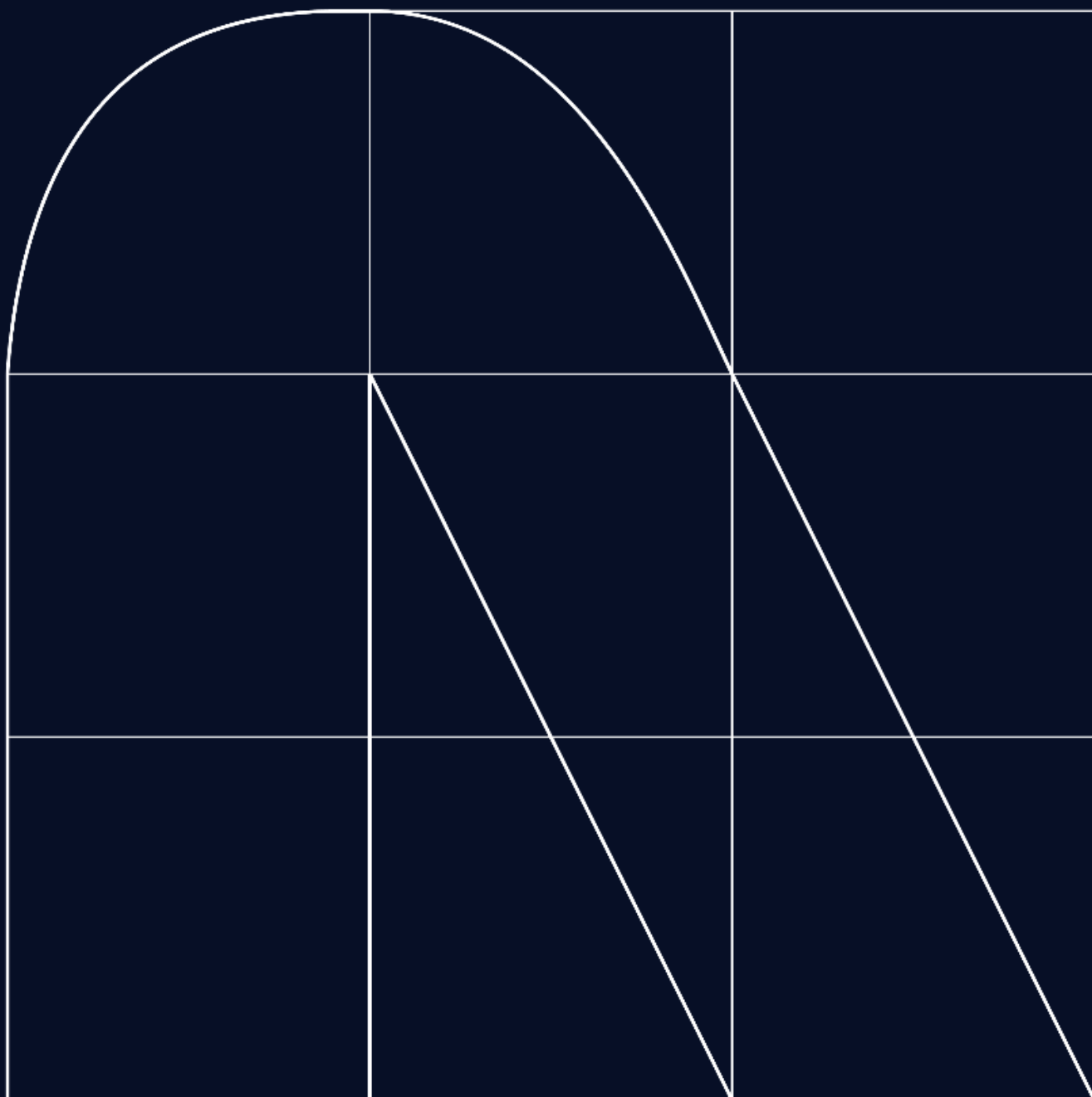
Número 87 | Febrero 2024

NTT DATA

Radar

El magazine de ciberseguridad



La importancia de saber quién es el enemigo (quien está detrás)

EDITORIAL por Jose Manuel Moreno

Empresas y organizaciones se enfrentan cada año a un mayor número de ataques, aumentando el nivel de sofisticación y provocando mayores daños tanto económicos y operativos como reputacionales a estas. Las personas o grupos que realizan este tipo de ataques, como normal general, suelen tener objetivos claros a la hora de ejecutarlos, así como sobre que víctimas o grupo de víctimas (sectores o industrias) deben realizarlo.

En el informe de Ciber_Amenazas y Tendencias 2023 publicado por CCN-CERT en el pasado mes de noviembre, se destaca el incremento de la sofisticación de los actores y grupos de amenaza, el uso de nuevas familias de malware y la evolución de los artefactos usados para realizar estos ataques.

