NÚMERO 83 | OCTUBRE 2023

NTT DATA
Trusted Global Innovator

Radar

El magazine de ciberseguridad

¿COMO GESTIONAR LOS RIESGOS EN LOS NUEVOS MODELOS DE INTELIGENCIA ARTIFICIAL?

En el tejido interconectado de nuestra era, la ciberseguridad trasciende su papel técnico para convertirse en el bastión que protege nuestra infraestructura digital. Es la salvaguardia de la confianza en nuestras operaciones diarias. La inteligencia artificial (IA) se utiliza en muchas aplicaciones comerciales y de producción, incluida la automatización, el procesamiento del lenguaje y el análisis de datos productivos.

Esto permite que, a nivel general, las empresas estén optimizando tanto sus procesos de fabricación, operaciones, y la mejora de su eficiencia interna. Y es que, a través de distintas reglas de programación informática, la IA permite que una máquina se comporte como un humano y resuelva problemas.

Es importante mencionar que ningún módulo de IA viene listo desde un comienzo para operar y funcionar como un verdadero apoyo a las labores de la empresa y la toma de decisiones. Es importante el decidir una estrategia y datos acotados para su entrenamiento y posterior puesta en funcionamiento. Las grandes compañías que actualmente están impulsando el uso de la IA tienen los recursos necesarios para montar la infraestructura necesaria para el entrenamiento (GPUs/TPUs, enormes bases de datos, etc.).

Los modelos pueden reentrenarse con datos específicos de empresas más pequeñas (técnica llamada Transfer Learning). En esta etapa de preprocesamiento el rol de los expertos relacionados con el sistema en entrenamiento es clave, de lo contrario el modelo hará predicciones no alineadas a la realidad.

La incorporación de la IA no queda exenta de la aparición de nuevas posibles brechas de seguridad y de protección de datos que las empresas deben considerar y a la cual deben dedicar recursos y tiempo. Las buenas prácticas recomiendan anonimizar los datos utilizados para el entrenamiento, pero hay veces que es posible re identificar su procedencia. Los modelos de machine learning y deep learning buscan patrones en los datos, por ello es importante que los datos entregados estén verificados/preparados por una persona experta (por ejemplo, un experto en data governance), ya que el modelo será tan bueno como los datos que se usaron para su entrenamiento.

Aquí surge un nuevo aspecto a considerar y de vital importancia. un sistema de IA, si bien puede convertirse en un gran aliado para la toma de decisiones para una empresa, también introduce una nueva serie de vulnerabilidades, las cuales pueden ser aprovechadas y explotadas de manera maliciosa a fin de extraer información sensible o bien tomar control del sistema.

Por eso, cumplir un marco mínimo de medidas y controles de seguridad por parte del sistema de IA se convierte en un requerimiento base al implementar el sistema y dar paso a un ambiente de producción. Una correcta elección de controles de seguridad y de desarrollo mínimo, ayudará a reforzar la seguridad y la privacidad de la información y aumentará la confianza en el uso de los sistemas IA. Este marco permitirá reconocer, medir y mitigar los riesgos de ciberseguridad que un sistema IA puede generar en una organización, minimizando el número de posibles brechas de seguridad que el sistema pueda tener en el momento

Enrique Bernao Rosado
Manager de Ciberseguridad en NTT DATA Europe & Latam

CIBERCRÓNICA

En esta edición del RADAR hablaremos sobre ataques a la cadena de suministro en el proceso de desarrollo de software, técnica conocida como ***Supply Chain Compromise*** según el Mitre. El uso de frameworks de desarrollo web modernos ha permitido prevenir técnicas de ataque web comunes, basta con analizar el TOP 10 OWASP 2021 para darse cuenta de que la explotación de inyecciones pasó a un tercer lugar.

Sin embargo, los cibercriminales también actualizan sus ataques, es por esto por lo que, en los últimos años los ataques a la cadena de suministro han estado en auge, basta con recordar el desastre causado por Log4j en 2021.

Un supply chain attack consiste una vulneración de un componente o librería de software ampliamente utilizado en el mercado con el fin de impactar las aplicaciones finales.

> “un error en la librería que interactúa con los motores de bases de datos, provocando que con parámetros envenenados fuese posible ejecutar sentencias SQL de consulta, modificación o eliminación.”

Desde entonces los ataques a la cadena de suministro se han convertido en una modalidad efectiva para los cibercriminales, quienes implementan diferentes tácticas y técnicas para afectar componentes de software o a sus desarrolladores.

Por ejemplo, podemos analizar el reciente ataque en junio sobre la solución MOVEit (CVE-2023-34362) software líder del mercado para transferir archivos de forma segura. Lo interesante es que los atacantes explotaron una inyección SQL en producción y utilizaron esta brecha para ganar acceso a bases de datos de compañías como BBC, British Airways, Aer Lingus, Boots, entre otras.

Al parecer los cibercriminales encontraron un error en la librería que interactúa con los motores de bases de datos, provocando que con parámetros envenenados fuese posible ejecutar sentencias SQL de consulta, modificación o eliminación.

Por otro lado, el usuario de conexión entre MOVEit y la base de datos se ejecuta con privilegios de administrador, posibilitando que los atacantes ganaran acceso de forma remota al servidor de aplicaciones. El grupo Cl0p es al parecer el implicado en el ataque, dado que utilizaron un backdoor conocido como LEMURLOOT para exfiltrar la información. Las compañías afectadas por el ataque fueron notificadas y el equipo de MOVEit activó su plan de respuesta a incidentes, generando los respectivos indicadores de compromiso y los parches asociados para mitigar la brecha.

