NÚMERO 74 | ENERO 2023

NTT DATA
Trusted Global Innovator

Radar

El magazine de ciberseguridad

NUEVO AÑO, NUEVO FOCO EN CIBERSEGURIDAD

Hemos finalizado un año, el 2022, en el que hemos visto normalizarse la situación del teletrabajo, y nos hemos acercado a modelos híbridos más susceptibles de permanecer en el tiempo. Esto enfoca a los profesionales de TI a mantener las infraestructuras creadas tanto para el trabajo online, como para dar servicios a sus clientes sin personarse físicamente en ninguna parte, pero a la vez siendo conscientes de que los encuentros físicos van a darse de nuevo. Por esto, aunque cambiamos de año, la mente de los profesionales de ciberseguridad sigue enfocada en conseguir una mayor madurez en seguridad en focos muy particulares:

- **Seguridad en cloud:** el cloud ha sido y seguirá siendo este año foco de las áreas de seguridad; su objetivo es adoptar modelos de seguridad en el cloud y ponerse de manera solvente en este camino. Aunque el camino pueda ser largo, es necesario tener una estrategia bien marcada para esa adopción y avanzar con paso firme en ella.
- **Seguridad enfocada en el factor humano:** las organizaciones han dado ya claros signos de que entienden que la mayoría de ataques podrían haber sido evitados por un ser humano. Por tanto, los esfuerzos en promover comportamientos ciberseguridad, más allá de la protección conseguida por herramientas, va a ser clave este año.
- **Definición de un framework correcto de ciberseguridad:** ante la existencia de un gran número de frameworks de seguridad (ISO27001, NIST, FFIEC, IAC62443 entre otros) cada organización se va a enfocar en definir su framework, claramente basado en éstos, pero tomando lo mejor de cada uno orientado a la organización. Además, poco a poco se ve una evolución de la medición cualitativa de riesgos, a la medición cuantitativa, usando metodologías como FAIR.

Para los que a esto les parezca poco, en este año al que damos la bienvenida veremos cómo evolucionan ciertas tecnologías, que si siguen el crecimiento esperado requerirán de nuevas visiones para proteger a los clientes. En particular, el metaverso, tecnología que llegó con paso fuero y ahora está en plena búsqueda de casos de uso para que los negocios comiencen su adopción. En cuanto las compañías estén convencidas de que se puede hacer negocio, nuestra vida y la de nuestros clientes irrumpirá en esta nueva dimensión y con ello la necesidad de asegurar privacidad e identidad.

Y las telcos siguen avanzando con el 5G, tecnología que nos permitirá una hiperconexión, y con ella, nuevos modelos de interacción con muchas compañías, como comunicaciones, retail o banca. Pero igualmente, será necesario un framework de seguridad que nos brinde confianza.

Todos estos desafíos para los profesionales de ciberseguridad nos llegarán este año 2023. Y desde ya estamos encantados trabajando en su resolución.

Miguel Ángel Thomas

Top Executive Principal Head of Cybersecurity en NTT DATA Europa & Latam

CIBERCRÓNICA

Iniciamos esta cibercrónica recordando los ciber ataques más conocidos del año 2022, como fueron los perpetrados por el grupo de hackers LAPSUS$, quienes atacaron a las multinacionales NVIDIA, SAMSUNG y a la empresa argentina mercado libre; los diferentes ataques que sufrieron entidades de salud en Colombia, así como la guerra cibernética que se desato tras la invasión de Rusia a Ucrania, donde Mijail Fedorov anunció el lanzamiento de un ejército informático.

Estas noticias alertaron a los CISO's de muchas compañías del mundo, los cuales invirtieron tiempo y recursos importantes para proteger la información de sus compañías. Sin embargo, algunos de estos esfuerzos no fueron suficientes para contrarrestar a los ciber delincuentes que día a día generan nuevas maneras de actuar y que parecieran estar siempre un paso adelante.

"WhatsApp sufre una brecha de seguridad y se han expuesto los números de teléfono de 360 millones de personas en 108 países"

En cuanto a los sucedidos durante el último mes del año, un ciberataque, ha dejado 'noqueado' al Teatro de la Ópera de Nueva York, el ciberataque en plena estación prenavideña, considerada su temporada alta, impide al Metropolitan Opera House vender entradas y pagar a sus empleados.