Los ataques de rasomware siguen siendo los más números, debido principalmente al retorno, principalmente económico, que obtienen los grupos amenaza con ellos. Según el informe “Cost of a Data Breach” de IBM, el daño económico medio en el último año de dichos ataques aumento un 144% con respecto a 2022. Los grupos de amenaza que más ataques de este tipo han ejecutado han sido LockBit 3.0, BlackCat (ALPHV), Hive, Conti y REvil.

Cuando tenemos que enfrentarnos al reto de proteger nuestras organizaciones, es crucial saber quien es el enemigo, quien está detrás de esos ataques. El hecho es que no todos lo grupos amenazas tienen los mismos objetivos ni usan las mismas técnicas y tácticas, y es aquí donde la inteligencia o Threat Intelligence cobra mayor relevancia.

¿Qué nos ofrece el Threat Intelligence y como sacar ventaja al oponente?
Los servicios de Threat Intelligence tienen como objetivo para una organización obtener la mayor información posible sobre el estado de ciberseguridad, identificar a los grupos amenazas que pueden atacar a nuestra organización, conocer las tácticas, técnicas y procedimientos (TTP) que utilizan dichos actores, y en la medida de lo posible, rastrear iterativamente los ataques que realizan dichos grupos sobre cualquier organización en el mundo.

Pero, una vez conseguida toda esa información, ¿qué hacemos con ella? Los datos por sí solos no permiten mejorar o aumentar la resiliencia de nuestra organización. Es por ello por lo que existen otros servicios preventivos que toman como punto de partida el Threat Intelligence.

•**Threat Hunting** este servicio preventivo tiene como objetivo analizar de manera activa los registros de las principales líneas de defensa de una organización buscando cualquier indicio de actividad sospechosa. Para ello parte de la información de inteligencia, identificando los principales actores y huellas dejan en las victimas, para buscar ese rastro en nuestros registros de seguridad (principalmente en el SIEM). Este servicio proactivo, por tanto, puede identificar de manera temprana la presencia de estos grupos en nuestros sistemas y activar niveles de protección específicos para protegernos contra ellos.

•**Detection Rules** otro servicio preventivo que permite aumentar la resiliencia de nuestra organización creando o implementando reglas de detección adicionales que permitan identificar la presencia o intento de ella de los grupos amenaza contra nuestra organización. Para ello el equipo de Threat Intelligence debe aportar cuanta más información mejor sobre que malware, exploit o vulnerabilidades usan nuestros enemigos, para que este servicio sea capaz de crear sistemas detección precisos.

•**Adversary Simulation** es un servicio que pretende simular el comportamiento de estos grupos amenazas contra nuestra organización. Es un ejercicio que es en esencia un Red Team pero que nace con el objetivo de imitar la actuación de un grupo amenaza contra nuestra propia organización. Este equipo tendrá como objetivo utilizar, en la medida de lo posible, la mismas TTP que los grupos amenazas y usar las herramientas y exploits más usados por los grupos “imitados”. Este servicio tiene mucho valor para proteger nuestra organización y medir el nivel de resiliencia de esta contra estos actores.

Como vemos, la evolución y el grado de sofisticación de nuestros enemigos nos obliga a conocerlos con el mayor detalle posible y usar esa información para aumentar el nivel de resiliencia de nuestra organización .

José Manuel Moreno
Cybersecurity Director

Expertos advierten el peligro inminente de la IA en el phishing

Cibercrónica por Adrián Álvarez Sánchez y Pablo García Díaz

De ahí que empresas como Trend Micro constantemente adviertan sobre los peligros de los grandes modelos de lenguaje. Ya que estos no solo son capaces de llevar estafas masivas de forma simultánea, sino también de generar empatía y confianza entre las posibles víctimas. Esta capacidad de automatizar y personalizar ataques hace que sean aún más peligrosos y difíciles de detectar.

Orange sufre un ciberataque, la contraseña en concreto era "ripeadmin" y era tan simple que cualquiera podría adivinarla. El atacante, pudo acceder a la cuenta como administrador y realizar cambios en la tabla de enrutamiento global, lo que provocó que los clientes de Orange no pudieran conectarse a Internet.

Sancho Lerena, CEO de la empresa de gestión IT y seguridad Pandora FMS, considera que “el nivel de ciberseguridad que hay en España sigue siendo inferior al requerido” y ciberataques como el acontecido en Orange y el que sufrió Vodafone el año pasado lo demuestran.

Como era de esperar, el ataque tuvo un impacto enorme en los usuarios de Orange, ya que muchos usuarios experimentaron problemas de conectividad, incluidos problemas para acceder a sitios web, aplicaciones y servicios de voz y datos.

Por otro lado, la empresa de telefonía Tigo informó de un incidente de ciberseguridad que afecta al suministro normal de algunos servicios específicos a un grupo limitado de clientes del segmento corporativo, no así a ningún otro servicio masivo o corporativo de telefonía, internet o billetera electrónica.
Un ciberataque ha conseguido penetrar en los sistemas informáticos de Carrefour Servicios Financieros y sustraer información personal de sus clientes. Según ha comunicado la compañía, la información robada incluye “datos personales básicos, de contacto, número de DNI entre otros datos”.