Otro ataque a la cadena de suministro que está afectando a la comunidad de Python es la reciente campaña iniciada en agosto, al parecer norcoreana, sobre librerías Open Source. Los cibercriminales estarían incluyendo código malicioso en dependencias ampliamente conocidas y que se gestionan con el famoso gestor de paquetes PyPI (pip). La técnica utilizada consiste en crear librerías con nombres y descripciones muy similares a las oficiales, pero con pequeñas variaciones, de tal manera que desarrolladores inconscientes importen estas librerías maliciosas como Vmconnector, Tableediter y pyVmomi, son algunas de las librerías afectadas.

Los cibercriminales clonan el proyecto oficial para posteriormente incluir fragmentos de código malicioso y, finalmente, cargarlas al gestor de paquetes de Python. Esto varía ligeramente el nombre la librería utilizando caracteres especiales. Según el análisis de ReversingLabs generado a partir de su plataforma Titanium, que es una herramienta utilizada para monitorear librerías OpenSource y analizar su código fuente (SAST), los cibercriminales habrían incluido código malicioso en la librería suplantada Vmconnect en donde se identificaron fragmentos de código con la capacidad de crear procesos del sistema operativo; enumerar información del sistema y ofuscar datos utilizando base64 y conexiones a sitios web remotos.

Al analizar los dominios encontrados en las url en el código fuente, Reversing Labs pudo determinar que posiblemente estaban relacionados con el grupo Lazarus (ampliamente conocidos por estar financiados por el gobierno de Corea del Norte), y que se ha atribuido recientes ataques de ransomware. Al parecer el vector está cambiando, pues la confianza que existe por parte de los desarrolladores en los gestores de paquetes y la falta de conciencia estarían jugando a favor del grupo cibercriminal. ReversingLabs también ha detectado estas mismas técnicas de ataque a la cadena de suministro en los gestores de paquetes de lenguajes como NodeJS (npm), Ruby (gem) y C# (nuget).

También podemos recordar el ataque a 3CX en marzo del año presente, de acuerdo con Mandiant, la aplicación de escritorio 3CX fue infectada con código malicioso luego de que cibercriminales norcoreanos comprometieran el ambiente de desarrollo de la compañía 3CX a través de sofisticados ataques a la red interna. El objetivo de los atacantes era modificar este software legítimo para incluir fragmentos de código tipo RAT, para ganar acceso no autorizado a los ordenadores de los usuarios finales de 3CX. El impacto del ataque es objeto de estudio meses después debido a que no se conocían técnicas tan sofisticadas y creativas.

Al parecer el ataque inició sobre un desarrollador de 3CX que instaló un software de trading con código malicioso, rápidamente los cibercriminales infectaron la máquina y la utilizaron como vector de entrada a la red interna. También se sabe que credenciales y secretos fueron comprometidos al analizar repositorios de código desde la cuenta del desarrollador. Con estos accesos los atacantes realizaron movimientos laterales hasta alcanzar los entornos de CI/CD de la aplicación de escritorio de 3CX. Según Mandiant, se ejecutaron técnicas de inyección de DLL y persistencia a nivel de servicios para incluir librerías maliciosas en el código fuente oficial de la aplicación. Mandiant atribuye el ataque al grupo cibercriminal norcoreano Nexus.

Por último, estos ataques a la cadena de suministro ya los atienden proveedores de herramientas de seguridad en aplicaciones. El equipo de Snyk, herramienta de análisis de vulnerabilidades en componentes de terceros, mantiene un listado actualizado de librerías maliciosas que se cargan a los gestores de paquetes tradicionales. Durante el mes de agosto el equipo de Snyk reportó más de 500 librerías maliciosas, en donde casi un 20% de ellas estaban escritas en lenguaje C y C++, lo cual puede indicar que incluso los dispositivos de internet de las cosas (IoT) están siendo objetivo de los cibercriminales.

Los ataques a la cadena de suministro seguirán siendo un vector de ataque efectivo para cibercriminales cuando las organizaciones no implementan medidas de seguridad adecuadas. Los procesos de desarrollo y adquisición de software, componentes y librerías de terceros deberán ser pilares de aseguramiento. La inversión en programas robustos de seguridad en aplicaciones es fundamental para garantizar que el ciclo de vida del software se encuentre asegurado, y que en caso de ciberataques en componentes y librerías de terceros se pueda reaccionar a tiempo. A corto plazo la implementación de Software Bill of Materials (SBOM) es imprescindible para determinar la superficie de ataque de las organizaciones frente a amenazas a la cadena de suministro del software.

USO DE FAIR COMO METODOLOGÍA CLAVE EN EL ANÁLISIS DE RIESGO CUANTITATIVO FAIR

Por: NTT DATA Europe & Latam

Ya se lleva hablando muchos meses de la metodología de riesgos cuantitativa FAIR. En una edición anterior de RADAR se introdujo la metodología y sus beneficios. Sin embargo, hay muchas dudas en su uso, el esfuerzo necesario para adoptarla en una organización y qué tipo de información es necesaria tener para poner esta metodología en marcha. En este artículo queremos acercarnos un poco más a cómo debemos aproximar el análisis de un escenario y qué tipo de preguntas nos vamos a tener que plantear.

Pongamos ejemplos de escenarios:

- Indisponibilidad de la banca web transaccional en el sector bancario
- Indisponibilidad de un canal de compras web en sector retail
- Indisponibilidad de una web de registro de seguros de una aseguradora

