NÚMERO 77 | ABRIL 2023

NTT DATA
Trusted Global Innovator

Radar

El magazine de ciberseguridad

SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA INTIMIDAD:ASPECTOS RELEVANTES PARA EL CONSEJO DE ADMINISTRACIÓN.

Los errores humanos, la falta de control, los fraudes internos o las acciones delictivas en el tratamiento de la información son cuestiones que empiezan a estar en la agenda de los Consejos de Administración de las empresas, ya que pueden provocar la paralización del negocio, pérdidas económicas directas (millones de US$), incumplimiento de la legislación e impacto negativo en la imagen, reputación y credibilidad de la empresa. Todo ello, no permite a la organización alcanzar adecuadamente sus objetivos corporativos.

La información es el recurso que permite la planificación de la organización y la operatividad de su negocio. Sin información disponible y protegida, la organización puede sufrir un incidente que, dependiendo de su tamaño y tipo de negocio, puede dejarla fuera del mercado durante un tiempo o para siempre, lo que afecta directa y negativamente a los accionistas.

Uno de los principios del Gobierno Corporativo es la “Sostenibilidad de la Organización”. Esto significa la continuidad de la información para llevar a cabo los servicios y/o elaborar los productos que pone a disposición del mercado. Por tanto, es responsabilidad del Consejo de Administración garantizar la existencia de un adecuado proceso de protección de la información.

Los accionistas, a través del Consejo de Administración, necesitan conocer los ciberriesgos y la madurez de protección de la información de la organización. Este nivel de madurez es el resultado de una evaluación detallada de diversos controles de seguridad de la información, ciberseguridad y protección de la privacidad. El Consejo necesita conocer la existencia (o no) de controles que eviten o minimicen la pérdida, robo o indisponibilidad de la información. Necesitan conocer la resistencia de la protección de la información.

El Centro para la Seguridad del Foro Económico Mundial, la Internet Security Alliance y la National Association of Corporate Director, en su documento Principles for Board Governance of Cyber Risk (2021), recomiendan que el Consejo de Administración y la Alta Dirección, se planteen una “organización ciber-resistente”:

- La ciberseguridad al servicio de la estrategia empresarial.
- Impulsores económicos e impacto del ciberriesgo.
- Alineación de la gestión del ciberriesgo con las necesidades de la empresa.
- Garantizar que la estructura organizativa respalde la ciberseguridad.
- Integrar la experiencia en ciberseguridad en la gobernanza del Consejo.
- Fomentar la resistencia y la colaboración sistémicas.

Nuestra Revista Radar de este mes presenta controles y nuevas tecnologías para facilitar la protección de la información y la generación de mejor información para el Consejo de Administración. FAIR (Factor Analysis Information Risk), una metodología cuantitativa de gestión de riesgos; Inteligencia Artificial y consideraciones sobre ChatGPT, y Tecnología Operativa (OT) que, según estimaciones de Gartner, tiene un mercado diez veces mayor que el de las Tecnologías de la Información (TI).

Enrique Bernao Rosado

Cybersecurity Manager en NTT DATA Europe & Latam

CIBERCRÓNICA

Iniciamos nuestra Cibercrónica con una preocupación que aqueja a muchas organizaciones a nivel mundial y es que GoDaddy, una de las principales compañías de alojamiento web del mundo, ha reportado una brecha de seguridad que ha comprometido su entorno de alojamiento compartido cPanel.

Según la empresa, atacantes desconocidos lograron ingresar a sus servidores y robar código fuente, así como también instalar malware en los sistemas. A pesar de que los informes de los clientes alertaron a GoDaddy sobre esta violación de seguridad a principios de diciembre de 2022, los atacantes lograron obtener acceso a la red de la compañía varios años antes.

> "BlackLotus, un bootkit sigiloso y extensible del firmware unificado (UEFI) que se ha convertido en el primer malware de conocimiento público capaz de evadir las defensas de Secure Boot"

Durante este tiempo, los atacantes pudieron utilizar sitios comprometidos para redirigir el tráfico a varios dominios desconocidos. Dado que GoDaddy es uno de los mayores registradores de dominios del mundo, esto es motivo de preocupación para los más de 20 millones de clientes en todo el mundo que utilizan sus servicios de alojamiento.

Por otra parte, ha aparecido BlackLotus, un bootkit sigiloso y extensible del firmware unificado (UEFI) que se ha convertido en el primer malware de conocimiento público capaz de evadir las defensas de Secure Boot, convirtiéndose en una amenaza potente en el panorama cibernético.

"Este bootkit puede ejecutarse incluso en sistemas Windows 11 totalmente actualizados con UEFI Secure Boot habilitado". Como podemos recordar, los bootkits de UEFI se despliegan en el firmware del sistema y permiten el control total del proceso de arranque del sistema operativo (SO), lo que hace posible desactivar los mecanismos de seguridad a nivel de SO y desplegar cargas útiles arbitrarias durante el inicio con altos privilegios.

Este kit de herramientas potente y persistente se ofrece a la venta por USD$ 5,000 (y USD$ 200 por cada nueva versión posterior) y está programado en ensamblador y C y tiene un tamaño de 80 kilobytes. También cuenta con capacidades de geocercado para evitar infectar computadoras en Armenia, Bielorrusia, Kazajstán, Moldavia, Rumania, Rusia y Ucrania.

