que es fundamental que las compañías estén alertas y se tomen medidas proactivas para proteger sus cadenas de suministro de los riesgos de ciberseguridad.

Julissa Calderón Loayza
Cybersecurity Expert Associate

Fortaleciendo los programas de seguridad en aplicaciones mediante Inteligencia Artificial Generativa

Artículo por Martín Bedoya

La seguridad en aplicaciones viene en auge desde que la industria del software descubrió que mover el aseguramiento del software a la izquierda, en el largo plazo, es más eficiente que solamente ejecutar pruebas. La seguridad en aplicaciones se refiere a prácticas y herramientas diseñadas para proteger el proceso de desarrollo de software contra amenazas, asegurando que desde el principio se incluyan controles para proteger la confidencialidad, integridad y disponibilidad.

Un programa de seguridad en aplicaciones se implementa integrando controles en el ciclo de vida del software, empleando herramientas automatizadas, formando los equipos y monitoreando constantemente para detectar y mitigar vulnerabilidades. La estrategia depende de cada organización, de su apetito de riesgo, de su proceso de desarrollo y del presupuesto destinado.

Implementar un programa de seguridad en aplicaciones resulta un desafío para las organizaciones debido a la falta de recursos especializados, la resistencia al cambio y la necesidad de equilibrar seguridad con tiempos de entrega. En términos de gobierno, en un programa de seguridad en aplicaciones se suelen emplear dos estrategias: Por un lado, se integran profesionales de seguridad a las células de desarrollo para que soporten las actividades de aseguramiento, esto resulta altamente efectivo pero costoso de mantener y escalar.

Por otro lado, se suelen ofrecer capacidades de seguridad específicas que son activadas bajo demanda por los equipos de desarrollo, este modelo, aunque es más barato y escalable, pierde agilismo y traslada parte de las actividades de seguridad a los mismos integrantes de la célula. Independientemente de la estrategia implementada, los programas de seguridad en aplicaciones pueden ser optimizados utilizando inteligencia artificial.

La inteligencia artificial generativa ofrece la posibilidad de optimizar las actividades de seguridad en cada fase del ciclo de vida del software, automatizando la detección de amenazas, mejorando la precisión de los análisis de riesgo, identificando vulnerabilidades, sugiriendo remediaciones equilibradas y, por supuesto, disminuyendo el sesgo de los profesionales de seguridad.

Mediante el uso de inteligencia artificial generativa, los profesionales de seguridad evalúan las historias de usuario con el fin de identificar riesgos potenciales, priorizarlos y recomendar medidas de mitigación, optimizando la planificación de la seguridad desde las primeras fases del desarrollo. Este proceso permite incrementar la cantidad de historias de usuario evaluadas por profesional, mejorando sustancialmente la capacidad de los programas de seguridad en aplicaciones.

Asimismo, la inteligencia artificial generativa permite industrializar los modelos de amenazas a partir de historias de usuario o diagramas de software, disminuyendo el entendimiento del negocio y reduciendo significativamente el tiempo empleado por los consultores para identificar potenciales amenazas, lo cual, en el largo plazo, permite atender una mayor demanda de células de desarrollo.

Por último, el análisis estático de código fuente basado en inteligencia artificial generativa posibilita la identificación patrones inseguros en el código, que pueden no ser detectados por herramientas tradicionales, a su vez proporcionan explicaciones detalladas y ofrecen recomendaciones para corregir vulnerabilidades, disminuyendo la deuda técnica y mejorando el time to market.

Uno de los grandes retos de los programas de seguridad en aplicaciones es la disminución del sesgo, comúnmente los profesionales con formación defensiva tienden a asegurar el software a partir de controles, mientras aquellos con experiencia ofensiva tienden a concentrarse en los ataques. La inteligencia artificial permite reducir este sesgo siempre y cuando se estructure efectivamente la interacción entre el profesional y el modelo generativo.