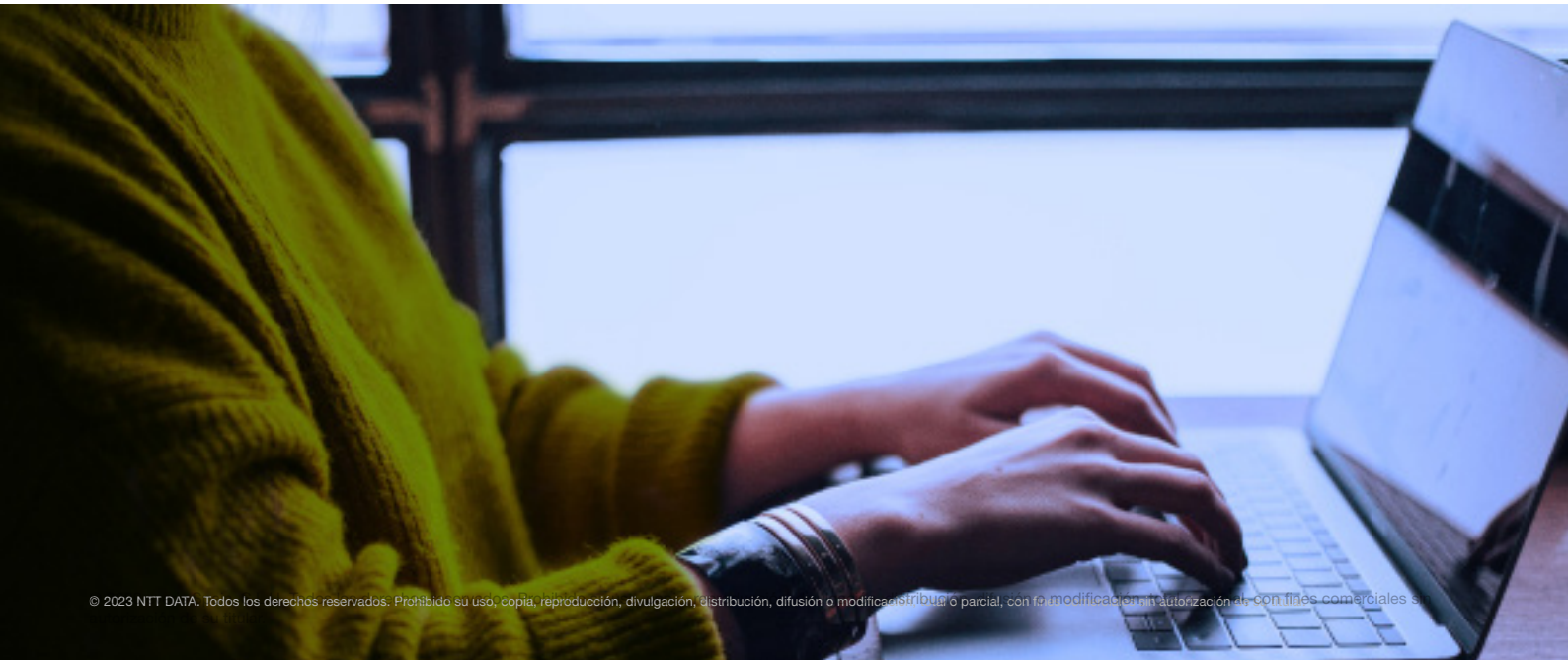
En estos escenarios, FAIR nos ayuda a responder a las siguientes preguntas:

- ¿Cuánto dinero voy a perder el próximo año en el escenario más probable por indisponibilidad de ese sistema?
- ¿Cuánto voy a perder como mínimo?
- ¿Y como máximo?

Datos concretos que presentados al C-level pueden ayudar a potenciar inversiones necesarias para mitigar los riesgos existentes. El primer paso: contextualizar en función de la organización, determinando el sector al que pertenece, sus procesos y activos críticos. Esto servirá para definir el alcance del escenario que se desea evaluar. El escenario debe contemplar un activo y un agente de amenaza, por ejemplo: web transaccional bancaria con pérdida de disponibilidad por un ramsonware. Es importante recalcar que cada escenario (activo + agente de amenaza) que encontremos debe ser analizado de manera separada en FAIR, aunque conforme se analicen escenarios y se releve la información, está va a ser aplicable a subsiguientes escenarios.

Una vez definido el escenario, podemos comenzar a realizar las evaluaciones de magnitud de pérdida y frecuencia de eventos de pérdida. Comenzaremos por la magnitud de pérdida, la cual se divide en dos categorías principales: **pérdida primaria** (pérdida directa para la organización y/o los stakeholder principales) y **pérdida secundaria** (pérdida para la organización y/o stakeholders principales a raíz de una reacción negativa de segundas o terceras partes).

Para las evaluaciones de magnitud de pérdida primaria, se debe pensar en 6 subcategorías: reputación, productividad, reemplazo, productividad, ventaja competitiva y multas.



Para comenzar con esta evaluación, nos tenemos que plantear las siguientes preguntas:

- Pérdida por productividad: tras el ataque y la pérdida de disponibilidad de la web transaccional, ¿cuántos trabajadores se ven afectados en el mejor de los casos? ¿y cuántos en el peor de los casos? Esas personas se quedarán sin trabajar, ¿qué salario perciben? y, por tanto, ¿cuál es la pérdida económica en el mejor y en el peor de los casos? Como el modelo nos pide también un valor de "más probable" podemos hacernos la pregunta en la situación más posible o simplemente hacer la media del valor mínimo y máximo.
- Costos de recuperación: la organización analizada debería contar con un plan de recuperación. ¿cuántas personas como mínimo ejecutarán este plan de recuperación? ¿y como máximo? ¿cuántas horas está contemplado que trabajen como mínimo? ¿y como máximo? ¿cuál es su tarifa? Con esta información podemos calcular cuánto costará la recuperación en un valor mínimo, máximo y podemos usar la media para el escenario más probable.
- Pérdida por multas y sentencias: el activo bajo análisis tendrá una serie de clientes que pueden verse afectados. ¿cuántos afectados habrá como mínimo? ¿y como máximo? ¿qué multa podríamos pagar si hubiera una denuncia? Con esta información ya se puede calcular cuánto pagaría la organización por multas y sentencias. El valor más probable se puede calcular pensando en el número de afectados posible y el costo de multa probable o simplemente como media de los valores mínimo y máximo.
- El daño reputacional causado en el escenario también debe cuantificarse. ¿qué pérdida por daño reputacional tendremos como mínimo? ¿y como máximo? Y lo más probable, ¿cuánto sería?
- Así mismo, habrá pérdidas por ventaja competitiva ante otras organizaciones que den el mismo servicio. Quizá aquí se pueda obtener la información de esta pérdida en datos históricos de incidencias donde haya habido movimientos de clientes hacia otra organización. ¿cuál fue la mínima pérdida registrada? ¿y la máxima? ¿y la más común?
- Por último, hay que considerar pérdidas por reemplazo si es que aplican. Es decir, en caso el activo o activos involucrados en el escenario deberían reemplazarse cuando suceda el escenario evaluado. Igualmente, se considerará el valor mínimo de reemplazo, máximo y más probable.