Desde el otro lado del mundo, el grupo de ciberespionaje chino Mustang Panda, alineado con China, ha sido visto utilizando un nuevo backdoor personalizado llamado MQsTTang como parte de una campaña de ingeniería social en curso que comenzó en enero de 2023. MQsTTang utiliza el protocolo de mensajería de IoT MQTT para las comunicaciones de control y comando.

Los ataques del grupo se han dirigido a entidades europeas en el contexto de la invasión de Ucrania por parte de Rusia el año pasado, aunque también se han observado ataques contra entidades desconocidas en Bulgaria y Australia, así como contra una institución gubernamental en Taiwán.

El backdoor MQsTTang permite la ejecución de comandos arbitrarios recibidos de un servidor remoto y se distribuye a través de archivos RAR que contienen un ejecutable que presenta nombres de archivo con temáticas diplomáticas. Los hallazgos se producen días después de que Symantec revelara una operación de ciberespionaje llevada a cabo por el grupo estatal chino APT41, que se dirigió a dos subsidiarias de un conglomerado asiático en el sector de materiales y compuestos.

Por otra parte, nos movemos hacia México, donde se ha detectado una nueva cepa de malware de cajeros automáticos llamada FiXS, la cual ha estado apuntando a bancos desde principios de febrero de 2023. FiXS se esconde dentro de otro programa que no es malicioso, y es compatible con cualquier máquina de cajero automático que soporte CEN/XFS. Se cree que los atacantes encontraron una manera de interactuar con el cajero automático a través de la pantalla táctil. Una de las características notables de FiXS es su capacidad para dispensar dinero 30 minutos después del último reinicio del cajero automático. FiXS es similar a otra cepa de malware de cajero automático llamada Ploutus.

Esta última ha permitido a los ciberdelincuentes extraer dinero de los cajeros automáticos utilizando un teclado externo o enviando un mensaje de texto. FiXS es la última de una larga lista de malware que ha apuntado a los cajeros automáticos para robar dinero. Se debe tener en cuenta que este tipo de malware se puede llegar a extender a la región y llegar a afectar cajeros de USA, centro y sur américa.

De esta manera cerramos nuestra Cibercrónica, seguiremos informando sobre actuales noticias del mundo de la ciberseguridad.

LA IMPORTANCIA DE UNA GESTIÓN EFECTIVA DE RIESGOS DE CIBERSEGURIDAD EN LAS ORGANIZACIONES

Por: NTT DATA Europe & Latam

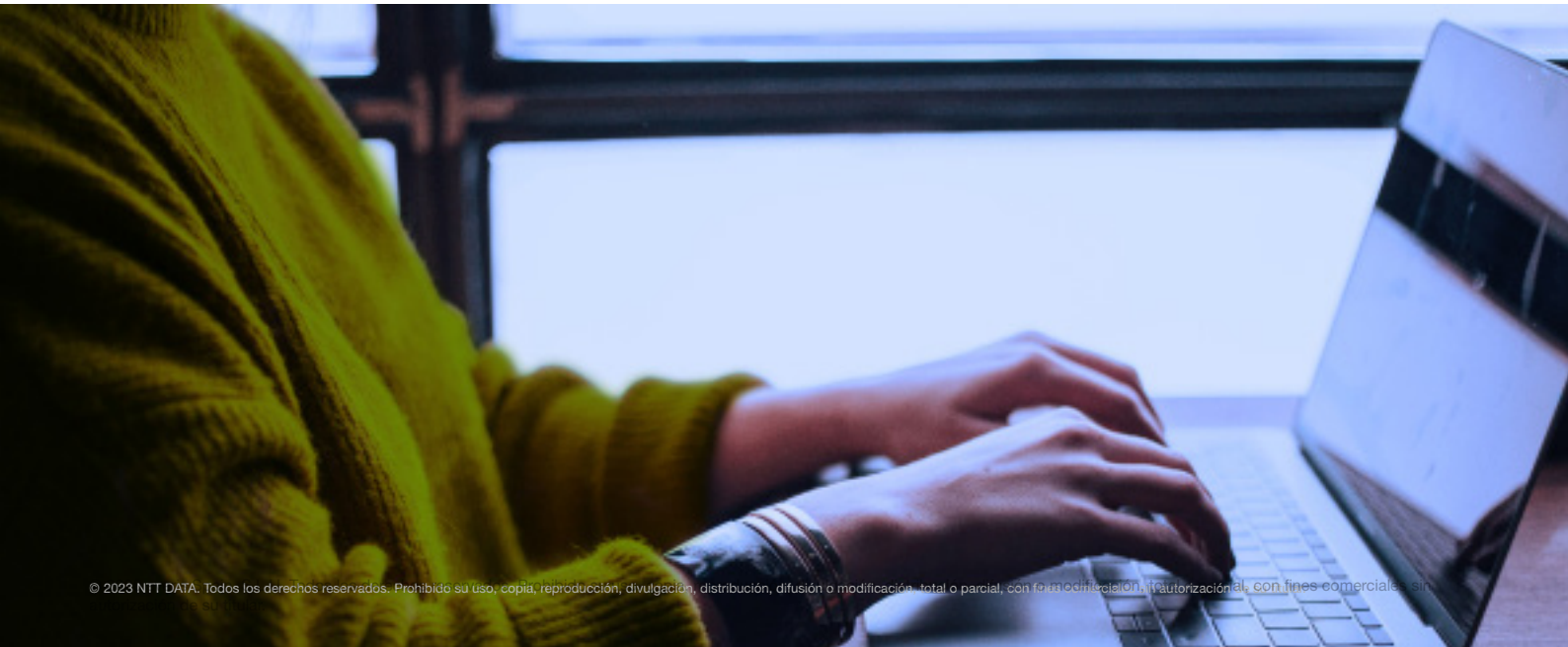
La gestión de riesgos de seguridad de la información y ciberseguridad busca garantizar las acciones que respalden la integridad, confidencialidad y disponibilidad de los activos de la información dentro de las organizaciones. Muchas compañías ya tienen una metodología de gestión de riesgos de seguridad de la información definida y madura, además de estar comprometidos a realizar acciones para tratar y mitigar sus riesgos pasando por diferentes etapas de identificación, el análisis y la evaluación, así como el tratamiento del riesgo.