La inteligencia artificial se ha convertido en una herramienta esencial para fortalecer la seguridad en aplicaciones, ofreciendo capacidades para automatizar procesos complejos y reducir errores humanos. En un mundo donde las aplicaciones crecen en volumen y complejidad, es fundamental enfrentar amenazas emergentes con rapidez y precisión. Integrar inteligencia artificial en el aseguramiento del ciclo de vida del software permitirá a las organizaciones abarcar un mayor ecosistema de aplicaciones y mejorar su postura de seguridad.

Martín Bedoya Rodríguez
Cybersecurity Expert Engineer

Ciberseguro como atajo a los *supply chain attacks*

Tendencias por Jose Cárdenas

La complejidad de la seguridad en la cadena de suministro radica en la interconexión y dependencia de múltiples actores, tecnologías y locaciones que componen las cadenas modernas. Esta complejidad se intensifica con la globalización, ya que los componentes provienen de diversas regiones, cada una con normativas de ciberseguridad distintas y riesgos geopolíticos potenciales. Esto requiere enfoques sólidos, como la utilización de ciberseguros para reducir las consecuencias financieras y operativas de un ataque.

Agencias como Cybersecurity Ventures estiman que el costo global anual de los ataques a la cadena de suministro de software para las empresas llegará a la impresionante cifra de 138 mil millones de dólares para 2031, frente a los 60 mil millones en 2025 y los 46 mil millones registrados en 2023. Con estas proyecciones, parece que los ciberdelincuentes podrían estar superando a las grandes empresas en términos de ganancias... mientras nosotros seguimos, una vez más, pagando las consecuencias.

Ciberseguro

Ante este costo de impacto muy creciente para los siguientes años, la necesidad de adquirir un ciberseguro sobre la inversión de capital y tiempo para asegurar los sistemas de las empresas toma más fuerza. Diversas compañías ofrecen en su parrilla de servicios los ciberseguros, la cual busca dar un respiro y tranquilidad a las empresas con un menor impacto ante un ataque cibernético como ransomware o un DDoS. Sin embargo, los términos del ciberseguro cambian conforme más víctimas tenemos.

Primas más caras

El incremento en las primas de los ciberseguros responde a la creciente complejidad de los ataques cibernéticos. Las aseguradoras han ajustado las primas para cubrir los mayores costos derivados de estos incidentes. No obstante, este aumento en el costo y la protección ha obligado a las empresas a demostrar que cuentan con medidas de seguridad robustas, como la autenticación multifactor y protección contra ransomware, para poder acceder a condiciones competitivas.

Aumento de exclusiones en los ciberseguros

Aunque las pólizas de ciberseguros pueden cubrir muchas cosas, hay algunos incidentes que tienden a no cubrir como:

- **Ingeniería social:** dado que los ataques de ingeniería social como el phishing manipulan a las personas para que comprometan la ciberseguridad desde dentro, las pólizas cibernéticas no siempre cubren estas pérdidas.
- **Ataques de Estado:** muchas políticas cibernéticas consideran que estos ataques son actos de guerra y no los cubren.

- **Ciberataques que aprovechan una vulnerabilidad conocida:** si los ciberatacantes explotan un fallo que la empresa conocía, pero no corrigió, muchas pólizas cibernéticas negarán la afirmación.

Segmentación de los ciberseguros

La segmentación de los ciberseguros se ha convertido en una tendencia clave debido a la diversidad de riesgos que enfrentan distintos sectores. En lugar de ofrecer pólizas genéricas, las aseguradoras están ajustando sus productos a las necesidades específicas de cada industria, como salud, banca o comercio electrónico. Por ejemplo, las empresas del sector salud requieren protección contra el robo de datos médicos, mientras que las organizaciones tecnológicas necesitan cobertura para la pérdida de propiedad intelectual.

Este enfoque permite a las aseguradoras proporcionar coberturas más precisas y eficaces, alineadas con los riesgos particulares de cada cliente, lo que también ayuda a optimizar el costo de las primas.