Por otro lado, todos los sitios web del Vaticano dejaron de funcionar durante la tarde del miércoles tras un supuesto ciberataque. El director del servicio de prensa de la Santa Sede, Matteo Bruni, declaró a la AFP que hubo intentos de acceso anómalos y que las investigaciones técnicas estaban en curso.

De nuevo Uber sufrió una nueva violación de datos que filtró las direcciones de correo electrónico de los empleados, los informes corporativos y la información de activos de TI robada a un proveedor externo en un incidente de ciberseguridad.

Los datos filtrados incluyen numerosos archivos que afirman ser código fuente asociado con plataformas de administración de dispositivos móviles (MDM) utilizadas por Uber y Uber Eats y servicios de proveedores externos.

Otra brecha de seguridad que ha ocurrido antes de finalizar el año ha sido con la aplicación de WhatsApp se han expuesto los números de teléfono de cerca de 360 millones de personas de un total de 108 países. Los números de teléfono de 360 millones de usuarios de esa aplicación de mensajería instantánea estarían a la venta en la darknet.

En otro orden de cosas, un grupo proveniente de Irán llamado Nemesis Kitten ha declarado ser el autor de un malware personalizado del que no había información hasta ahora, denominado Drokbk, el cual utiliza GitHub como medio para filtrar datos de un ordenador infectado o para ejecutar comandos.

Iniciamos un nuevo año en el cual se presume que estará lleno de noticias de ciber seguridad no solo relacionadas con 0days de múltiples plataformas en la nube, sino también por la evolución de ataques relacionados con ransomware y sus diferentes mutaciones, así como los ataques a satélites que de acuerdo con lo sucedido con VIASAT en febrero de 2022, muestra las capacidades y evolución de los ataques persistentes.

Por otra parte, se presagia que las plataformas de correo serán un blanco clave en la obtención de información de grandes compañías en diferentes sectores, incluyendo entidades gubernamentales por las diferentes situaciones geopolíticas que se presentan a nivel mundial. La extracción de información y los ataques destructivos a infraestructuras industriales traerán mucho de qué hablar pues son objetivos claros para los principales grupos de hackers en el mundo.