Información como la robada a la financiera de Carrefour se considera muy sensible para la ciberseguridad personal.

Poseerla no habilita a un atacante para sustraer dinero directamente de la cuenta bancaria de la víctima o hacer compras en su nombre sin consentimiento, pero facilita enormemente las suplantaciones de identidad y las estafas. En este momento hay varias campañas de ataque de este tipo activas en España.

Se ha encontrado que ciertas versiones de org.apache.struts:struts2-core son vulnerables a la ejecución remota de código (RCE) a través de la manipulación de los parámetros de carga de archivos que permiten realizar un “path traversal” (CVE-2023-50164). Bajo ciertas condiciones, es posible subir un archivo malicioso, que puede ser ejecutado en el servidor. De hechos como este, se puede recalcar probar y sanitizar todas las entradas del servidor antes de añadirlas a las aplicaciones en producción.

Discord-Recon es un bot creado para el reconocimiento de bug bounty, escaneos automáticos y recopilando información a través de un servidor de Discord. Un atacante podría ejecutar comandos de Shell en el servidor sin tener un rol de administrador. Los desarrolladores ya se han puesto manos a la obra y han conseguido mitigar esta vulnerabilidad en la versión 0.0.8 del bot.
Esto data la importancia de no utilizar herramientas o programas de fuentes no seguras y que no hayan realizado ciertas pruebas de seguridad en servidores públicos (CVE-2024-21663).

También, se han identificado nuevos CVEs como el CVE-2023-51448 que trata sobre una vulnerabilidad dentro de la función de receptores de notificaciones SNMP de Cacti-s que podría permitir a un actor de amenaza revelar todos los contenidos de la base de datos de Cacti o, dependiendo de la configuración de la base de datos, incluso activar la ejecución de código remoto (RCE).

Ciberseguridad OT: Cómo gestionar una auditoria industrial

Por Alejandro Alonso Rodríguez

En la era digital actual, la ciberseguridad se ha convertido en un pilar fundamental para todas las industrias. Sin embargo, en el ámbito industrial, su importancia es aún mayor. La ciberseguridad industrial se ocupa de proteger los sistemas de control industrial (ICS) que son fundamentales para el funcionamiento de nuestras infraestructuras críticas. Estos sistemas, que incluyen una variedad de dispositivos y redes, son responsables de supervisar y controlar los procesos industriales en sectores como la energía, la fabricación, el transporte y las utilities.

A medida que estos sectores se vuelven cada vez más digitalizados y conectados, también se vuelven más vulnerables a una variedad de amenazas cibernéticas. Desde ataques dirigidos por actores estatales hasta incidentes causados por errores humanos, las amenazas a la ciberseguridad industrial son diversas y en constante evolución. Este artículo explorará en profundidad la importancia de la ciberseguridad industrial, las amenazas actuales y cómo las organizaciones pueden protegerse eficazmente en este panorama digital en constante cambio.

En el último informe de la empresa Claroty “The Global State of Industrial Cybersecurity 2023: New Technologies, Persistent Threats and Maturing Defenses.” (https://claroty.com/resources/reports/the-global-state-of-industrial-cybersecurity-2023) Se concluye que un 75% de las empresas industriales ha sido objetivo de un ransomware. Del total de organizaciones afectadas por ransomware, cerca de un 69% tuvo que pagar el rescate.
Esto pone de manifiesto varios hechos:
- Aunque el 47% de las empresas encuestadas se manifestó preocupada por la seguridad, el ámbito OT está lejos de la madurez de seguridad que hay en el ámbito IT. Dado que el ciclo de vida de los sistemas industriales es de 20 años, a menudo se encuentran sistemas legacy o protocolos no seguros que, en sus orígenes, no se encontraban preparados para la integración con el mundo IT y, mucho menos, con las nuevas amenazas.

- A pesar de los nuevos estándares de ciberseguridad industriales y los esfuerzos por un marco normativo común para la integridad de los procesos de OT, muchas de las empresas siguen sin tener un gobierno claro que las prepare contra ciberincidentes en entornos productivos.

Uno de los objetivos del área de ciberseguridad OT de NTT DATA es, precisamente, establecer la hoja de ruta de las empresas del sector industrial para que tengan un nivel de madurez óptimo al enfrentarse a estas amenazas.
Para ello, una de las principales armas, son los marcos normativos entre los que destacan, sobre todo, dos: La NIST 800-82 y la ISA 62443.

Las normas NIST 800-82 e ISA 62443 son dos marcos de referencia cruciales en el ámbito de la ciberseguridad, especialmente diseñadas para garantizar la seguridad de los sistemas de control industrial (SCI) y los sistemas de automatización. Ambas normativas abordan la necesidad crítica de proteger las infraestructuras críticas y los procesos industriales contra amenazas cibernéticas, que podrían tener consecuencias devastadoras.