Actualmente existen muchas metodologías y marcos de referencia publicados y aplicados para la gestión de riesgos, sobre los cuales observamos que las organizaciones en su mayoría optan por alinearse a métodos de evaluación cualitativos, lo cual les ha servido para determinar el valor que representan los riesgos en materia de impacto y probabilidad.

Si bien en determinados casos, la metodología definida asigna rangos cuantitativos de exposición de riesgo, esta asignación es una "posibilidad" mas no una "probabilidad" como tal sustentada en información que lo soporte.

En relación con los riesgos de SI, los principales actores clave como son los CISOs, Gestores de riesgos de seguridad, responsables de Tecnología, los directivos y socios entre otros, se cuestionan lo siguiente:

- ¿La gestión que realizamos es suficiente para responder y sustentar las inversiones de seguridad que necesitamos hacer?
- ¿Los resultados de la gestión de riesgos que aplicamos sirve para sustentar la valorización de riesgos críticos para la compañía?
- ¿El impacto final que representa para la organización analiza valores en base a declaraciones de posibilidad cercanas a la realidad?
- ¿La metodología de riesgos es un apoyo para sustentar la planificación de acciones a realizar como parte del programa de seguridad de información en un horizonte de corto, mediano y largo plazo considerando la urgencia y las principales dolencias que tenemos?



La alternativa del uso de métodos cuantitativos que ayuden a definir con mejor exactitud las decisiones a tomar está generando un mayor interés debido a la importancia de sustentar los costes que podrían comprometerse en caso de En caso de que se presente y se haga efectivo un, así como la necesidad de sustentar las inversiones en seguridad.

Adicionalmente, la toma de decisiones correctas en base a información relevante representa un gran reto en cualquier proceso de las compañías. La gestión de riesgos de seguridad de información y ciberseguridad no es la excepción: analizar información para conocer de forma cercana la probabilidad de que ocurra un evento de riesgo ayudará a actuar de forma proactiva aplicando controles necesarios.

Por el contrario, actuar de forma reactiva cuando el "incendio" ya ha ocurrido podría impactar de sobremanera.

Es por esto que los responsables se encuentran en búsqueda de mejorar sus análisis de riesgo y enfocarlos a valores tangibles en términos monetarios de pérdida, lo cual les brinda la capacidad de llevar a la gestión de riesgos a un siguiente nivel, siendo capaces de sustentar las inversiones requeridas.

Además, podrán definir con este valor la asignación de un horizonte de implementación a corto, mediano y largo plazo.

Para aplicarlo, una buena alternativa es el uso del marco FAIR definida inicialmente para riesgos de ciberseguridad (se puede utilizar para analizar otros tipos de riesgos).

Este marco analiza el riesgo en base a una taxonomía jerárquica, sobre el cual, un primer nivel está compuesto por "frecuencia del evento de pérdida" y "magnitud de la pérdida".

Estos términos en siguientes niveles se componen por otros valores que en suma ayudarán a llegar al dato del valor del riesgo de forma independiente considerando el escenario al cual se enfrenta.

Ahora bien, las compañías que deseen comenzar a utilizar una metodología de análisis de riesgo cuantitativa deben atravesar procesos de transformación y transición, sobre todo para ser capaces de medir pérdidas, resiliencia de sus controles y porcentaje de éxito de atacantes.

Como parte del proceso de adopción de la nueva metodología estará la medición de estas variables o la puesta en marcha de nuevos controles que permitan a la organización tener información válida en los siguientes meses.

Para comenzar el camino, las organizaciones pueden utilizar información basada por ejemplo en el sector, siempre y cuando represente una buena fuente de datos. Esto servirá para retar a los supuestos y efectuar el análisis con estimaciones de mayor acierto, lo cual será de mayor valor para las empresas.

En este proceso de adopción, por último, las compañías pueden mirar las metodologías de análisis de riesgos cuantitativa y cualitativa como complementarias, y es que no es necesario que la cualitativa desaparezca.

Se puede decidir ejecutar el análisis cuantitativo en los escenarios de mayor impacto para la organización y enfocarse en obtener la información de esos casos únicamente.

Una famosa frase de Peter Drucker dice que "Lo que no se puede medir no se puede controlar; lo que no se puede controlar no se puede gestionar; lo que no se puede gestionar no se puede mejorar."

Pues bien, lo positivo de este nuevo enfoque es que permite medir y cuantificar el impacto económico de un ataque en una organización. Y esto nos permitirá controlar, gestionar y mejorar el proceso de gestión de riesgos.