CIBERSEGURIDAD EN TECNOLOGÍAS DE OPERACIÓN (OT) ENMARCADA DENTRO DE LA ARQUITECTURA EMPRESARIAL

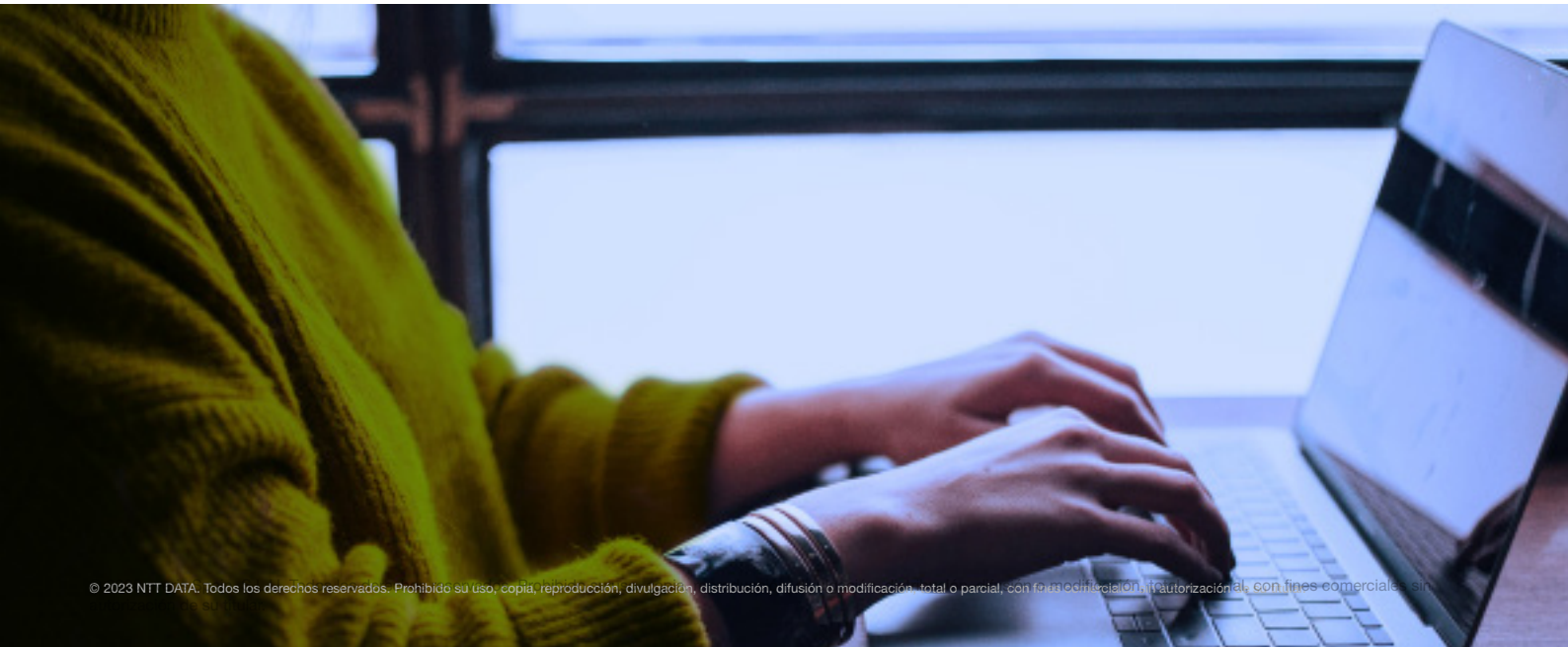
Por: NTT DATA Europe & Latam

Uno de los grandes desafíos que enfrentan los arquitectos de ciberseguridad es poder enmarcar en una arquitectura empresarial convergente las diferentes capas de los servicios que dan soporte a sus requerimientos propios y particulares del negocio y articular dos redes que conceptualmente tiene grandes diferencias pero que juntas deben armonizar para que la información fluya y sea utilizada de forma segura.

Uno de los grandes desafíos que enfrentan los arquitectos de ciberseguridad es poder enmarcar en una arquitectura empresarial convergente las diferentes capas de los servicios que dan soporte a sus requerimientos propios y particulares del negocio y articular dos redes que conceptualmente tiene grandes diferencias pero que juntas deben armonizar para que la información fluya y sea utilizada de forma segura.

Al diseñar una arquitectura de seguridad para un entorno en tecnologías de operación (OT, por sus siglas en ingles), se recomienda separar dicha red OT de la red corporativa. El tráfico de red y sus políticas en estas dos redes es diferente, pues servicios como el correo electrónico y el acceso remoto entre otros normalmente se permitirán en la red tecnologías de información (IT, por sus siglas en inglés) pero no se permitirán en las redes OT. Al inicio era común la coexistencia de tráfico de los dispositivos de OT sobre infraestructura IT, pero en el uso de la red corporativa los protocolos de comunicación de OT quedan expuestos a ciberataques o de embotellamiento. El uso de redes separadas permite una mayor flexibilidad para enfrentar los requisitos de seguridad y rendimiento en los dos entornos.

En la implementación de las nuevas tendencias como la transformación digital, el costo de la instalación de OT o el mantenimiento la infraestructura a menudo significa que se requiere una conexión entre OT y otras redes de TI propias o de terceros. Esta conexión representa un riesgo adicional para el que, en muchos casos, los proveedores sugieren soluciones que no tienen en cuenta la ciberseguridad y no consideran controles para estas conexiones, solo se concentran en el flujo de la información y el propietario de dicha infraestructura, al realizar implementaciones de esta manera queda expuesto y puede generar vulnerabilidades manifiestas (e.g conexión de segmentos de red IT y OT por medio de un PC o server con dos tarjetas de red) que explotadas por atacantes experimentados sacrifica la seguridad de los entornos IT y OT.



En este sentido, dos aspectos que cobran gran relevancia para diseñar arquitecturas seguras en OT, se describen en la figura 1:

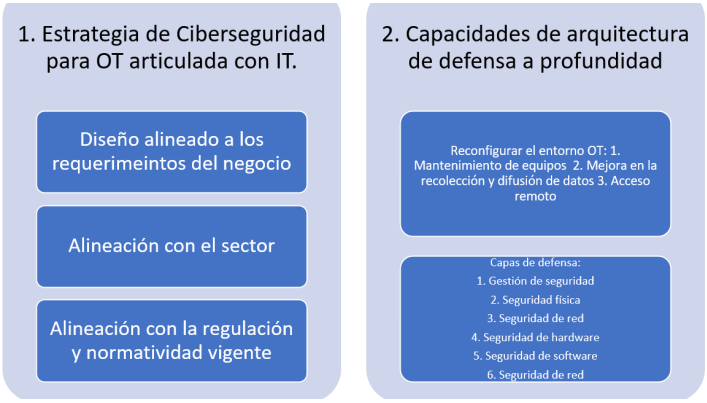


Figura 1: Aspectos relevantes para la construcción de arquitecturas seguras en OT.