Recordemos que la magnitud de pérdida se divide en dos partes (primaria y secundaria), por lo que ahora hay que analizar las pérdidas provocadas por segundas o terceras partes. Para la pérdida secundaria, analizamos la siguiente información:

- Pérdida secundaria por respuesta: la afectación a los clientes va a generar que parte del equipo de trabajo de la organización se enfoque a la notificación de estos clientes. ¿quántos clientes van a requerir atención como mínimo? ¿y como máximo? ¿y el valor más probable cuanto será? Y ¿cuál será el costo de notificación? Con esto ya se puede calcular la pérdida de productividad secundaría mínima, máxima y más probable.
- Pérdida secundaria por multas y sentencias: podrían existir reclamos y denuncias de parte de nuestros clientes o derivadas de que ellos a su vez son multados por sus propios clientes, porque nuestro incidente afectó a un servicio que no pudieron dar en tiempo y forma. En este caso debe realizarse un análisis de cuál sería el mínimo esperado por estas multas, sentencias o sanciones. ¿qué valor sería el más probable y qué podríamos esperar en el peor caso?
- Pérdida secundaria por productividad: para este valor debemos pensar qué equipo adicional debemos contratar para hacer frente a las denuncias y reclamaciones que vamos a recibir. Por ejemplo, la organización podría necesitar reforzar el departamento legal o contar con asesores legales de forma externa. En este punto pensaremos cuantas personas necesitaremos adicionales como mínimo, como máximo y de forma más probable, por cuanto tiempo y su tarifa. Con estos valore, podremos calcular valor mínimo, medio y máximo.
- Pérdida secundaria por reputación: Este valor se refiere a pérdida de valor de acciones e incumplimiento de proyecciones de captación de clientes. Se deberá pensar en cuanto como mínimo vamos a perder por estos eventos, cuanto como máximo y cuanto sería lo más probable.

Una vez contestadas todas estas preguntas, se concluye el análisis de pérdidas monetarias del escenario. El último paso es determinar la frecuencia de eventos de pérdida y vulnerabilidad del activo en alcance del escenario.

Para la frecuencia de eventos de pérdida se puede realizar un análisis de los incidentes dados en el pasado y se debe determinar cuántos eventos como

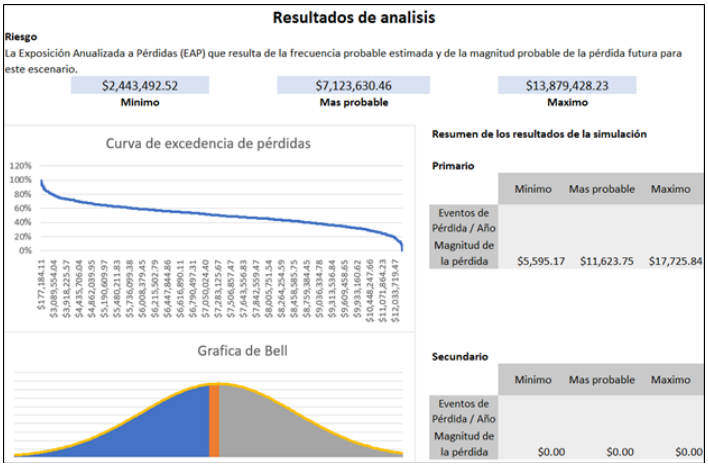
mínimo se tendrán el próximo año, como máximo y en promedio. Por ejemplo, en un escenario de indisponibilidad de un activo, se puede revisar cuantas veces ese activo quedo indisponible en los últimos 5 años, y tomar el valor mínimo, el máximo y una media como el más probable.

Y, por último, y quizá la cuestión más compleja del análisis: medición de la resistencia del activo. Este activo contará con diferentes medidas de seguridad ya aplicadas en la organización, esto reducirá en gran medida la vulnerabilidad ante los atacantes ¿en qué % de ataques, en el mejor de los casos, se espera que los controles de seguridad eviten el ataque? ¿y en el peor de los casos? ¿y en el más probable?

Ahora sí, con toda la información recolectada es posible ingresar toda la información a la herramienta de análisis, lo que nos permite tener una estimación de la pérdida. Lo interesante de FAIR es que nos devolverá 3 valores:

- Valor 1: valor mínimo de pérdida.
- Valor 2: valor de pérdida más probable.
- Valor 3: valor máximo de pérdida.

Adicional a esto, la herramienta nos provee de una visualización de cuantos eventos por año es posible tener (basado en la información de eventos y vulnerabilidad proporcionados). Es decir, podremos decir cuántos eventos habrá como mínimo, como máximo y en el escenario más probable.



Una vez logrado este punto comienza la estrategia. ¿Qué proyectos podemos ejecutar para aumentar la resistencia? ¿en cuánto va a mejorar esa resistencia? ¿y cuánto nos dice el modelo que perderemos con esa nueva medida de seguridad? Lo importante será definir qué medidas, iniciativas, inversiones e implementaciones realizar y buscar que estos proyectos tengan un impacto económico mayor que su coste en pérdidas. A partir de ese momento, las compañías podrán utilizar todo el potencial de FAIR.