El NIST 800-82, desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos, se centra en proporcionar pautas y recomendaciones para la seguridad de los sistemas de control industrial. Este documento abarca desde la evaluación de riesgos hasta la implementación de medidas de seguridad efectivas, asegurando la integridad, confidencialidad y disponibilidad de los sistemas en entornos industriales.

Por otro lado, la norma ISA 62443, creada por la Sociedad Internacional de Automatización (ISA), es un estándar global que se enfoca en la seguridad cibernética de los sistemas de automatización y control. Este marco ofrece una estructura integral para la identificación, evaluación y mitigación de riesgos cibernéticos en los sistemas de control, considerando aspectos específicos de la seguridad en procesos industriales.

Ambas normativas son esenciales para establecer prácticas de ciberseguridad robustas en entornos industriales, contribuyendo a la protección de activos críticos, la continuidad operativa y la salvaguarda de la integridad de los procesos industriales ante las crecientes amenazas.

Sin embargo, es necesario huir de la "consultoría de papel" y no limitar la ciberseguridad a una "checklist" de controles. Es necesario aportar un valor añadido y que, tanto el ámbito estratégico como el ámbito técnico avancen de la mano durante un proyecto de ciberseguridad OT.
Por eso en NTT DATA, durante un proyecto de gobierno OT, seguimos varias etapas donde, cada una, es un nivel más profundo, más técnico y más detallado que el anterior.

Son 8 niveles fundamentales que hay que revisar y por los que hay que guiarse cuando se afronta un proyecto de ciberseguridad industrial:

1. **Politicas, procedimientos y concienciación**: La base de la ciberseguridad en entornos operacionales reside en el establecimiento de políticas y procedimientos robustos. Estas directrices proporcionan la estructura necesaria para enfrentar amenazas en sistemas de control industrial. La concienciación del personal, por otro lado, es igualmente esencial, cultivando una comprensión profunda de los riesgos y fomentando prácticas seguras. Un personal bien informado es una línea de defensa crucial contra posibles ataques, y la claridad de las políticas garantiza una implementación efectiva.

Debe existir, al menos, una política de seguridad general que incluya el entorno OT y unos procedimientos operativos claros (gestión de actualizaciones, gestión de permisos, gestión de copias de seguridad...etc).

En muchas ocasiones, se observa que el conocimiento operativo reside en unas pocas personas y esto hace que los procesos sean extremadamente dependientes, que no haya responsabilidades claramente definidas y que la transmisión de conocimiento interna sea poco efectiva o inexistente

2. **Segmentación de red**: La segmentación de red desempeña un papel vital en la protección de sistemas críticos. Al dividir la infraestructura en segmentos, se limita la propagación de amenazas y se asegura que los sistemas cruciales operen en un entorno controlado. Este enfoque estratégico minimiza riesgos y salvaguarda la continuidad operativa, asegurando que incluso en caso de una intrusión, el impacto se mantenga bajo control. Gracias a la ISA 62443, tenemos las herramientas para poder definir las zonas de seguridad, los conductos de comunicación y poder adecuar las medidas de seguridad a los requisitos de cada zona. No todas las zonas de red en un entorno OT requieren el mismo grado de protección ni la misma atención.

3. Defensa de protocolos y transporte: La seguridad en las capas de transporte y protocolos es esencial para mantener la integridad de las comunicaciones en entornos industriales. Resistir ataques a estas capas significa garantizar la autenticidad y la confidencialidad de los datos transmitidos. La implementación de medidas de seguridad robustas en este ámbito es crucial para proteger la comunicación entre dispositivos y sistemas de control.

Muchos de los protocolos OT que se usan a día de hoy, por naturaleza, son poco seguros (Modbus, Profinet-DCP...etc). Sin embargo, esto no quiere decir que no podamos implementar medidas de seguridad perimetrales o medidas mitigatorias para contener ataques en caso de que una de sus vulnerabilidades sea explotada.

4. Seguridad de red: La configuración y gestión efectiva de dispositivos de red son los pilares de una red segura. Firewalls, sistemas de prevención de intrusiones y la detección y respuesta en tiempo real son elementos clave para defender contra amenazas cibernéticas. Una red bien protegida proporciona la base necesaria para la operación segura y confiable de sistemas de control industrial. Uno de los puntos clave, cuando hablamos de entornos de operación, es la visibilidad. No podemos proteger lo que no podemos ver. Por esto es importante el despliegue de sistemas de monitorización y vigilancia de activos.

Muchos de los sistemas actuales como Nozomi, Claroty, Armis...etc están perfectamente adaptados para hacer este descubrimiento de activos de manera pasiva. Controlar nuestros activos OT, nos hace ser conscientes de nuestra superficie de ataque y priorizar la resolución de vulnerabilidades, segmentación y contención de los ataques.