IMPACTO DE LOS CIBER INCIDENTES EN INFRAESTRUCTURA CRÍTICAS EN NUESTRA VIDA DIARIA

Por: NTT DATA Europe & Latam

La última edición de la revista de seguridad informática "Cybersecurity Today" informó sobre los recientes ataques cibernéticos en entornos industriales y la necesidad de mejorar la seguridad en estas áreas.En los últimos meses, ha habido varios ataques cibernéticos en la industria que han causado interrupciones en la producción y pérdidas financieras considerables. Uno de los ataques más notables fue el que afectó a una importante planta de producción de petróleo y gas en el Medio Oriente, que se vio obligada a cerrar temporalmente debido a una intrusión en su sistema de control industrial.

Ciberseguridad Industrial, riesgo de vidas humanas.

La ciberseguridad industrial es de vital importancia para salvaguardar la vida de las personas. Las infraestructuras críticas, como las plantas de energía, las plantas de tratamiento de agua y las instalaciones de transporte, están altamente automatizadas y dependen de los sistemas de control industrial para su correcto funcionamiento. Un ciberataque en estos sistemas puede causar graves daños a la salud pública, el medio ambiente y la economía.

Por lo tanto, es crucial que estas instalaciones cuenten con medidas de seguridad sólidas para proteger sus sistemas de control industrial contra posibles amenazas cibernéticas.

La ciberseguridad industrial no solo protege las infraestructuras críticas, sino que también ayuda a garantizar la continuidad de la producción y el suministro de bienes y servicios esenciales para la sociedad. En resumen, la ciberseguridad industrial es fundamental para salvaguardar la vida de las personas y proteger la economía de los posibles efectos dañinos de un ciberataque.

Ciberataque a planta de agua.

En febrero de 2021, se informó de un ciberataque a una planta de tratamiento de agua en la ciudad de Oldsmar, Florida, en Estados Unidos. Según las autoridades locales, un hacker desconocido logró acceder a los sistemas de la planta y aumentó el nivel de hidróxido de sodio (NaOH) en el agua tratada.

El ataque fue detectado rápidamente por un operador de la planta, quien notó un aumento en el nivel de NaOH en el agua tratada y lo corrigió antes de que se produjera algún daño. La planta fue desconectada temporalmente de Internet y se llevó a cabo una investigación para determinar la naturaleza del ataque y su origen.

Las autoridades locales y federales confirmaron que el ataque fue perpetrado por un hacker externo y que fue realizado a través de un software de acceso remoto no autorizado. La planta de tratamiento de agua mejoró sus medidas de seguridad e implementó nuevas medidas para proteger sus sistemas de control industrial.

Este incidente destaca la necesidad de mejorar la ciberseguridad en las infraestructuras críticas, como las plantas de tratamiento de agua, para evitar posibles daños a la salud pública y el medio ambiente. Las autoridades locales y federales han instado a todas las instalaciones críticas a que revisen sus sistemas de seguridad y actualicen sus medidas de protección contra posibles ciberataques

¿Qué medidas debe tomar la industria para protegerse con herramientas de ciberseguridad en entornos industriales?

Aquí exponemos algunas de estas medidas:

1. Implementar una política de seguridad: La industria debe establecer una política de seguridad clara y detallada, que describa los procedimientos de seguridad que deben seguirse para garantizar la protección de los sistemas de control industrial. Esto puede incluir reglas de acceso, políticas de contraseñas y medidas de seguridad física.
2. Utilizar herramientas de seguridad: La industria debe implementar herramientas de seguridad, como firewalls, sistemas de detección de intrusiones y software antivirus, para proteger los sistemas de control industrial contra posibles amenazas. Estas herramientas pueden ayudar a detectar y prevenir ataques cibernéticos antes de que causen daños.

3. Actualizar regularmente el software: La industria debe actualizar regularmente el software de los sistemas de control industrial para garantizar que estén protegidos contra las últimas amenazas de seguridad. Esto puede incluir aplicar parches de seguridad y actualizaciones de software para cerrar vulnerabilidades conocidas.
4. Limitar el acceso: La industria debe limitar el acceso a los sistemas de control industrial a solo aquellos empleados que necesitan acceso para realizar sus funciones. Se pueden implementar controles de acceso físicos y lógicos para garantizar que solo se permita el acceso a los sistemas a personas autorizadas.
5. Realizar pruebas de penetración: La industria debe realizar pruebas de penetración regulares para evaluar la eficacia de sus medidas de seguridad. Esto puede ayudar a identificar posibles vulnerabilidades y áreas que necesiten mejoras en la protección de la seguridad.

¿Por qué es importante el desarrollo de un Plan de Emergencia?

Un plan de emergencia para ataques cibernéticos a la industria OT debe ser integral y abarcar todas las fases del proceso, desde la prevención hasta la recuperación. Las organizaciones dado la superficie de amenaza actual y debido a la proliferación de nuevos ciberdelincuentes, deben estar no solo al tanto de campañas con objetivos industriales, sino que además deben considerar sistémicamente pilares defensivos para minimizar el impacto de un ataque dirigido a su organización.

A continuación, se describen las acciones clave que deben incluirse en un plan de emergencia efectivo:

- Preparación: identificar los activos críticos y los puntos vulnerables de la infraestructura OT, evaluar los riesgos y establecer medidas de seguridad adecuadas para prevenir ataques.
- Detección: establecer sistemas y herramientas de detección de intrusiones para detectar ataques en tiempo real.
- Contención: aislar los sistemas afectados y detener la propagación del ataque.
- Investigación: determinar la causa y alcance del ataque, recopilar información y documentar los hechos.
- Mitigación: implementar medidas para minimizar los daños causados por el ataque.
- Recuperación: restaurar los sistemas y la funcionalidad de la infraestructura OT a su estado previo al ataque.
- Evaluación: revisar el plan de emergencia y las acciones tomadas, identificar posibles mejoras y ajustar el plan en consecuencia.