La integración OT y TI es cada vez más necesaria, y evoluciona a medida en que las organizaciones se adaptan a los requerimientos actuales, y que se presentan en el entorno próximo, el sector el tipo de industria y los cambios a nivel global, en los aspectos relacionados con ciberseguridad.

El uso de los principios de una arquitectura de defensa a profundidad requiere la implementación de las capas de defensa mencionadas, lo cual implica un entorno de seguridad que involucre y este en línea con las personas, los procesos y la tecnología, dando como resultado el fortalecimiento del sistema de seguridad, en el que los atacantes tengan mayores dificultades para penetrar el entorno sin ser detectados.

Otro aspecto de gran relevancia para mejorar el diseño de una arquitectura de ciberseguridad en OT es la arquitectura de confianza cero o Zero Trust Architecture (ZTA, por sus siglas en inglés).

ZTA se enfoca en la protección de los recursos basado en las decisiones de autorización otorgadas a partir de una evaluación de las solicitudes, en lugar de una autorización implícita.

Tradicionalmente, a los usuarios de red se les otorga permisos a los diferentes recursos de la organización por ser considerados confiables; por tanto, los dispositivos de protección no mitigan los riesgos a estos usuarios, dejando desprotegido el entorno de los usuarios que hacen parte del mismo.

Además, con la creciente prevalencia de la computación distribuida, las comunicaciones inalámbricas y móviles, junto con los entornos de nube y de nube híbrida, los perímetros y límites de la red tradicional se están volviendo menos definidos.

Para estas situaciones, las organizaciones podrían considerar incorporar los principios de confianza cero en su arquitectura de seguridad.

Para migrar la arquitectura a un entorno de confianza cero se deben tener en cuenta aspectos como el nivel de madurez de la organización y la capacidad técnica junto con las inversiones en dinero y tiempo que esto implica. Así como, la eficiencia en la operación es decir aquello relacionado con la capacidad de respuesta y los requerimientos que supone implementar ZTA (Figura 2).

Figura 2: Desafíos de implementación de una ZTA

Otro aspecto objeto de estudio es el retraso que generaría en las comunicaciones la respuesta de múltiples dispositivos OT enviando credenciales para el funcionamiento correcto de ZTA, se deben tomar previsiones de redundancia según el proceso que sea monitoreado y controlado, un embotellamiento en la red OT es indeseable pues sobre ella también se gestionan funciones safety (seguridad de personas en OT).

Para finalizar el último aspecto es el registro de identidades que en muchos casos no son personales sino atribuibles a un conjunto de personas que compartes perfiles por turno productivo que afecta la filosofía de ZTA.

Varios de los principios enunciados anteriormente pueden ayudar en conjunto con otras tecnologías a aumentar la ciberseguridad en un entorno de OT en constante cambio.

¿QUÉ RIESGOS DE SEGURIDAD PUEDE ESCONDER EL METAVERSO?

Por: NTT DATA Europe & Latam

Se dice del metaverso que es la siguiente fase de internet, una nueva realidad virtual, la red social del mañana, entre otras. La realidad virtual, realidad aumentada, redes sociales, videojuegos son las bases que pueden formar parte del metaverso, pero solo cuando colaboran entre sí. El metaverso para una persona es ir por la calle observando anuncios en realidad aumentada, consultando sus redes sociales, y luego llegar a casa para jugar a un juego en realidad virtual, sin que en ningún momento note la transición de plataformas o se interrumpa su experiencia.

El metaverso está por llegar en maneras tanto predecibles como inesperadas. Al igual que todas las tendencias, habrá un cambio de hábitos de uso y consumo, un periodo de adaptabilidad para los usuarios de esta nueva tecnología. De igual forma, los riesgos de seguridad serán mucho más altos de lo que hayamos imaginado en un principio.

El número de compañías que están explorando las posibilidades del metaverso está creciendo y, por eso, las grandes firmas de ciberseguridad están estudiando el impacto que puede tener este mundo virtual. Metaverso, al igual que otras redes de TI, tiene riesgos de privacidad y seguridad de datos. Sin embargo, es necesario desarrollar una estrategia individual considerando las características de esta tecnología.