TENDENCIAS

Seguridad y privacidad en Inteligencia Artificial

Según el Artificial Intelligence Index Report (2023), alrededor de 31 países han emitido y/o aprobado algún marco normativo relacionado con IA durante el periodo 2016 a 2022. El objetivo de dicha regulación es brindar lineamientos de privacidad y seguridad que sean considerados para proyectos que involucren el diseño, desarrollo y despliegue de un sistema IA.

Entonces ¿qué se debe hacer para garantizar la seguridad y privacidad de un sistema IA? Para que un sistema IA sea seguro y garantista del derecho de protección de datos personales, se debe verificar si cumple con controles legales, organizativos y técnicos. Para ello, es fundamental que, en base a un framework enfocado en la regulación vigente, se pueda realizar una evaluación para determinar cuál es el nivel de madurez del sistema IA y de ser el caso, adoptar las medidas correctivas necesarias.

Pero ¿qué dominios deben analizar en un framework de inteligencia artificial?

a) Lo primero, se debe asegurar una correcta identificación y transparencia del sistema IA. Se deben analizar aspectos como: propósito, identificación de responsabilidades, transparencia e identificación de contexto de uso y asegurar que esa información exista.

b) Fundamentos del sistema IA: Asegurar que los fundamentos del sistema IA están correctamente definidos. Se deben analizar aspectos como: identificación de la política de desarrollo, adecuación de los modelos teóricos base, así como del marco metodológico e identificación de la arquitectura básica.

c) Gestión de los datos: Asegurar que los procesos de recopilación, almacenamiento, procesamiento y protección de los datos utilizados por un sistema IA están correctamente definidos. Se deben analizar aspectos como: determinación del origen de las fuentes de datos, control del sesgo, preparación y calidad de los datos.

d) Gestión del riesgo: Asegurar la identificación, evaluación, control y supervisión de los riesgos asociados con la implementación y operación de un sistema IA. Se deben analizar aspectos como: mapeo, medición y gestión.

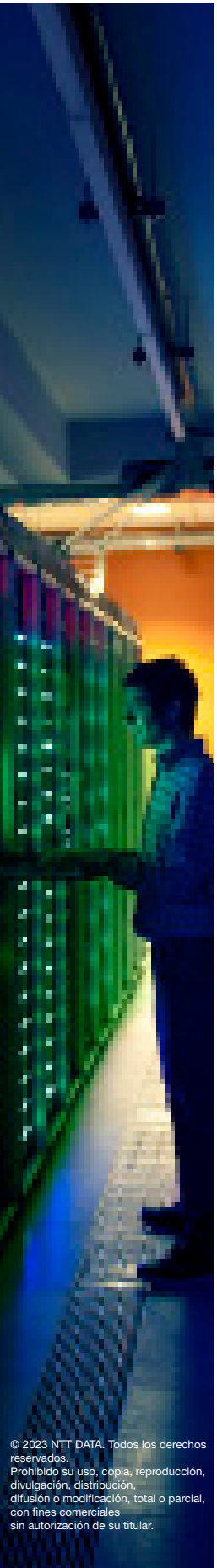
e) Intercambio de información sobre incidentes y fallos del funcionamiento: Asegurar la efectiva comunicación entre organizaciones y partes interesadas en relación con los incidentes de seguridad, las vulnerabilidades y los fallos de funcionamiento en un sistema IA. Se deben analizar aspectos como notificación de incidentes graves, acceso a datos y al código fuente del sistema IA.

f) Verificación y validación: Asegurar que el sistema IA funcione de acuerdo con los requisitos establecidos y produzca resultados precisos y confiables. Se deben analizar aspectos como: coherencia, rendimiento, seguridad y trazabilidad.

Una profunda revisión de estos dominios y adaptación de los sistemas de inteligencia artificial para que lo cumplan permitirá a las organizaciones sacar el máximo partido a esta tecnología, sin poner en riesgo su negocio ni la confianza de sus clientes.

VULNERABILIDADES

Reciba nuestro boletín completo de parches y vulnerabilidades suscribiéndose **aquí**.



OneView

CVE-2023-30908;-2650;-4304
Fecha: 07/09/2023

Descripción.El pasado 7 de septiembre se publicó una vulnerabilidad crítica (CVE-2023-30908) que afecta al producto OneView, dedicado a la administración de infraestructuras desarrollado por Hewlett Packard Enterprise. A su vez, se han publicado también dos vulnerabilidades (CVE-2023-2650 (Alta) y CVE-2022-4304 (Media) sobre el mismo producto.

Estas vulnerabilidades permiten a un atacante remoto omitir la autenticación y obtener un acceso no autorizado a HPE OneView, debido a cómo la herramienta maneja las credenciales del usuario, se puede manipular una solicitud explícitamente diseñada para HPE OneView.

Mediante la explotación de estas vulnerabilidades un atacante puede obtener información confidencial, como claves de cifrado y contraseñas o realizar un ataque de denegación de servicio (DoS) contra HPE OneView.

Enlace: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04530en_us
https://nvd.nist.gov/vuln/detail/CVE-2023-30908

Productos afectados. Todas aquellas versiones anteriores a v8.5 o v6.60.05 LTS.

Solución: La solución recomendada para hacer frente a esta vulnerabilidad es aplicar los últimos parches de seguridad posteriores v8.5 o v6.60.05 LTS.

Linux

CVE-2023-35082
Fecha: 06/09/2023

Descripción.

Esta vulnerabilidad de desbordamiento está asociada la función route4_change del archivo net/sched/cls_route.c. A través de la manipulación de un input desconocido se causa una vulnerabilidad de clase desbordamiento de búfer.

Los efectos exactos de un ataque con éxito no son conocidos, aunque podría ocasionar denegaciones de servicio y una posible escalada de privilegios. Actualmente no se conoce exploit para dicha vulnerabilidad.