Es importante destacar que un plan de emergencia efectivo debe ser práctico, accesible y actualizado regularmente. Además, es esencial que todos los empleados estén familiarizados con el plan y sepan su papel en caso de un ataque cibernético. La colaboración y el trabajo en equipo son esenciales para una respuesta efectiva a un ataque cibernético en la industria OT.

La prevención de incidentes OT es un proceso continuo y requiere un compromiso constante de la organización. Al adoptar medidas de seguridad efectivas y trabajar en colaboración con expertos en seguridad, las organizaciones pueden proteger sus activos industriales y garantizar la continuidad del negocio.

TENDENCIAS

GPT: Una puerta que abre caminos

Si bien en nuestra última edición explicamos algunas generalidades de ChatGPT (chatbot desarrollado por OpenAI) en cuanto a su definición, objetivo, pros y contras de cara al usuario común, se hace necesario también hablar del impacto que comienza a forjarse a nivel corporativo para su adopción y gracias a la evolución del modelo GPT.

Desde que se liberó su uso en noviembre 2022, ChatGPT ha sido el foco de un debate constante en materia de seguridad. Sin embargo, es importante hacer una retrospectiva para darnos cuenta de su progreso y el papel de tenerlo como aliado para darle ese tinte de confiabilidad en el ámbito empresarial.

Como es sabido por todos, OpenAI es una compañía gobernada por la organización sin ánimo de lucro -OpenAI Incorporated- pero además conformada por otra subsidiaria con fines de lucro -OpenAI Limited Partnership., Desde que comenzaron a desarrollar su idea en el 2015 fue solo hasta el 2019 cuando dieron inicio a su relación con uno de los gigantes tecnológicos -Microsoft- para entrenar sus modelos con tecnología Azure, facilitando de esta manera que OpenAI no renunciara a su propósito de investigación y por otro lado, Microsoft continuara madurando sus productos como su proveedor exclusivo en la nube hasta tal punto de llegar a implementar una interfaz de aplicaciones (API) que le permitiera su llegada tanto al mundo empresarial como a los desarrolladores para construir soluciones de una manera más segura sobre sus modelos GPT, CODEX y DALL-E

En términos sencillos, los definiremos:

- GPT, ejecuta una variedad de tareas de lenguaje natural, usado para ejecutar preguntas-respuestas, resúmenes de texto, traducción automática y conversación AI.
- CODEX, basado en GPT-3 convierte el lenguaje natural en código. No está diseñado para reemplazar el trabajo de los programadores, lo que busca es ayudarles en la codificación de ciertos fragmentos rutinarios u optimizar código existente.
- DALL.E, crea imágenes a partir de una descripción en lenguaje natural.

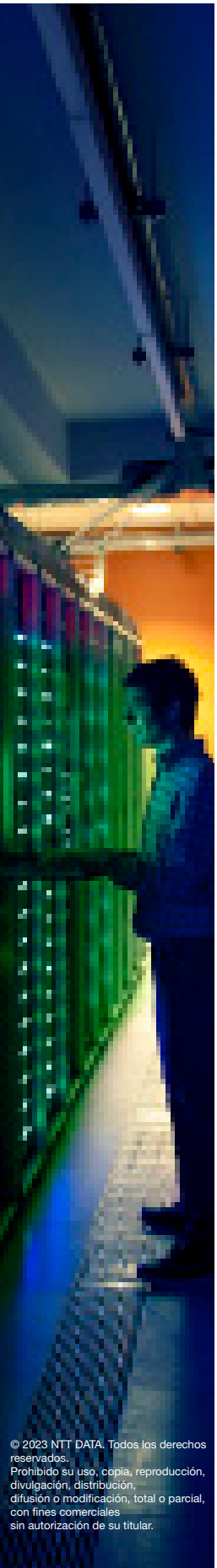
Con todo el auge y las bondades del ChatGPT, algunos de estos modelos pueden pasar desapercibidos, aunque ya empiezan a cobrar relevancia en el entorno de las grandes compañías para aportar mejoras en los tiempos de respuesta, en efectividad y en la experiencia de usuario, factores que vienen siendo determinantes en los últimos años en la interacción de usuario con respecto a un producto o servicio.

Finalmente, es sumamente importante aclarar que el simple hecho de contar con uno de estos módulos, no implica que todo funcionará como por arte de magia para la organización, hay que ser conscientes que solo forman una parte de la solución y alrededor de ellos habrá una pieza importante para trabajar sobre los controles a implementar en la comunicación de los servicios a ser definidos en el backend y asegurar que tanto los usuarios internos como externos que tengan acceso sean validados y reciban lo que sus funciones les permitan.

Para esto, se hace necesario no perder de vista dos conceptos que siempre irán de la mano y son complementarios en el éxito de una solución hoy, SEGURIDAD y PRIVACIDAD. La SEGURIDAD orientada a protegerse contra las amenazas maliciosas mientras que la PRIVACIDAD garantiza que solo aquellos usuarios que estén autorizados para acceder a los datos puedan hacerlo.