Igualmente, importante es el análisis de las políticas de red implementadas en elementos como los firewalls.
Muchas veces, se establecen políticas temporales o poco robustas confiando en que serán breves y están controladas, pero en muchas ocasiones, es precisamente un mal bastionado o una mala implementación de los elementos de seguridad de red, las que sirven como puerta de entrada a atacantes: Un firewall mal implementado es peor que no instalar un firewall

5. Seguridad física y lógica: La seguridad física es la primera línea de defensa contra accesos no autorizados, mientras que los controles de acceso y la vigilancia añaden capas de protección. La seguridad lógica, mediante la gestión de identidades y accesos, complementa estas medidas, asegurando que solo personal autorizado tenga acceso a sistemas y datos críticos. La combinación de enfoques físicos y lógicos crea una barrera robusta contra amenazas internas y externas.

6. Hardening de aplicaciones: La seguridad de las aplicaciones es esencial para prevenir vulnerabilidades. El hardening de aplicaciones implica configuración adecuada y gestión proactiva de parches. Esta medida procura evitar la explotación de posibles vulnerabilidades, garantizando que las aplicaciones utilizadas en sistemas de control sean resistentes y seguras. Además, es de vital importancia tener sistemas de control para las aplicaciones que se puedan o no instalar en nuestras estaciones de ingeniería u ordenadores del área de OT.

Afortunadamente muchos fabricantes han desarrollado soluciones de whitelisting y blacklisting de software adaptados a estos sistemas y con los que incluso podremos integrar las alertas en nuestro SIEM para actuar rápidamente contra un programa malicioso o no permitido en nuestra red.

Igualmente, muchas de estas soluciones nos ayudan a monitorizar y proteger nuestros sistemas contra uno de los vectores de entrada de malware más frecuente en OT: Los USB

7. Hardening de activos: La configuración segura de activos, como servidores, estaciones de trabajo, PLC, SCADA...etc es crucial para la protección contra amenazas. Una gestión eficaz de cuentas y contraseñas, junto con controles de acceso, refuerza la seguridad de estos activos. Estas medidas aseguran que los sistemas y datos críticos estén resguardados contra accesos no autorizados y manipulaciones indeseadas. Es importante disponer de unas guías de buenas prácticas tras la instalación de nuevo equipamiento. Muchas veces, los valores por defecto y los servicios implementados directamente por el fabricante, dejan puertas abiertas a atacantes externos.

8. Hardening de dispositivos embebidos: Los dispositivos embebidos, como PLC y sistemas SCADA, requieren medidas específicas para prevenir manipulaciones no autorizadas. El hardening de estos dispositivos implica la aplicación de actualizaciones de firmware, parches de seguridad y protección contra manipulaciones no autorizadas. Estas acciones son cruciales para mantener la integridad y seguridad de los procesos en entornos industriales. De igual manera, es importante controlar el software y la programación de estos dispositivos. Es importante contar con un sistema que nos alerte en caso de que la integridad de estos dispositivos se vea comprometida o alterada.

Aportar esta visión de 360 grados tanto estratégica como técnica da más valor a la consultoría experta en OT y ayuda a ver resultados desde el primer minuto del proyecto que, en entornos como el de OT donde lo importante es la disponibilidad, es precisamente nuestro objetivo.
La llegada de los dispositivos conectados e inteligentes al mundo industrial ha hecho que tengamos que adaptar, no solo las tecnologías, sino también la consultoría y la manera de entender la seguridad sobre un ámbito con una amplia obsolescencia, y donde los cambios no son triviales.

Alejandro Alonso Rodríguez
OT Cybersecurity Manager

Desinformación en año electoral

TENDENCIAS por Miguel Tuimil

La desinformación electoral es una creciente preocupación global que implica la difusión intencionada de información falsa o engañosa para influir en la opinión pública y afectar los resultados electorales. Este fenómeno se ha intensificado con el aumento de las plataformas de redes sociales y servicios de mensajería instantánea, donde noticias falsas y teorías de conspiración pueden propagarse rápidamente. Los actores malintencionados a menudo aprovechan las emociones y polarizaciones existentes para sembrar discordia y manipular la percepción de los votantes, siendo una gran amenaza para la democracia y la confianza de los ciudadanos en las instituciones.

Este **2024** los procesos electorales en Estados Unidos, India, Taiwan y otras 40 naciones, serán terreno fértil para la ingeniería social y las campañas de desinformación.

De acuerdo a la de Unesco, las desinformaciones electorales se pueden agrupar en 4 tipos generales:

1. Las acusaciones de fraude son frecuentemente las más difundidas durante las elecciones. Buscan demostrar un fraude organizado y coordinado por las autoridades nacionales, locales y/o electorales, como por ejemplo fotos de supuestas urnas con sellos rotos o capturas de actas de escrutinio con errores que pretenden confirmar un fraude. Típicamente, las irregularidades involuntarias no benefician sistemáticamente a ningún partido, mientras que las intencionales suelen sesgar los resultados a favor de alguna agrupación.