Por ejemplo, los datos de los usuarios de Metaverso residen en diferentes servidores en todo el mundo. Es necesario discutir cómo proteger a los usuarios ya sea cuando realicen una transacción o compartan información por medio de una conversación.

Suponen que principalmente la seguridad se verá comprometida en los dispositivos IoT como gafas inteligentes y cascos de realidad virtual, riesgos relacionados con el robo de identidades, el fraude en los pagos y la seguridad online. Aunque el metaverso potenciará las identidades virtuales, permitiendo a los individuos realizar muchas tareas que antes estaban limitadas al mundo físico tradicional, también ejercerá más presión sobre los procesos de autenticación.

Protección de datos

La privacidad de datos siempre ha sido un foco cuando se trata de la ciberseguridad, para este caso el metaverso se enfrenta al manejo de datos sensibles para los usuarios que estarán viviendo la experiencia, ahora bien, es necesario definir qué entidad estará a cargo de procesar y proteger dichos datos y más importante aún en el caso de un ataque efectivo ¿Quién se hará responsable de la filtración de esos datos?

El ataque dirigido a los usuarios no es el único foco por el cual el metaverso debe preocuparse, levantar una experiencia de comunicación para usuarios en tiempo real implica estar preparado para ataques concentrados en su propio dominio, como por ejemplo infiltrarse en secciones privadas irrumpiendo la password con un ataque de fuerza bruta, inundando el servicio bajo un ataque DDOS o la usurpación de identidades dentro de esta experiencia. Antes de maravillarse con todos los servicios, entretenimiento y ambientes que rompen con lo conocido y son posibles gracias a esta nueva tecnología, el metaverso debe asegurar a sus usuarios seguridad, ante todo.

Si bien las nuevas tecnologías como el metaverso siempre se presentarán como un nuevo entorno con límites más lejanos en comparación a los ya establecidos, es necesario que todo lo que se genere en este nuevo entorno tenga como base los pilares de la ciberseguridad, un ambiente sin límites de creación pero que presenta altos fallos en su seguridad.

Por lo tanto, debemos seguir velando por la privacidad y protección de datos de los usuarios, el metaverso no puede significar una excepción. Las tecnologías involucradas recopilarán muchos más datos, incluyendo aquellos que son altamente sensibles como los datos biométricos. Las empresas, deben asegurar que la privacidad esté integrada en el propio diseño del metaverso. Hay que velar por los correctos procesos que relacionarán los datos esenciales, por ende, entender quién será el responsable de recogerlos, procesarlos y sobre todo protegerlos.

TENDENCIAS

La computación cuántica como amenaza para los estándares de cifrado a llave pública actuales

Hoy en día, la mayoría de los protocolos de comunicación se basan en de tres funcionalidades criptográficas esenciales para realizar la transmisión de datos de forma segura y eficaz, estas son el cifrado a clave pública, las firmas digitales y el intercambio de llaves. Para lograr que estas funcionalidades cumplan con el objetivo de alterar la información para que no sea manipulada o robada, se han definido una serie de cifrados asimétricos como RSA, ECC y DSA que basan su cómputo en problemas matemáticos como factorización del producto de dos grandes números primos, el cifrado de curvas elípticas o el cálculo de un logaritmo discreto, los cuales son difíciles o intratables para los computadores convencionales.

No obstante, con la creciente investigación sobre las capacidades de los computadores cuánticos dichos problemas matemáticos pueden ser solucionados en cuestión de horas. La computación cuántica se está enfocando en usar aspectos de la mecánica cuántica, como el entrelazamiento o la superposición cuántica, para realizar cálculos a velocidades inconcebibles para los ordenadores clásicos. Por lo cual, cifrados como RSA, la curva elíptica y otras técnicas de cifrado podrían, en teoría, romperse con estos aumentos de velocidad en cuestión de horas, haciendo que los algoritmos de cifrado asimétricos más conocidos sean susceptibles de ataques cuánticos.

Frente a esta amenaza, el Instituto Nacional de Estándares y Tecnología (NIST) abrió, el 20 de diciembre de 2016, el espacio para la solicitud de candidaturas para Algoritmos Criptográficos Post-Cuánticos de Clave Pública y a julio 5 de 2022 se ha anunciado la selección de cuatro algoritmos candidatos que representan el primer acercamiento a estándares de criptografía post-cuántica y se basan en buscar problemas matemáticos que sean computacionalmente difíciles tanto para computadores convencionales como cuánticos. Para cifrado general se ha seleccionado CRYSTALS-Kyber. Por otro lado, para la funcionalidad de firmas digitales el NIST ha seleccionado CRYSTALS-Dilithium, FALCON y SPHINCS+.