Aseguradoras más estrictas

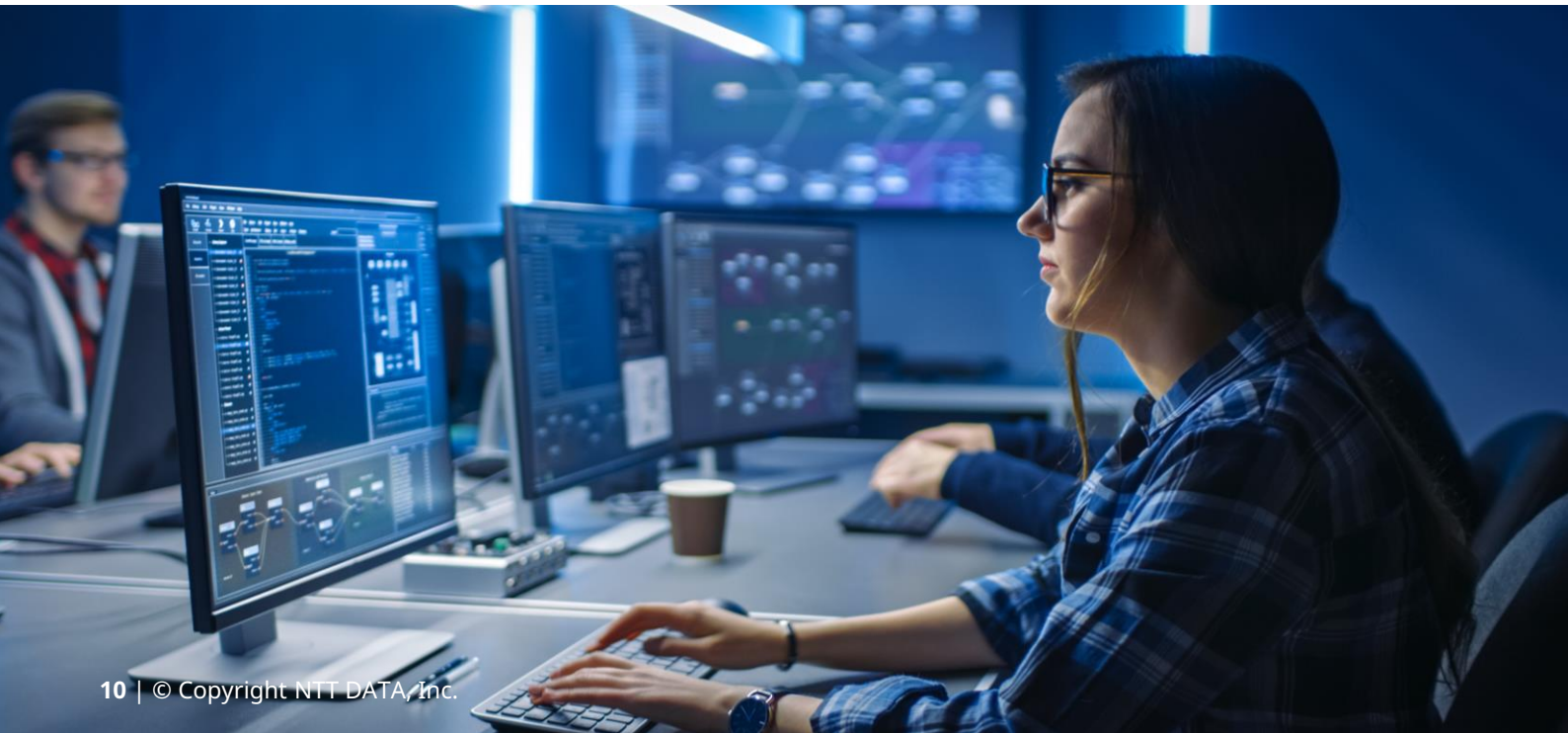
Las aseguradoras están implementando requisitos más estrictos. Algunas incluso no ofrecen una cotización de seguro si la empresa no cuenta con medidas de seguridad como autenticación multifactor, cifrado de datos, Zero Trust o políticas similares.

Además, algunas compañías de seguros están adoptando un enfoque más consultivo, brindando a los asegurados y dueños de negocios acceso a herramientas de seguridad y proveedores de servicios que les ayuden a fortalecer su posición en ciberseguridad.