VULNERABILIDADES

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



Fortinet

CVE-2023-25610
Fecha: 08/03/2023

Descripción. El pasado 8 de marzo se publicó una vulnerabilidad crítica que afecta a la interfaz administrativa de FortiOS y FortiProxy y que podría permitir a un atacante ejecutar código arbitrario en el dispositivo o realizar un ataque de DOS en la interfaz gráfica del usuario mediante él envió de peticiones específicamente diseñados para ello. La Vulnerabilidad CVE-2023-25610 seria provocada por un "buffer underflow" o subdesbordamiento del buffer. En este tipo de vulnerabilidad el buffer de la aplicación cargaría la información que se le proporcionase a una velocidad inferior al tiempo de procesamiento de este, lo que provocaría una solicitud de memoria adyacente.

Enlace: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25610
https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-productos-fortinet-0
https://www.fortiguard.com/psirt/FG-IR-23-001

Productos afectados. Esta vulnerabilidad afecta a las siguientes versiones de FortiOS y FortiProxy:

- FortiOS: 7.2.0 hasta la 7.2.3.; 7.0.0 hasta la 7.0.9.; 6.4.0 hasta la 6.4.11.; 6.2.0 hasta la 6.2.12.; 6.0 todas sus versiones.
- FortiProxy: 7.2.0 hasta la 7.2.2.; 7.0.0 hasta la 7.0.8.; 2.0.0 hasta la 2.0.11.; 1.2 todas sus versiones.; 1.1 todas sus versiones.

Solución: La solución principal para solventar esta vulnerabilidad consiste en actualizar FortiOS o FortiProxy a las siguientes versiones:

- FortiOS: 7.4.0 o superiores.; 7.2.4 o superiores.;7.0.10 o superiores.; 6.4.12 o superiores.; 6.2.13 o superiores.
- FortiProxy: 7.2.3 o superiores.;7.0.9 o superiores.;2.0.12 o superiores.
- FortiOS-6K7K: 7.0.10 o superiores.;6.4.12 o superiores.;6.2.13 o superiores.

El fabricante también ha proporcionado una serie de soluciones alternativas para aquellos que no puedan actualizar sus productos a estar versiones.

- Deshabilitar la interfaz de administrativa HTTP/HTTPS.
- Limitar el rango de IPs que pueden comunicarse con la interfaz administrativa de las aplicaciones.

Aruba

CVE-2023-22747; 22748;22749;22750;22751;22752.
Fecha: 01/03/2023

Descripción. On 01 March, a report was published by several researchers detailing numerous vulnerabilities that could affect Aruba products. This report notifies the existence of 33 vulnerabilities classified as: 6 critical, 19 important and 8 moderate. In the following, we will detail the critical vulnerabilities: A number of vulnerabilities have been reported that could lead an attacker to execute arbitrary code by sending specifically crafted packets to UDP port (8211) using the Aruba Networks Access point management protocol (PAPI). The CVEs for this vulnerability are as follows: CVE-2023-22747, CVE-2023-22748, CVE-2023-22749 and CVE-2023-22750. The other two critical vulnerabilities affecting Aruba products would allow through a buffer overflow the execution of arbitrary code on the system by sending specially crafted packets to UDP port (8211) using the PAPI protocol. This is a remote code execution vulnerability. The CVEs for this vulnerability are as follows: CVE-2023-22751 and CVE-2023-22752.

Enlace: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04454en_us
https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt

Productos afectados.

Las vulnerabilidades afectan a los siguientes productos de Aruba:

ArubaOS: 8.6.0.19 y versiones anteriores, ArubaOS: 8.10.0.4 y versiones anteriores, ArubaOS: 10.3.1.0 y versiones anteriores y SD-WAN: 8.7.0-2.3.0.8 y versiones anteriores. Esta vulnerabilidad también afecta a varios productos de Aruba para los cuales no se va a seguir dando soporte.

Solución: La solución principal consiste en actualizar a las siguientes versiones de los productos afectados de Aruba: ArubaOS: 8.10.0.5 y versiones siguientes; ArubaOS: 8.11.0.0 y versiones siguientes; ArubaOS: 10.3.1.1 y versiones siguientes; SD-WAN: 8.7.0.0-2.3.0.9 y versiones siguientes; Adicionalmente Aruba también ha publicado una serie de recomendaciones para minimizar las posibilidades de verse afectado por una de estas vulnerabilidades: Para minimizar las posibilidades de una explotación, se deben restringir la comunicación entre el controlador/puertas de acceso y el punto de acceso mediante un segmento único de capa 2 o una Vlan. Adicionalmente, si el controlador/puertas de enlace y puertas de enlace cruzan a la capa 3 se aconseja tener reglas del firewall que restrinjan las comunicaciones de los dispositivos. Por último, activando la seguridad extra para el protocolo PAPI que se proporciona desde el fabricante, prevendrá las vulnerabilidades.

PARCHES

Cisco

Fecha: 02-03-2023

Descripción. Cisco ha publicado una actualización de firmware para la interfaz de administración web de sus teléfonos IP de la serie 6800, 7800 y 8800, que soluciona la siguiente vulnerabilidad critica:
CVE-2023-20078: Esta vulnerabilidad podría permitir a un usuario remoto sin autorización ejecutar código arbitrario o causar un ataque de denegación de servicio en la interfaz web de administración de los teléfonos IP de Cisco de la serie 6800, 7800 y 8800. Esta vulnerabilidad era producida por un fallo en la validación de la información introducida permitiendo así a un atacante explotar esta vulnerabilidad mandando solicitudes especialmente diseñadas para ello.