La ventaja principal de estos nuevos algoritmos es que utilizan problemas matemáticos relacionados con retículos, estos resultan ser computacionalmente más difíciles de resolver tanto para computadores tradicionales como cuánticos. Esto se conocerá de ahora en adelante como criptografía basada en retículo y será el primer paso para la mitigación de ataques cuánticos a los cifrados de llave pública.

VULNERABILIDADES

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

Fortinet

CVE-2022-42475
Fecha: 12/12/2022

Descripción. Fortinet publicó el pasado lunes un aviso de seguridad donde informa sobre una vulnerabilidad 0-day categorizada como crítica que afecta a FortiOS SSL-VPN, a la que se le ha asignado el identificador CVE-2022-42475. Además, reconoce que es consciente de la explotación efectiva de la misma al menos en una instancia. Esta vulnerabilidad puede llevar a un tipo de desbordamiento de búfer llamado heap overflow o desbordamiento de montículo, pudiendo resultar en ejecución remota de código arbitrario (ACE) por parte de un atacante no autenticado utilizando solicitudes diseñadas específicamente para ello.

Enlace: https://olympecyberdefense.fr/vpn-ssl-fortigate/

https://www.fortiguard.com/psirt/FG-IR-22-398

Productos afectados. Esta vulnerabilidad afecta a los siguientes productos de Fortinet:

FortiOS:

- Las versiones desde la 7.2.0 hasta la 7.2.2.
- Las versiones desde la 7.0.0 hasta la 7.0.8.
- Las versiones desde la 6.4.0 hasta la 6.4.10.
- Las versiones desde la 6.2.0 hasta la 6.2.11.

FortiOS-6K7K:

- Las versiones desde la 7.0.0 hasta la 7.0.7.
- Las versiones desde la 6.4.0 hasta la 6.4.9.
- Las versiones desde la 6.2.0 hasta la 6.2.11.
- Las versiones desde la 6.0.0 hasta la 6.0.14.

Solución: Actualizar a la última versión del software. En los casos en los que no sea posible actualizar, se recomienda lo siguiente:

- Desactivar la función VPN-SSL si no resulta esencial.
- Supervisar los registros y verificar que no se hayan producido accesos no autorizados.
- Restringir las conexiones desde IP particulares mediante la configuración de las reglas de acceso.

Citrix

CVE-2022-27518
Fecha: 13/12/2022

Descripción. Se ha reportado una nueva vulnerabilidad 0-day de severidad crítica, cuya explotación podría permitir a un atacante remoto no autenticado la ejecución de código arbitrario en los dispositivos vulnerables. Esto se debe a que no se mantiene el control completo sobre los recursos durante su ciclo de vida. Se han reportado varios ataques que aprovechan esta vulnerabilidad, por lo que se recomienda la actualización de los dispositivos en la mayor brevedad posible.

Enlace: https://support.citrix.com/article/CTX474995/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202227518

https://www.citrix.com/blogs/2022/12/13/critical-security-update-now-available-for-citrix-adc-citrix-gateway/

https://media.defense.gov/2022/Dec/13/2003131586/-1/-1/0/CSA-APT5-CITRIXADC-V1.PDF

Productos afectados.

Citrix ADC y Citrix Gateway, versiones:

- anteriores a 12.1 y EOL;
- 13.0 anteriores a 13.0-58.32;
- 12.1 anteriores a 12.1-65.25.

Citrix ADC 12.1-FIPS, versiones anteriores a 12.1-55.291.

Citrix ADC 12.1-NDcPP, versiones anteriores a 12.1-55.291.

Solución: Aplicar los parches de seguridad correspondientes.

PARCHES

VMware

Fecha: 08-12-2022

Descripción. Se ha publicado una nueva actualización que soluciona un total de nueve vulnerabilidades en varios productos de VMware. En concreto, dos de las anteriores vulnerabilidades mencionadas son de severidad crítica y su explotación podría permitir la ejecución de comandos. Una de ellas permitiría inyectar comandos a través de la API REST y la otra aplicaría a un atacante con privilegios locales que podría ejecutar código en el host.