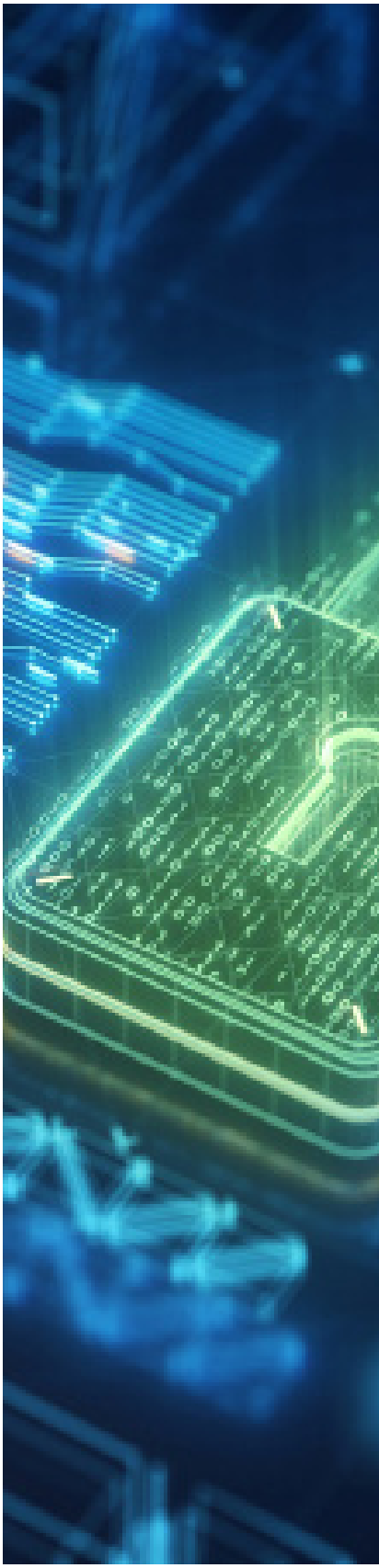
Enlace: https://www.debian.org/security/2023/dsa-5492
https://www.suse.com/security/cve/CVE-2023-4206.html
https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=b80b829e9e2c1b3f7aae34855e04d8f6ecaf13c8

Productos afectados. Los recursos afectados por esta vulnerabilidad son los siguientes:

- Red Hat Enterprise Linux 8 o posterior
- SUSE Linux Enterprise Desktop/Server 15 o anterior
- Debian 6.1.38-1 o anterior y 4.19.249-2 (versión 6.1.52-1 corregida)

Solución: La resolución consistirá en la actualización a las últimas versiones publicadas por cada fabricante.de forma definitiva estas vulnerabilidades.

PARCHES



Apple

Fecha: 07-09-2023

Descripción. Apple ha publicado una actualización de seguridad para iOS y iPadOS que corrige dos exploits zero-day (CVE-2023-41064 y CVE-2023-41061), El fallo de seguridad afecta a la última versión (16.6) del sistema operativo iOS, fue descubierto por los investigadores de Citizen Lab, la cual pertenece a la familia zero-click, al conseguir infectar al dispositivo con el malware Pegasus sin necesidad de intervención del usuario.

El exploit involucra archivos adjuntos PassKit que contenían imágenes maliciosas enviadas desde una cuenta de iMessage del atacante a la víctima para el software Pegasus de NSO Group.

Esta vulnerabilidad está asociada a un desbordamiento de búfer sobre el componente ImageI/O, que permite a las aplicaciones leer y escribir la mayoría de los formatos de archivos de imágenes.

Enlace:
https://citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/
https://support.apple.com/en-us/HT213905

Productos afectados:
La vulnerabilidad afecta a todas las versiones soportadas (16.6 y anteriores).
Solución:
Los parches se aplican instalando las versiones iOS 16.6.1 y iPadOS 16.6.1.

Google Chrome

Fecha: 11-09-2023

Descripción. Google ha lanzado una actualización de seguridad para una vulnerabilidad crítica de zero-day en Chrome (CVE-2023-4863). Esta vulnerabilidad se explota mediante un desbordamiento de búfer en el componente que maneja WebP, un formato de archivo de gráficos rasterizados que reemplaza los formatos de archivo JPEG, PNG y GIF.

La ejecución de esta vulnerabilidad puede provocar fallos denegación de servicio o permitir la ejecución de código malicioso en los sistemas.

Dicha vulnerabilidad puede estar siendo explotada ya que Google es consciente de que existe exploit para dicha vulnerabilidad, según ha sido informado por Apple Security Engineering y Architecture (SEAR) y The Citizen Lab de la Escuela Munk de la Universidad de Toronto.

Enlace: https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html
https://nvd.nist.gov/vuln/detail/CVE-2023-4863

Productos afectados: La vulnerabilidad afecta a todas las versiones anteriores a 116.0.5845.187 para Mac y Linux, y 116.0.5845.187/.188 para Windows.

Solución: Google ha lanzado una actualización automática a las nuevas versiones 116.0.5845.187 para Mac y Linux, y 116.0.5845.187/.188 para Windows.

EVENTOS

FS-ISAC FinCyber Today Summit

1 - 4 de octubre de 2023 |

Esta cumbre es un evento presencial de varios días para profesionales de la seguridad informática que trabajan en instituciones financieras. Muestra a los asistentes cómo pueden aplicar en la vida real las nuevas tendencias y prácticas en materia de seguridad informática para proteger mejor su organización. El evento acoge varios temas. Por ejemplo, “Fraude, identidad y dinero”, “GRC y resiliencia” e “Intel y ataques globales”. Los asistentes pueden elegir el tema que mejor se adapte a sus necesidades empresariales.