Conclusión:

Las organizaciones deben ajustarse a un entorno de amenazas en constante cambio, lo que implica no solo contar con una estrategia de seguridad sólida, sino también incorporar soluciones como los ciberseguros. Estos seguros se están consolidando como una herramienta clave para reducir los riesgos financieros y operativos derivados de los ciberataques, aunque su eficacia depende de que las empresas implementen las medidas preventivas adecuadas. Además, la colaboración con aseguradoras y proveedores de servicios de seguridad se está volviendo un elemento crucial para reforzar la resiliencia de las organizaciones ante los ciberataques.

Jose Cárdenas Camacho
Cybersecurity Analyst



Phishing a través de DocuSign: distribución de malware desde fuentes de confianza.

Tendencias por Samuel Santos y Nicolas Fernandez

A comienzos del pasado mes de noviembre, los investigadores de Wallarm dieron la voz de alarma sobre una reciente táctica de phishing en la que grupos de ciberdelincuentes estarían explotando la API de la compañía DocuSign, una conocida plataforma de firma de documentos y envío de facturas electrónicas.

Los atacantes habrían encontrado un modo de enviar correos electrónicos que, al provenir de la propia plataforma legítima, imitan con precisión las facturas y notificaciones que se envían regularmente.

Según fuentes como Trellix, este ciberataque se estaría produciendo especialmente en Japón, Norteamérica, Oceanía y Centro Europa, y estaría distribuyendo una versión modificada del malware conocido como Remcos RAT cuyo fin es la ejecución remota de comandos en la víctima.

¿En qué consiste el ataque?

Este esquema se basa en el envío masivo de correos de DocuSign con documentos de Office manipulados. Estos archivos contendrían objetos OLE (Object Linking and Embedding), que llaman a realizar parte del proceso de carga del documento desde una fuente externa controlada por el atacante.

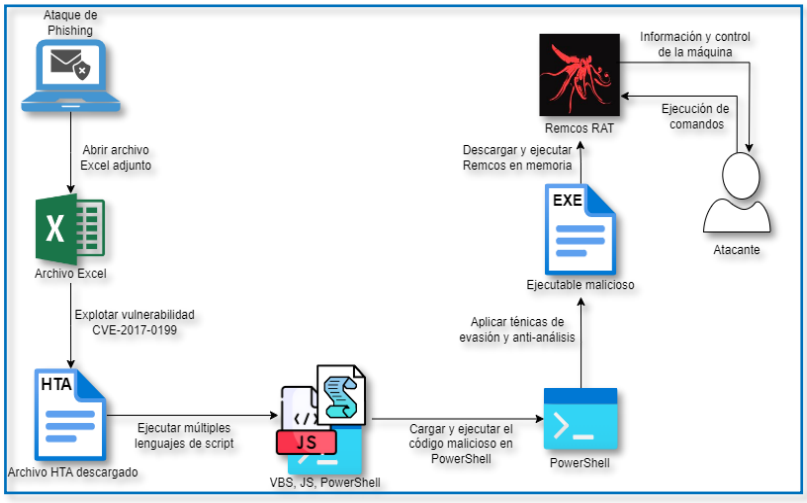
Mediante esta carga externa del documento, los ciberdelincuentes se aprovechan de la vulnerabilidad pública CVE-2017-0199 contenida en algunas versiones del paquete Office para realizar la ejecución de un fichero HTA (HTML Application) ofuscado en distintas capas de código JavaScript, Visual Basic y PowerShell.

El objetivo final de este código será ejecutar una consola de PowerShell que, aplicando diferentes técnicas de evasión, ejecutará una variante del software malicioso conocido como Remcos RAT, permitiendo a los ciberdelincuentes conectarse a través de un Command & Control a la maquina víctima. Desde ese servidor, los ciberdelincuentes podrán controlar el dispositivo infectado, ejecutar comandos, moverse lateral o verticalmente dentro de la red, y extraer información sensible.