Enlace:
https://www.vmware.com/security/advisories/VMSA-2022-0030.html
https://www.vmware.com/security/advisories/VMSA-2022-0031.html
https://www.vmware.com/security/advisories/VMSA-2022-0032.html
https://www.vmware.com/security/advisories/VMSA-2022-0033.html

Productos afectados:
ESXi, Center Server, Cloud Foundation, vRealize Network Insight (vRNI), Workspace ONE Access, Identity Manager (vIDM), Workstation Pro / Player, y Fusion Pro / Fusion.

Solución: Instalar las actualizaciones correspondientes.

Siemens

Fecha: 14-12-2022

Descripción. Siemens ha publicado nuevas actualizaciones de seguridad que corrigen 139 vulnerabilidades en un gran número de sus productos. La explotación de las vulnerabilidades de severidad crítica podría permitir la realización de denegaciones de servicio, la omisión de autenticación, la ejecución de código arbitrario, el desbordamiento de enteros o la escritura fuera de límites

Enlace: https://support.industry.siemens.com/cs/start?lc=es-ES

Productos afectados:
Todas las versiones de:
- Simcenter STAR-CCM+;
- Polarion ALM;
- JT2Go;
- distintos modelos de SIPROTEC 5 listados en SSA-552874 y SSA-223771;
- PLM Help Server 4.2.

SICAM PAS/PQS, versiones:
- anteriores a 7.0;
- 7.0 y superiores hasta la anterior a 8.06.

Teamcenter Visualization, versiones listadas en SSA-700053 y SSA-360681.
Parasolid, versiones listadas en SSA-588101.
SIMATIC WinCC, distintas versiones y modelos listados en SSA-547714.
APOGEE PXC Series, versiones anteriores a: 3.5.5; 2.8.20.
TALON TC Series, versiones anteriores a 3.5.5.
SIMATIC, RUGGEDCOM, SCALANCE y SIPLUS, distintas versiones y modelos listados en SSA-413565, SSA-412672, SSA-382653, SSA-363821 y SSA-333517.
Calibre ICE, versiones 2022.4 y superiores.
Mcenter, versiones 5.2.1.0 y superiores.
Mendix:
- Email Connector, versiones anteriores a 2.0.0;
- Workflow Commons, versiones anteriores a 2.4.0.

Solución: Actualizar a las nuevas versiones de los productos afectados.

EVENTOS

International Conference on Cybersecurity, Cyberwar and Cyberthreats ICCCC

9 - 10 de enero 2023 |

La Conferencia Internacional sobre Ciberseguridad, Ciberguerra y Ciberamenazas tiene como objetivo reunir a los principales científicos académicos, investigadores y becarios de investigación para intercambiar y compartir sus experiencias y resultados de investigación sobre todos los aspectos de la Ciberseguridad, Ciberguerra y Ciberamenazas. También proporciona una plataforma interdisciplinaria de primer nivel para los investigadores, profesionales y educadores para presentar y discutir las innovaciones más recientes, las tendencias y las preocupaciones, así como los desafíos prácticos encontrados y las soluciones adoptadas en los campos de la ciberseguridad, la ciberguerra y las ciberamenazas.

Enlace: https://waset.org/cybersecurity-cyberwar-and-cyberthreats-conference-in-january-2023-in-bali

SANS Security East 2023

16 de enero de 2023 |

Durante SANS Security East podrás adquirir conocimientos de ciberseguridad del mundo real de la mano de los mejores expertos del sector, experimentar la formación interactiva con laboratorios prácticos, practicar habilidades durante los torneos NetWars y establecer contactos con tus compañeros en tiempo real.