Enlace: https://www.fsisac.com/events/2023-fincyber-today-summit

CSA Virtual Research Summit

17 de octubre de 2023 |

CSA organiza un evento especial en el que se presentarán los proyectos de investigación que definirán la seguridad en la nube el próximo año. Con la vista puesta en las importantes tendencias de la nube y la ciberseguridad, la Cumbre de Investigación de la CSA ofrecerá las últimas actualizaciones en proyectos de investigación nuevos y existentes y proporcionará herramientas y orientaciones fundamentales para la comunidad que adopte la nube. Con la nube finalmente afianzada como el principal sistema de TI en todo el mundo, la seguridad en la nube es ahora la base de los programas de ciberseguridad.

Enlace: https://www.csaresearchsummit.com/event/17e14892-a68e-4db9-82a9-528bf4bdbb4e/summary

Capacitaciones Blackhat

23 - 26 de octubre 2023 |

SecTor se ha forjado la reputación de reunir a expertos de todo el mundo para compartir sus últimas investigaciones y técnicas sobre amenazas clandestinas y defensas corporativas. La conferencia ofrece una oportunidad inigualable para que los profesionales, directivos y ejecutivos de la seguridad informática se pongan en contacto con sus homólogos y aprendan de sus mentores. Este año SecTor lanza el programa “Certified Pentester”, un examen práctico de un día de duración.

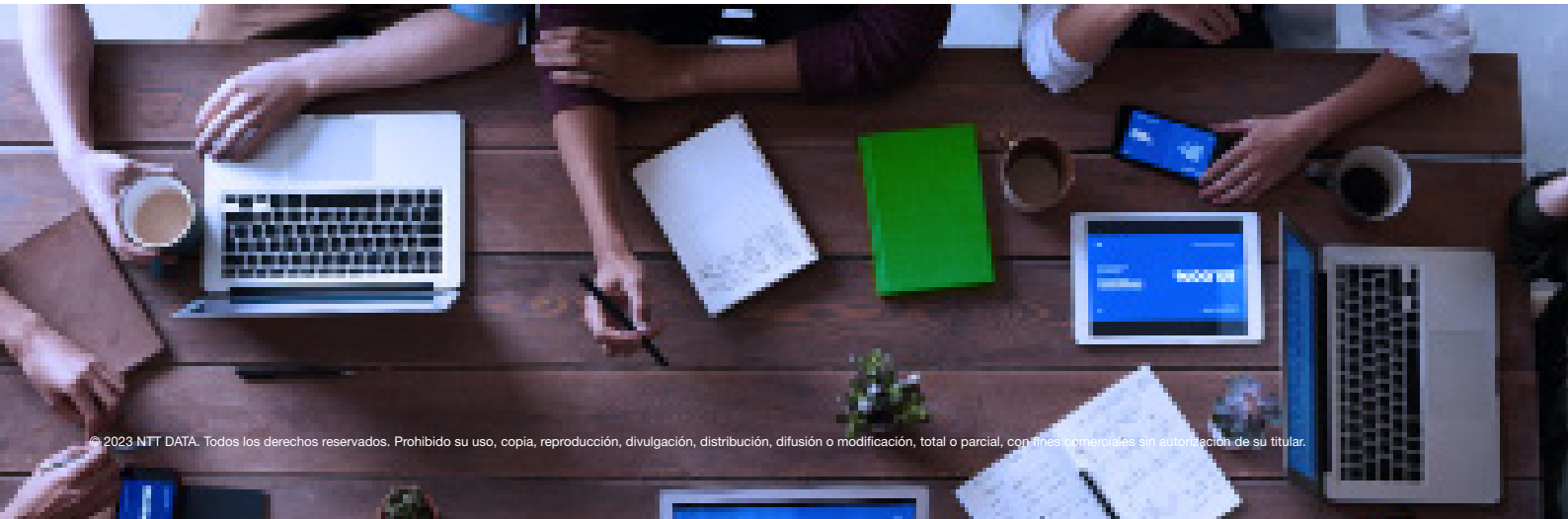
Enlace: https://www.blackhat.com/sector/2023/

SANS Ciber Solutions Fest

27 - 28 de octubre 2023 |

Esta conferencia ayuda a las organizaciones a planificar sus inversiones en seguridad. Su objetivo es poner en contacto a proveedores y líderes de opinión del sector con profesionales y responsables de la toma de decisiones en materia de seguridad. Es gratuita y se celebra íntegramente en línea.

Enlace: https://www.sans.org/blog/coming-soon-sans-cyber-solutions-fest-2021/



RECURSOS

Cloud Native application protection platform survey report

Microsoft encargó a CSA la elaboración de una encuesta y un informe para comprender mejor los conocimientos, actitudes y opiniones del sector en relación con la seguridad de la CNAPP. La encuesta se realizó en línea en abril de 2023 y recibió 1201 respuestas de profesionales de TI y seguridad. El informe tiene como objetivo proporcionar información sobre las prioridades y desafíos de seguridad en la nube de las organizaciones, revelar el estado actual de la implementación de CNAPP e identificar los métodos actuales y los desafíos en la gestión de la postura de seguridad, la protección de la carga de trabajo en la nube y DevSecOps.

Enlace: https://cloudsecurityalliance.org/artifacts/state-of-cnapp-survey-report/

CSA Assurance Education FAQ

El Certificado de Conocimientos de Auditoría en la Nube (CCAK) y la Formación de Auditor Líder STAR son dos ofertas de formación en aseguramiento que forman parte del programa de Seguridad, Confianza, Aseguramiento y Riesgo (STAR) de CSA, el mayor programa de aseguramiento en la nube del mundo.

Enlace: https://cloudsecurityalliance.org/artifacts/csa-assurance-education-faq/

Configuraciones seguras en dispositivos industrial

Son tan importantes las bases del hardware y software que se tienen configuradas e instaladas en el sistema, como las bases de la ingeniería social que se han enseñado a los empleados, puesto que la cadena se rompe por el eslabón más débil y ese, somos los seres humanos. En este articulo INCIBE nos Brinda, entre otras cosas, una lista de buenas practicas para el bastionado de dispositivos OT.