2. Las que se refieren a personas no habilitadas que supuestamente votan. Durante las elecciones circulan muchos contenidos que buscan atacar a las minorías, asegurando que personas migrantes votarán en países donde no está permitido o sin cumplir con las condiciones legales cuando el voto de extranjeros está habilitado. También circulan desinformaciones que afirman que personas fallecidas están incluidas en el censo electoral o que se utilizan documentos de identidad de personas fallecidas para votar. Sin embargo, en muchos casos, se trata de errores en el registro que son corregidos por las autoridades.

3. Las que refieren al proceso mismo de votación. Durante las elecciones, suelen circular contenidos falsos que buscan desorientar o generar miedo en los ciudadanos sobre el momento de la elección. Cada país tiene distintas normas que establecen cuándo un voto debe ser anulado o impugnado (es decir, no contabilizado como válido).

4. Declaraciones o propagandas falsas de los candidatos. Se emplea la edición y manipulación de fotos, así como imágenes sacadas de contexto. Para las declaraciones falsas, se utilizan marcos o logos de algún medio de comunicación con la imagen de un candidato y una supuesta frase. También circulan videos manipulados o sacados de contexto, y audios paródicos o falsamente atribuidos a los candidatos.

Combatir la desinformación en elecciones requiere esfuerzos coordinados de gobiernos, plataformas tecnológicas y ciudadanos. Las estrategias incluyen la verificación de hechos, la promoción de la alfabetización mediática, la transparencia en la publicidad política en línea y la colaboración internacional para abordar las campañas de desinformación transfronterizas. Es fundamental fortalecer la resiliencia de la sociedad ante la desinformación, promoviendo una ciudadanía informada y crítica que pueda discernir entre información veraz y engañosa en el contexto electoral.

Vulnerabilidades

Múltiples vulnerabilidades en Juniper Secure Analytics

Fecha: 28 de diciembre de 2023
CVEs: CVE-2023-40787 y 17 más

CVSS: 9.8
CRÍTICA

Descripción

Recientemente se han reportado dieciocho vulnerabilidades en Juniper Secure Analytics. De las dieciocho vulnerabilidades, dos son de severidad crítica, siete de severidad alta, otras siete de severidad media y dos de severidad baja.

A continuación, se indican las vulnerabilidades de severidad crítica:

- CVE-2023-40787: vulnerabilidad relacionada con la ejecución de consultas SQL en SpringBlade V3.6.0. En particular, ocurre cuando los parámetros enviados por el usuario no van entre comillas, esto provoca una inyección SQL.
- CVE-2023-46604: vulnerabilidad que podría permitir a un atacante remoto con acceso de red a un cliente o a un *broker* OpenWire basado en Java ejecutar comandos *shell* arbitrarios, manipulando tipos de clase serializados en el protocolo OpenWire para hacer que el cliente o el *broker* (respectivamente) instancien cualquier clase en el *classpath*.

Productos afectados

La vulnerabilidad afecta a la siguiente versión del producto:

- Juniper Secure Analytics, versiones hasta 7.5.0 UP7.

Solución

El fabricante recomienda tener sus productos actualizados siempre a la última versión, para así evitar riesgos de seguridad asociados a nuevas vulnerabilidades. En particular, se recomienda actualizar a la versión de Juniper Secure Analytics versión 7.5.0 UP7 IF03, en esta actualización se corrigen las vulnerabilidades identificadas.

Referencias

- www.incibe.es
- supportportal.juniper.net

Vulnerabilidad de inyección SQL en Ivanti EPM

Fecha: 4 de enero de 2024
CVEs: CVE-2023-39336

CVSS: 9.6
CRÍTICA

Descripción

Desde Ivanti se ha descubierto recientemente una vulnerabilidad crítica en su producto EPM (*Endpoint Manager*).

La vulnerabilidad descubierta, de tipo inyección SQL, permite a un atacante con acceso en la red interna ejecutar consultas SQL arbitrarias de forma que se obtiene el resultado de las consultas sin necesidad de autenticación. Esto puede permitir a un atacante controlar los dispositivos que ejecutan el agente de Ivanti EPM.

Además, cuando el servidor central está configurado para utilizar SQL Express, la vulnerabilidad detectada podría llevar a una ejecución remota de código (RCE) en el servidor central.

Productos afectados

La vulnerabilidad afecta a las siguientes versiones del producto Ivanti EPM:

- Ivanti EPM 2021.
- Ivanti EPM 2022 previas a *Service Update* 5.

Solución

El fabricante recomienda actualizar el producto Ivanti EPM a la versión 2022 SU5.

Referencias

- www.incibe.es
- forums.ivanti.com
- www.ivanti.com

Parches

CRÍTICA **Nuevos parches de seguridad para productos Microsoft**

Fecha: 10 de enero de 2024
CVE: CVE-2024-0057 y 47 más

Descripción

El pasado 10 de enero Microsoft lanzó una serie de actualizaciones para remediar múltiples vulnerabilidades de seguridad en sus sistemas operativos Windows y otros *softwares*. En total, se han publicado 48 vulnerabiliades, de las cuales 2 son críticas, 26 importantes y 20 de severidad media.