Enlace:
https://cve.report/CVE-2023-20078
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP#details

Productos afectados:
- teléfonos IP Cisco versión 6800, 7800 y 8800.

Solución: Actualizar los parches de seguridad publicados por el fabricante del dispositivo correspondiente.

Apple

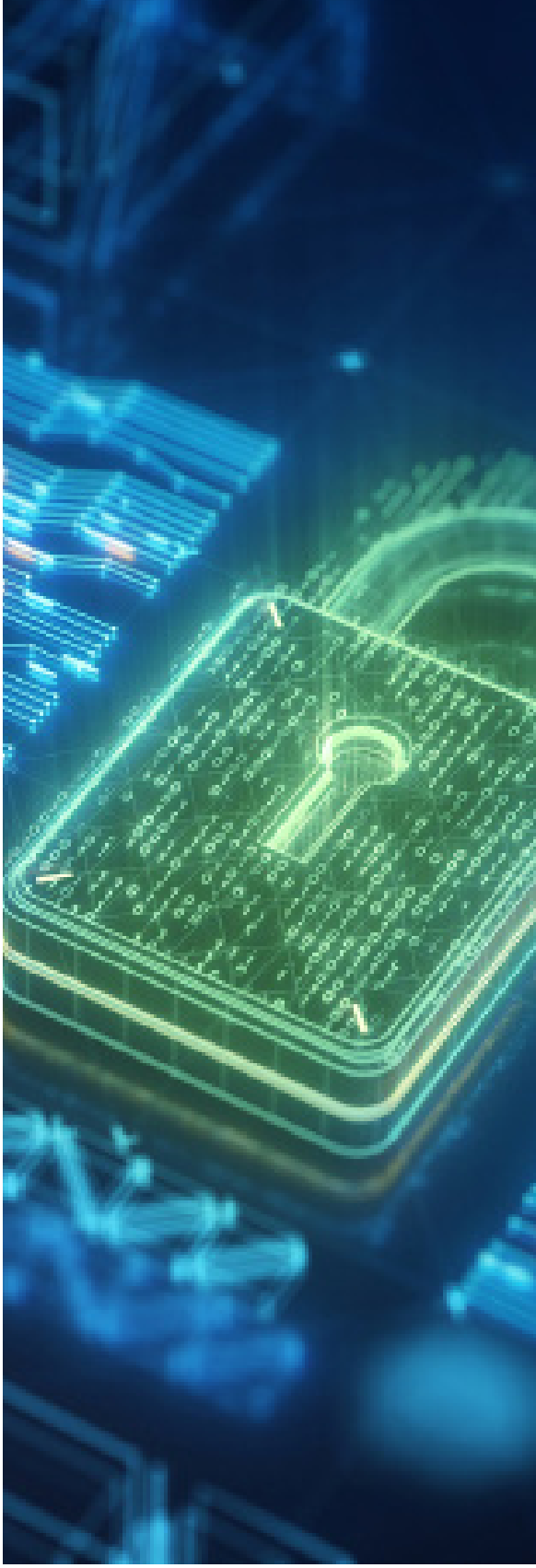
Fecha: 02-02-2023

Descripción. Apple ha publicado un reporte de seguridad en el que se indican múltiples actualizaciones para sus dispositivos iPadOS, iOS y macOS Estos parches solucionan las vulnerabilidades: CVE-2023-23531, con severidad critica, CVE-2023-23530, con severidad alta.
- CVE-2023-23531: esta vulnerabilidad permitiría a un atacante la ejecución de código arbitrario en el equipo mediante la explotación de las expresiones de NSPredicate las cuales podían saltarse la validación realizada por el componente NSPredicateVisitor lo cual permite al atacante saltarse cualquier tipo de validación.
- CVE-2023-23530: En el caso de esta vulnerabilidad un atacante podría mediante la explotación de las listas negras utilizadas por NSPredicate, las cuales impedían la utilización de ciertas clases o métodos que podían poner en entredicho la seguridad del dispositivo. El borrado de estas listas podría permitir a un atacante la ejecución de código arbitrario en el equipo.

Enlace: https://techmonitor.ai/technology/cybersecurity/apple-security-vulnerabilities-ios-macos-ipados
https://www.trellix.com/en-us/about/newsroom/stories/research/trellix-advanced-research-center-discovers-a-new-privilege-escalation-bug-class-on-macos-and-ios.html

Productos afectados:
Las vulnerabilidades corregidas afectaban a las siguientes versiones:
- MacOS 13.2 y anteriores.
- iOS 16.3 y anteriores.
- iPadOS 16.3 y anteriores.

Solución: Actualizar los parches de seguridad publicados por el fabricante del dispositivo correspondiente.



EVENTOS

Cisco Develop 2023

5 - 6 de abril de 2023 |

Un evento donde explorar las ideas y perspectivas del software empresarial y nativo de la nube con visión de futuro. Los asistentes se conectarán en persona o virtualmente para debatir perspectivas contemporáneas y aprendizajes pertinentes para trabajar con tecnologías en la nube.

Enlace: https://developer.cisco.com/develop/2023

TecnoSec

26 - 27 de abril 2023 |

El evento de Altas Tecnologías de Seguridad e Inteligencia, Tecnosec 2023, es un punto de encuentro para las instituciones y los cuerpos de seguridad de Infraestructuras Críticas. Tecnosec es el enclave ideal para propiciar encuentros nacionales e internacionales y cultivar contactos valiosos para la industria de la seguridad.