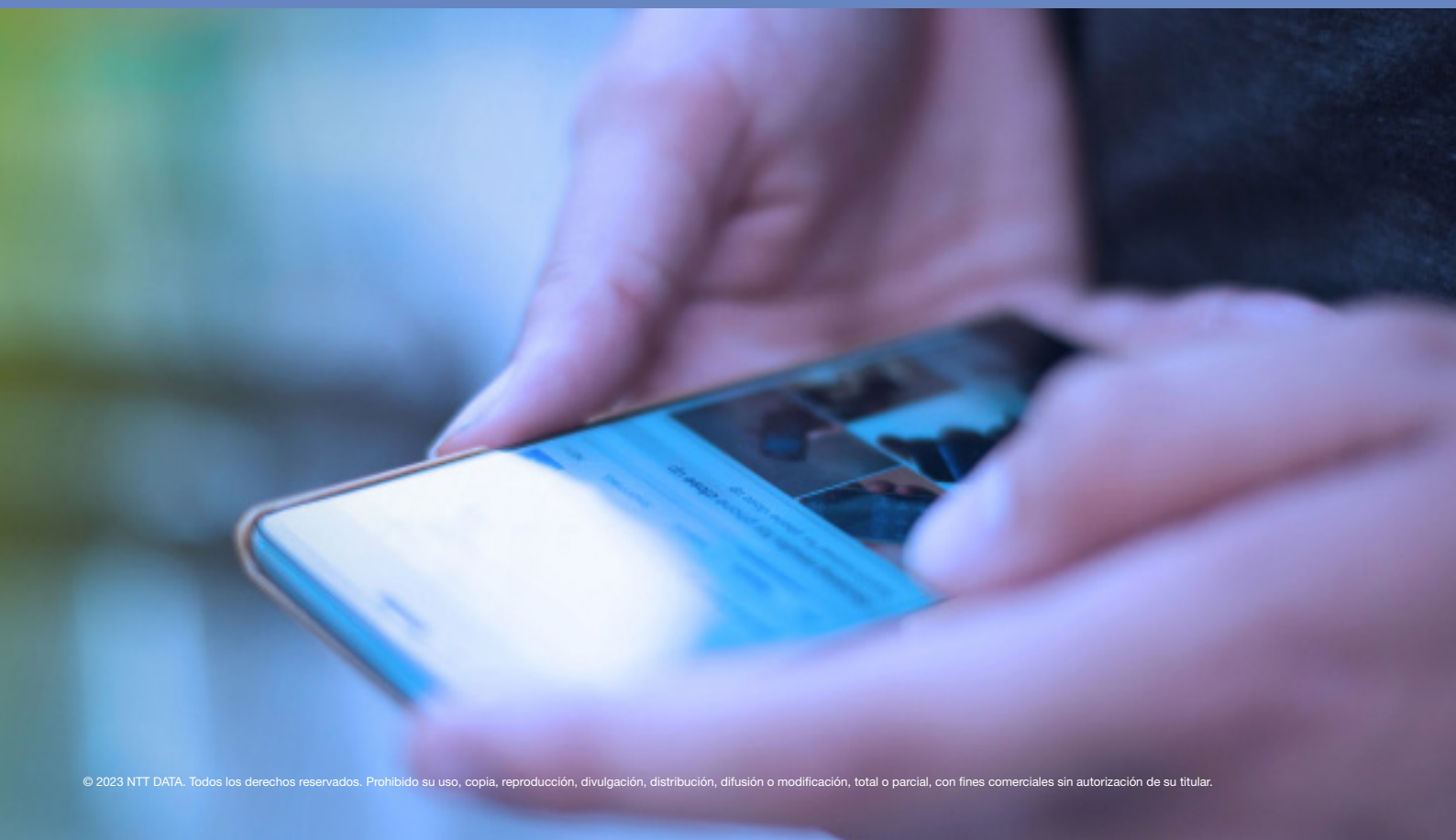
Enlace: https://www.incibe.es/incibe-cert/blog/configuraciones-seguras-en-dispositivos-industriales

Accesos externos en SCI

El acceso externo es una tecnología que cada vez más será implementada en las empresas debido a los beneficios que produce, como la comodidad que ofrece a los empleados y la reducción de los gastos.

Aun así, cabe destacar que con esta tecnología hay que tener mucho cuidado, ya que también puede provocar diferentes problemas de ciberseguridad hacia la empresa, como el acceso de usuarios no deseados o el robo de información delicada, es por ello que el uso de herramientas, como las conexiones VPN o la implementación de equipos dedicados a la monitorización, como el SOC OT, son muy importantes para garantizar la seguridad de los accesos remotos.

Enlace: https://www.incibe.es/incibe-cert/blog/accesos-externos-en-sci-arma-de-doble-filo



RESPONSABLES CIBER

María Pilar Torres Bruna

Directora de Ciberseguridad en NTT DATA Latam y Perú

maria.pilar.torres.bruna@emeal.nttdata.com

Carla Passos Schwarzer

Directora de Ciberseguridad en NTT DATA Brasil

carla.passosschwarzer@emeal.nttdata.com

Miguel Angel Garzon Ramirez

Manager de Ciberseguridad en NTT DATA Colombia

miguel.angel.garzon.ramirez@emeal.nttdata.com

Fernando Vilchis

Director de Ciberseguridad en NTT DATA México

fernando.vilchisrivero@emeal.nttdata.com

Nestor Gerardo Ordoñez

Manager de Ciberseguridad en NTT DATA EE.UU

nestor.ordonez.ramirez@emeal.nttdata.com

Jose Uzcategui

Manager de Ciberseguridad en NTT DATA Chile

jose.uzcategui@emeal.nttdata.com


NTT DATA
Trusted Global Innovator
powered by the
cybersecurity NTT DATA team
nttdata.com