A continuación, se detallan las vulnerabilidades categorizadas como críticas:

- CVE-2024-0057: vulnerabilidad que afecta a NET, .NET Framework, y Visual Studio por la cual un atacante podría utilizar un certificado X.509 que no sea de confianza por medio de una API para insertar ese certificado y aprovechar el error que devuelva para insertar código malicioso.
- CVE-2024-20674: esta vulnerabilidad afecta a al protocolo de seguridad Kerberos de Windows, donde un atacante autenticado, al realizar una suplantación de red local, puede enviar un mensaje Kerberos malicioso a la víctima cliente y hacerse pasar por el servidor de autenticación Kerberos.

El resto de las vulnerabilidades pertenecen a varios tipos: elevación de privilegios, elusión de funciones de seguridad, ejecución remota de código, divulgación de información, denegación de servicio y suplantación de identidad.

Productos afectados

Dichas vulnerabilidades abarcan un gran número de productos Microsoft. Dichos productos pueden consultarse en: msrc.microsoft.com

Solución

Aplicar el parche de seguridad correspondiente en los productos afectados.

Referencias

- msrc.microsoft.com
- es-la.tenable.com

CRÍTICA **Parches críticos para GitLab Community y Enterprise Edition**

Fecha: 11 de enero de 2024
CVE: CVE-2023-7028

Descripción

GitLab recomienda encarecidamente parchear a sus últimas versiones sobre los productos GitLab Community Edition (CE) y Enterprise Edition (EE, ya que contienen importantes importantes correcciones de seguridad.

Los atacantes que exploten la vulnerabilidad CVE-2023-7028 pueden restablecer las contraseñas de las cuentas de usuarios de GitLab. No están extentos aquellos usuarios con doble factor de autenticación, por lo que también son vulnerables los usuarios con 2FA.

El fabricante ha confirmado que no se ha detectado ningún abuso de esta vulnerabilidad en plataformas administradas por GitLab.

Esta vulnerabilidad afecta a las instancias autoadministradas de GitLab que ejecutan las versiones previamente descritas.

Esta vulnerabilidad cuenta con su prueba de concepto (PoC) y un exploit publicado.

Productos afectados

Las diferentes versiones afectadas por dicha vulnerabilidad son los siguientes:

- 16.1 antes de 16.1.5
- 16.2 antes de 16.2.8
- 16.3 antes de 16.3.6
- 16.4 antes de 16.4.4
- 16.5 antes de 16.5.6
- 16.6 antes de 16.6.4
- 16.7 antes de 16.7.2

Solución

Gitlab recomienda a los administradores de instancias de GitLab que habiliten 2FA para todas las cunetas y actualicen a las versiones 16.7.2, 16.6.4, 16.5.6 de GitLab CE y EE.

Referencias

- about.gitlab.com
- nvd.nist.gov

Eventos

SANS Offensive Operations London 2024

El SANS Offensive Operations London 2024 se llevará a cabo en línea y de manera presencial del 5 al 10 de febrero. Existen múltiples cursos que ofrecen conocimientos prácticos sobre temas especializados, tales como análisis forense de Windows, fundamentos de seguridad en entornos de red, endpoint, nube y pruebas de penetración de aplicaciones web y hacking ético

Link

HackCon

La conferencia nacional noruega sobre ciberseguridad HackCon, tiene como objetivo cada año, dentro de los temas que son de gran relevancia, observar alrededor de 1200 a 1400 presentaciones e investigaciones para elegir a las absolutamente mejores ponencias para la HackCon. De todas las presentaciones/investigaciones, se selecciona aproximadamente un uno por ciento (12 cada año) para tener la oportunidad de hablar en la HackCon. Este año se celebrará desde el 12 al 14 de febrero en la ciudad de Oslo en Noruega.
Link

Zero Trust World

El Zero Trust World es un evento que se lleva a cabo en Orlando, Estados Unidos del 26 al 28 de febrero en el cual los asistentes adquirirán conocimientos y habilidades necesarias para avanzar hacia una postura de ciberseguridad de confianza cero. Habrá conferencias magistrales por la mañana, sesiones de trabajo por la tarde, laboratorios prácticos de hacking y una sala de exposiciones repleta de proveedores con soluciones para explorar.
Link

SecureWorld Financial Services

La conferencia virtual de SecureWorld Financial Services es un destacado evento que busca reunir a expertos de la industria financiera con el fin de brindar orientación sobre temas críticos de los servicios financieros y su impacto en la ciberseguridad. Durante 1 día, ofrece información clave sobre cómo las instituciones financieras pueden prepararse a los ciber ataques, la disrupción tecnológica y temas relacionados con la privacidad de datos en el sector financiero.
Link