¿Por qué es efectivo este ataque?

El punto fuerte de este vector de ataque es el abuso de la API legítima de DocuSign, y refleja una evolución en el phishing tradicional: en lugar de engañar al usuario a través de servidores maliciosos y correos con falsa apariencia de legitimidad, los atacantes ahora usan plataformas de confianza como vectores de ataque, engañando a sus objetivos con comunicaciones que parecen totalmente auténticas.

Al enviar correos a través de DocuSign, los ciberdelincuentes logran que sus mensajes sean considerados como legítimos por los filtros de seguridad.



Esto les permite evadir mecanismos tradicionales de detección de phishing y aumentar la tasa de apertura de los correos, ya que el destinatario reconoce a DocuSign como una fuente confiable.

Conclusión

El uso de la API de DocuSign para llevar a cabo ataques de phishing evidencia la constante innovación de este tipo de acciones, utilizando plataformas confiables para ejecutar campañas de malware de gran eficacia. Este ataque, que se sirve de vulnerabilidades antiguas en software de uso frecuente, resalta la relevancia de entender y mantenerse alerta a los peligros en un entorno de ciberseguridad cada vez más complejo.

Nicolas Fernandez
Cybersecurity Analyst

Samuel Santos
Cybersecurity Analyst

Vulnerabilidades

Vulnerabilidad crítica en la librería Java AsyncHttpClient (AHC)

Fecha: 2 de diciembre de 2024
CVE: CVE-2024-53990

CVSS: 9.2

CRÍTICA

Descripción

La librería AsyncHttpClient (AHC) permite a las aplicaciones Java ejecutar solicitudes HTTP y gestionar respuestas de manera asíncrona de forma sencilla.

Sin embargo, se ha descubierto la vulnerabilidad CVE-2024-53990, por la cual el CookieStore automático puede sobrescribir *cookies* definidas explícitamente si coinciden en nombre, lo que en entornos multiusuario podría provocar el uso incorrecto de dichas *cookies*, generando posibles problemas de autenticación o exfiltración de datos.

Solución

Los desarrolladores de *backend* que utilizan autenticación de terceros y renovación de *tokens* pueden presentar fallos de autenticación y gestión de sesiones debido a la sobreescritura involuntaria de *cookies*.

Por ello, el fabricante recomienda actualizar a la versión 3.0.1 con la mayor brevedad posible.

Productos afectados

Esta vulnerabilidad afecta a las siguientes versiones:

- Versión 3.0.0 de la librería AHC

Referencias

- incibe.es
- github.com

Vulnerabilidades

Vulnerabilidad crítica DoS en la NASA

Fecha: 5 de diciembre de 2024
CVE: CVE-2024-54130

CVSS: 9.2

CRÍTICA

Descripción

La NASA ha descubierto una nueva vulnerabilidad en su red interplanetaria de superposición (ION), un modelo de redes que soportan retrasos e interrupciones (DTN).

La vulnerabilidad crítica CVE-2024-54130 provoca el cese de respuesta del nodo a los paquetes entrantes, desencadenando un escenario de denegación de servicio (DoS). Para ello debe llegar un paquete con un identificador de punto final (EID) cuyo valor sea dtn:none.

Como consecuencia, las comunicaciones espaciales y el intercambio de datos podrían verse afectados.

Solución

Para mitigar la vulnerabilidad se recomienda seguir los siguientes pasos:

- Actualizar a la versión 4.1.3s o posterior de ION-DTN-BPv7.
- En caso de no poder actualizar de manera inmediata, realizar controles de acceso para reducir la exposición.
- Analizar los sistemas para identificar conductas inusuales.
- Considerar aplicar un sistema para bloquear o limpiar paquetes con EID inesperados.
- Elaborar y conservar un plan de acción en caso de explotación exitosa.

Productos afectados

La vulnerabilidad afecta a las siguientes versiones:

- Anteriores a la 4.1.3s de ION-DTN-BPv7.