Enlace: https://www.tecnosec.es/

RSA Conference 2023

24 - 27 de abril de 2023 |

La Conferencia RSA es una de las conferencias de ciberseguridad más grandes y conocidas del mundo. Se lleva a cabo todos los años en San Francisco y atrae a más de 40,000 asistentes de todo el mundo. Los temas cubiertos en RSA incluyen todo, desde gestión de riesgos y cumplimiento hasta seguridad en la nube y seguridad móvil.

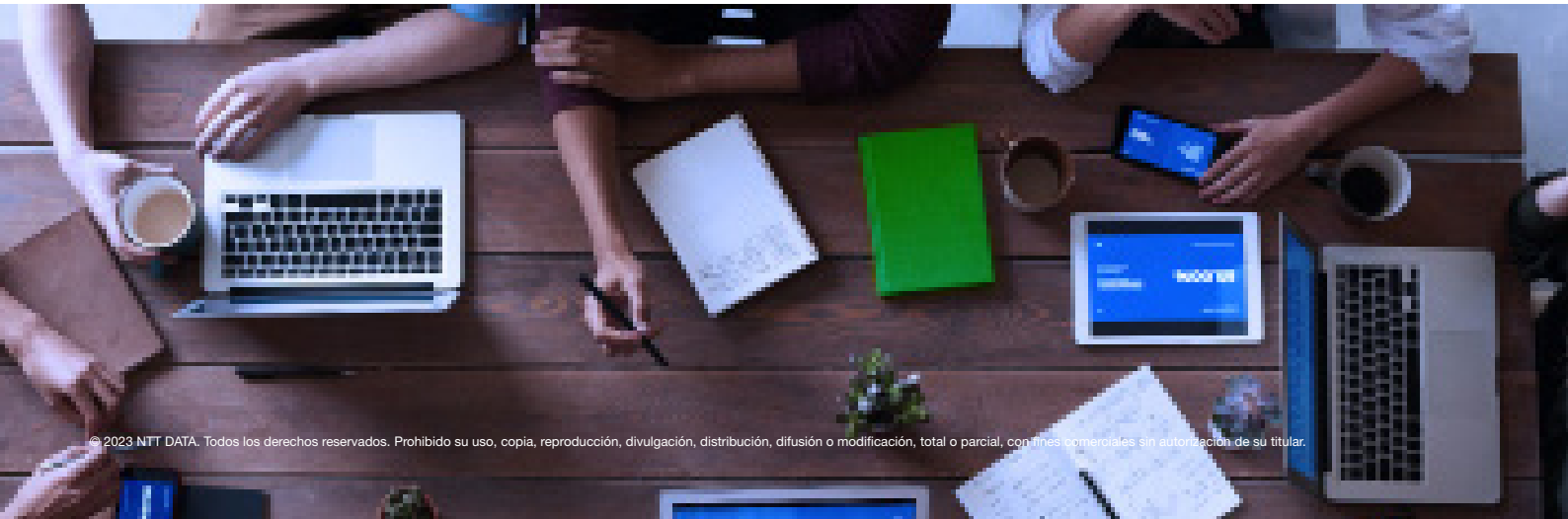
Enlace: https://www.rsaconference.com/usa

SANS Pen Test Austin 2023

17 - 22 de abril de 2023 |

SANS Pen Test Austin 2023 son seis días de formación en profundidad y práctica en pruebas de penetración, red teaming, purple teaming y desarrollo de exploits para profesionales que necesitan saber cómo encontrar vulnerabilidades dentro de sus organizaciones, comprender el riesgo y priorizar los recursos basándose en posibles ataques del mundo real.

Enlace: https://www.sans.org/cyber-security-training-events/pen-test-austin-2023/



RECURSOS

¿Conoces tus riesgos? INCIBE

Para ayudar a las empresas a evaluar su estado de ciberseguridad y a avanzar hacia mayores niveles de protección, INCIBE pone a su disposición una herramienta de autodiagnóstico especialmente diseñada para este fin. A través de una serie de preguntas se guiará al usuario para que determine su estado en seguridad de la información, qué riesgos amenazan el funcionamiento de la empresa y qué aspectos debe mejorar. Todo ello, para empezar a medir. Para empezar a mejorar.

Enlace: https://www.incibe.es/protege-tu-empresa/conoces-tus-riesgos

CSA CCM v4.0 Addendum - IBM Cloud Framework for Financial Services

Este documento es un apéndice de CSA CCM v4.0 para IBM Cloud Framework for Financial Services v1.1.0 que contiene la asignación de controles entre CCM e IBM Cloud Framework for Financial Services. El documento tiene como objetivo ayudar a las organizaciones que cumplen con IBM Cloud Framework for Financial Services a satisfacer los requisitos de CCM.

Enlace: https://cloudsecurityalliance.org/artifacts/csa-ccm-v4-0-addendum-ibm-cld-framework/

STAR Enabled Solutions FAQ

Una Solución Habilitada STAR es un producto o servicio que utiliza el marco CCM o el Cuestionario de la Iniciativa de Evaluación de Consenso (CAIQ). Sus tecnologías y herramientas han sido evaluadas y cumplen los requisitos de seguridad establecidos por la CSA. Este proceso de verificación permite a las empresas desplegar más fácilmente herramientas que se alinean o cumplen con STAR, el marco CCM, y las mejores prácticas.

Enlace: https://cloudsecurityalliance.org/artifacts/star-enabled-solutions-faq/


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