Recursos

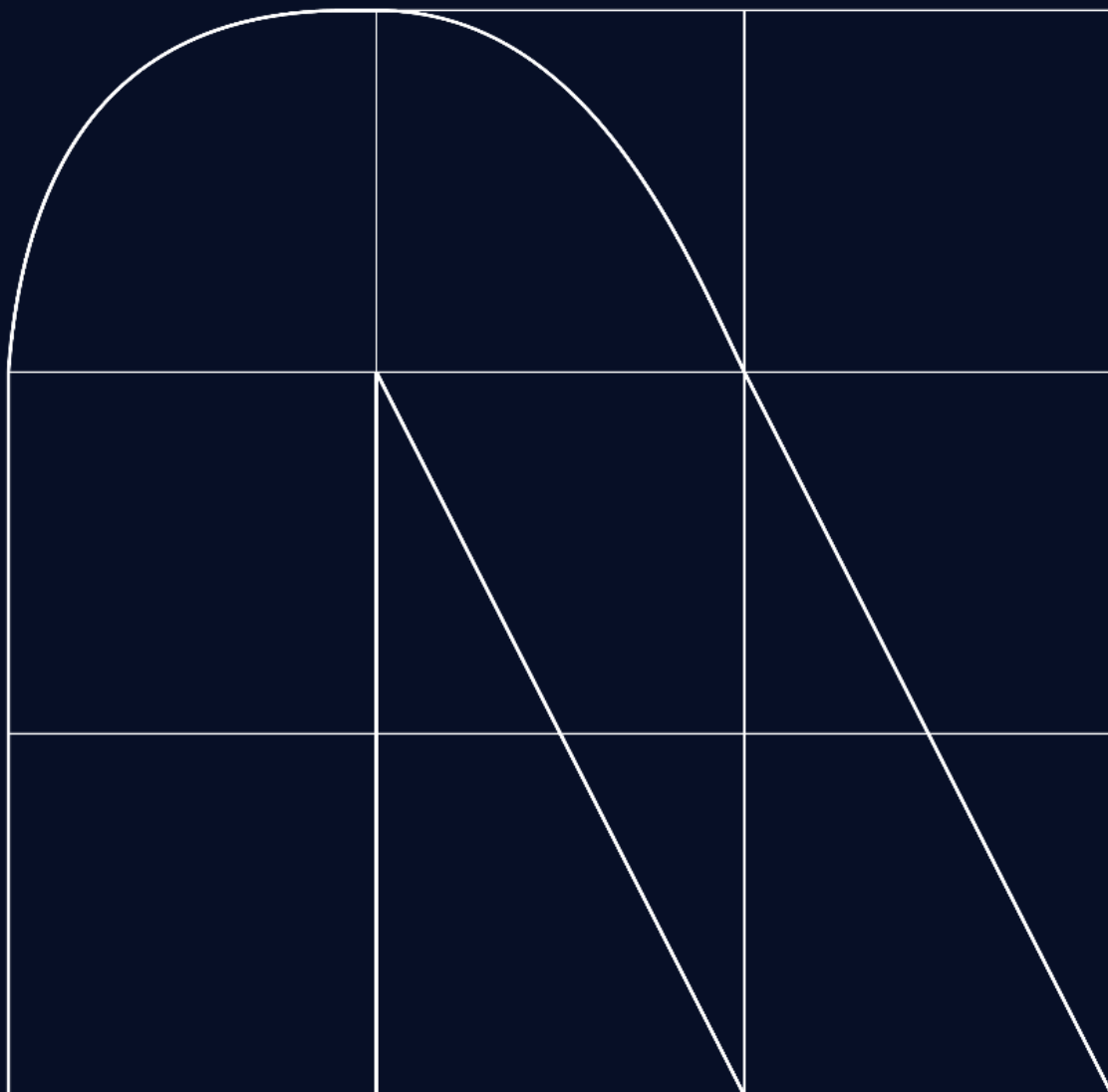
0dAI
0dAI es una plataforma SaaS (Software as a Service) orientada a la ciberseguridad impulsada por inteligencia artificial. Ofrece una gran variedad de servicios como: Desarrollo de Malware, ingeniería social, desarrollo de exploits y análisis de SOC entre una amplia gama.
Link

WebCheck
WebCheck es una herramienta de código abierto que permite realizar un análisis completo de aplicaciones web, recopilando información relevante como puede ser: cookies, registro DNS, geolocalización del servidor y cabeceras.
Link

CUPP
CUPP es una herramienta que permite al usuario desarrollar diccionarios personalizados con información relativa al atacado, como puede ser el nombre de la empresa, familiar o la fecha de tu nacimiento permitiendo así, un ataque más dinámico.
Link

CervantesSec
CervantesSec es una plataforma colaborativa de código abierto para pentesters que permite un ahorro de tiempo en la gestión de sus proyectos, permitiendo desarrollar plantillas customizadas, gestionar vulnerabilidades y asignar roles y permisos a los participantes del equipo.
Link

T-Pot
T-Pot es una plataforma de honeypot todo en uno, que permite una visualización clara de un mapa global con ataques en vivo y una gran variedad de herramientas que permitirán facilitar la compresión de los ataques que se está produciendo.
Link



Powered by the cybersecurity NTT DATA team

es.nttdata.com