Referencias

- incibe.es
- nvd.nist.gov
- github.com

Parches de seguridad para Veeam Service Provider Console (VSPC)

Fecha: 3 de diciembre de 2024
CVE: CVE-2024-42448 y 1 más

Crítica

Descripción

Veeam ha publicado actualizaciones para mitigar dos vulnerabilidades (1 crítica y 1 alta) de VSPC, plataforma BaaS y DRaaS remota que administra copias de seguridad:

- CVE-2024-42448: vulnerabilidad crítica (9.9) que permitía a un agente de administración la ejecución remota de código, lo que podía desencadenar en posteriores ataques.
- CVE-2024-42449: un agente de administración podía extraer *hashes* NTLM y eliminar archivos de la cuenta de servicio de VSPC.

Para ambas, era condición necesaria que el agente tuviera autorización en el servidor VSPC. Esta vulnerabilidad demuestra la importancia de los controles de acceso.

Productos afectados

Las actualizaciones de seguridad afectan a las siguientes versiones:

- VSPC, versión 8.1.0.21377.
- Todas las versiones 8.X previas a la 8.1.0.21377.
- Todas las versiones 7.X.

Solución

Veeam recomienda la actualización a la versión 8.1.0.21999 de VSPC lo antes posible.

Referencias

- socradar.io
- qualys.com
- blog.segu-info.com

Actualizaciones de QNAP ante vulnerabilidad crítica de inyección SQL

Fecha: 6 de diciembre de 2024
CVE: CVE-2024-50387

Crítica

Descripción

Se han lanzado una serie de actualizaciones para corregir una vulnerabilidad crítica (CVSS: 10.0) detectada en varias versiones del sistema operativo QNAP. La vulnerabilidad en cuestión está identificada como CVE-2024-50387.

En caso de ser explotada, esta vulnerabilidad podría permitir a los atacantes remotos inyectar código SQL malicioso con el fin de comprometer las bases de datos expuestas.

Estas inyecciones de código malicioso SQL podrían suponer un compromiso de algunos aspectos básicos de la seguridad como la confidencialidad y la integridad.

Productos afectados

Los productos afectados por dicha vulnerabilidad son:

- SMB Service versiones anteriores a la 4.15.002.
- SMB Service h versiones anteriores a la h4.15.002.

Solución

Se recomienda actualizar SMB Service a la versión más reciente donde se ha corregido el problema:

- SMB Service 4.15.002 y posteriores
- SMB Service h4.15.002 y posteriores

Referencias

- incibe.es
- nvd.nist.gov
- qnap.com

Eventos

AI Infrastructure & Architecture Summit 2025
13-15 de Enero

El AI Infrastructure & Architecture Summit 2025 se llevará a cabo del 13 al 15 de enero de 2025 en Londres, Reino Unido. Este evento se centrará en la construcción de modelos de IA personalizados e infraestructuras escalables para implementaciones a nivel empresarial. Contará con sesiones lideradas por expertos de organizaciones como Microsoft, HSBC, Citi, Wells Fargo, L'Oreal y AstraZeneca, abordando temas como modernización de plataformas de datos, optimización de recursos computacionales y estrategias de MLOps.

Enlace

I Jornada de ciberseguridad en el sector financiero
22 Enero

La I Jornada de Ciberseguridad en el Sector Financiero, organizada por Red Seguridad y la Fundación Borredá, se celebrará el 22 de enero de 2025 en formato online (en diferido) y con aforo presencial limitado mediante invitación. Bajo el lema «DORA: fortaleciendo un marco sólido de resiliencia», el evento analizará el impacto del reglamento DORA en la continuidad y calidad de los servicios financieros, destacando la ciberseguridad como un imperativo estratégico. Contará con la participación de reconocidos CISOs y expertos de instituciones como BBVA, Mapfre, ING y Grupo Santander.

Enlace

CyberSec Asia 2025
22-23 Enero

Cybersec Asia 2025 se llevará a cabo el 22 y 23 de enero de 2025 en el Centro Nacional de Convenciones Reina Sirikit (QSNCC) en Bangkok, Tailandia, como parte de la "Cybersec Asia x Thailand International Week 2025", organizada por la NCSA. Este evento reúne a líderes en ciberseguridad, gestión de datos y soluciones en la nube de las regiones CLMVT (Camboya, Laos, Myanmar, Vietnam y Tailandia) y APAC. Con más de 5,000 asistentes, 140 expositores y 100 ponentes, es una plataforma clave para explorar tendencias, iniciativas gubernamentales y oportunidades de crecimiento en la industria, además de establecer conexiones estratégicas.

Enlace

The AI Regulation Summit 2025
27 Enero

La AI Regulation Summit se celebrará el 27 de enero de 2025 en el Centro de Londres. Este evento reunirá a expertos internacionales para abordar los enfoques regulatorios globales en torno a la inteligencia artificial, incluyendo el AI Bill del Reino Unido, la Regulación de la IA en la UE y la estrategia de los EE.UU. sobre IA. Se analizarán temas clave como privacidad de datos, protección al consumidor, ciberseguridad, propiedad intelectual y ética de la IA. Además, se explorarán mejores prácticas en gestión de riesgos para proveedores y usuarios de sistemas de IA.

Enlace

OPEX Week: Business Transformation World Summit 2025
27-29 Enero

El OPEX Week: Business Transformation World Summit 2025 se llevará a cabo del 27 al 29 de enero de 2025 en Miami, celebrando su 26ª edición. Este evento reunirá a más de 100 ponentes, incluidos Chief Transformation Officers de grandes marcas como Walmart, Goldman Sachs, McDonald's, L'Oreal y Air Canada, quienes compartirán sus conocimientos sobre la transformación empresarial en la era de la IA. La agenda incluye 14 talleres, 16 grupos de discusión interactivos, 4 grupos de enfoque por industria y una zona de innovación en IA.

Enlace

Recursos

➢ NIS Investments 2024 de ENISA

El informe "NIS Investments 2024" de ENISA evalúa cómo la Directiva NIS 2 ha influido en las inversiones y la madurez en ciberseguridad en la UE, basándose en datos de 1,350 organizaciones de los 27 estados miembros. Asimismo, presenta una visión previa a la implementación de la Directiva NIS 2, incluyendo métricas clave para sectores críticos y manufactura, ayudando a preparar evaluaciones futuras. Es una herramienta esencial para responsables de políticas y organizaciones que buscan alinearse con los estándares europeos.

Enlace

➢ Cybersecurity Snapshot: AI Security Roundup: Best Practices, Research and Insights de Tenable

El artículo de Tenable presenta un resumen sobre las mejores prácticas y nuevas investigaciones relacionadas con la seguridad en inteligencia artificial (IA). Incluye análisis sobre cómo proteger aplicaciones impulsadas por IA, la mitigación de riesgos asociados al "Shadow AI" y la integración de estrategias de confianza cero en infraestructuras críticas. Además, destaca herramientas y enfoques innovadores para abordar amenazas emergentes en ciberseguridad.

Enlace

➢ Nueva Ley de Protección de Datos Personales en Chile

El Tribunal Constitucional de Chile aprobó la nueva Ley de Protección de Datos Personales, alineándola con estándares internacionales. Esta ley fortalece los derechos de los ciudadanos sobre su información, establece obligaciones estrictas para las organizaciones en su tratamiento y crea una agencia reguladora especializada. Es un paso clave hacia una mayor seguridad y privacidad en el entorno digital del país.

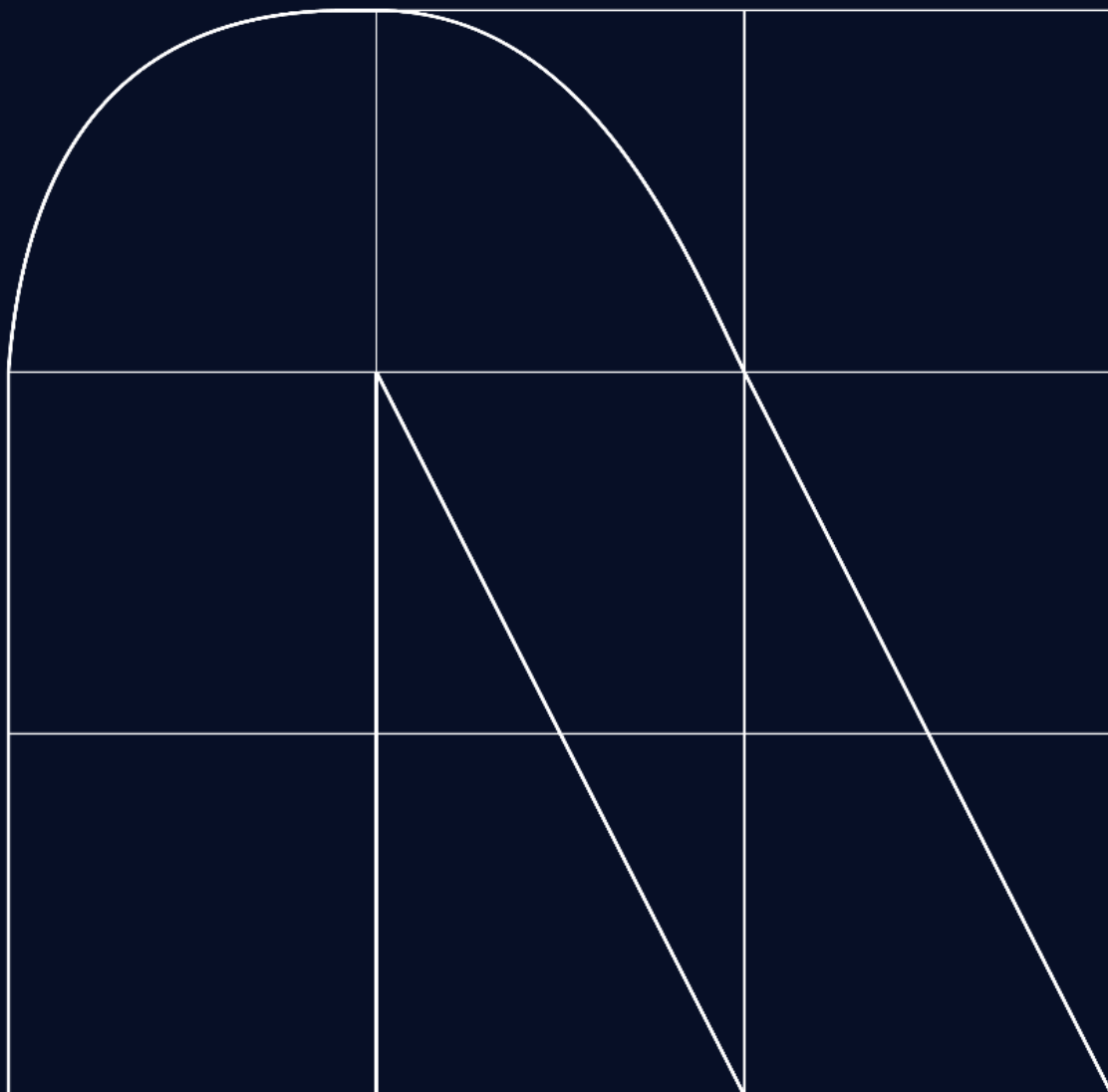
Enlace

➢ Nuevo Reglamento de Protección de Datos Personales en Perú

Se publicó el nuevo reglamento de la Ley 29733, Ley de Protección de Datos Personales, en el diario oficial El Peruano. Este reglamento representa un gran avance para el Perú en la era digital, al incorporar novedades como evaluaciones de impacto preventivas, códigos de conducta, reportes de incidentes en 48 horas, y el derecho a la portabilidad de datos. Además, refuerza la protección de menores, moderniza la seguridad con estándares internacionales, y flexibiliza el cumplimiento territorial, alineando al país con las mejores prácticas globales.

Enlace

Suscríbete a RADAR



Powered by the cybersecurity NTT DATA team

es.nttdata.com