Enlace: https://www.sans.org/cyber-security-training-events/security-east-2023/

Cybersecurity Standardisation Conference 2023

7 de enero de 2023 |

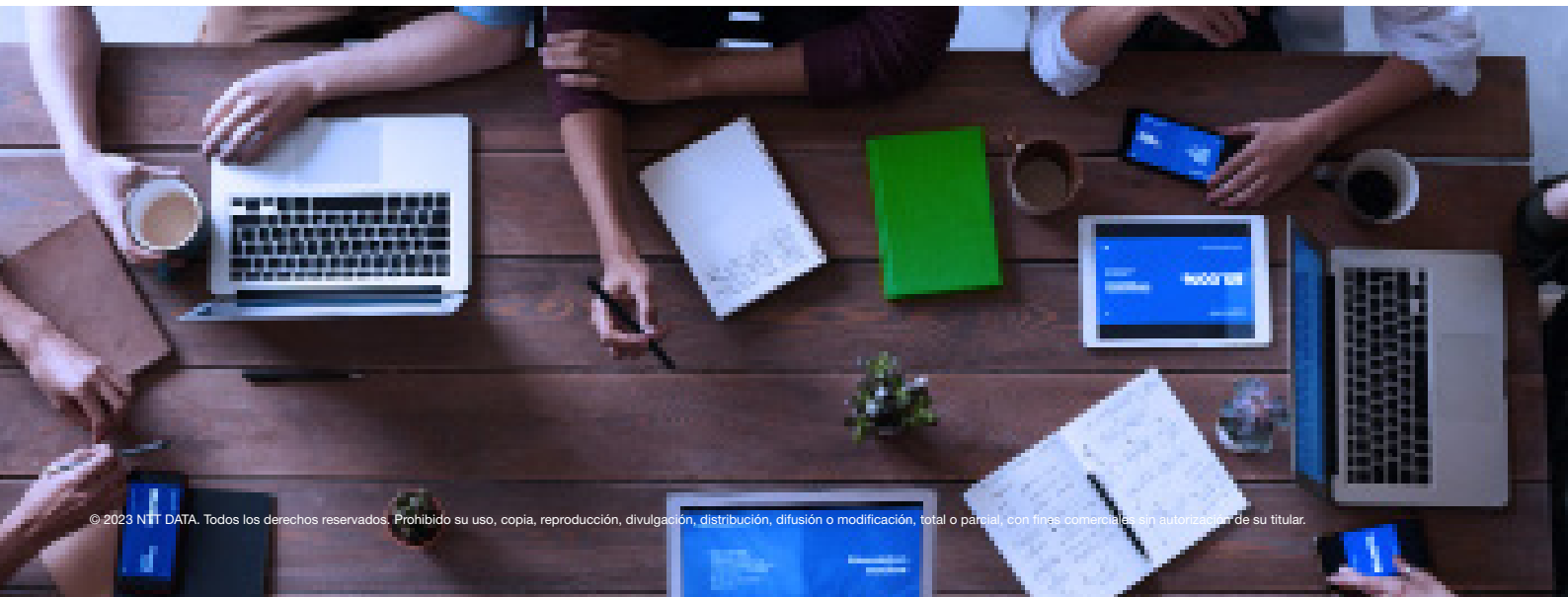
Por séptima vez, los organismos europeos de normalización CEN, CENELEC y ETSI, unen sus fuerzas con ENISA, la Agencia de la Unión Europea para la Ciberseguridad, para ofrecer una conferencia híbrida de normalización de la ciberseguridad sobre “La normalización europea en apoyo de la legislación de la UE sobre ciberseguridad”.

Enlace: https://www.enisa.europa.eu/events/cybersecurity_standardisation_2023

Día Internacional de la Protección de Datos

28 de enero de 2023 |

El día 28 de enero de 2023 se celebra a nivel mundial el día Internacional de la Protección de Datos, cuyo objetivo es concienciar y promover buenas prácticas relacionadas con el uso de la protección de datos, derechos y obligaciones de los usuarios; por ello, os recomendamos estar atentos a los webinars, charlas, cursos, talleres, etc. que se presenten en este día.



RECURSOS

Zero Trust as a Security Philosophy

Este documento analiza lo que significa la Confianza Cero para su organización, tanto desde el punto de vista de los proveedores como de las soluciones tecnológicas, y ofrece recomendaciones para desarrollar una estrategia y una arquitectura de apoyo que respalde a la organización y sus flujos de trabajo, alineando la TI con los objetivos y resultados empresariales.

Enlace: https://cloudsecurityalliance.org/artifacts/zero-trust-security-philosophy/

Servicio "Tu ayuda en Ciberseguridad" de INCIBE

Esta iniciativa también de INCIBE tiene como principal objetivo es sensibilizar y concienciar a los ciudadanos, menores de edad y empresas sobre el uso seguro y responsable de Internet y la tecnología, Además, aborda la importancia de tomar precauciones en su vida digital, ya que la actual situación, motivada por la pandemia, ha incrementado lo que se denomina 'superficie de riesgo', es decir, a mayor uso de la tecnología, mayor espacio para la aparición del ciberdelito y las ciberamenazas.

Enlace: https://www.incibe.es/sala-prensa/notas-prensa/el-servicio-tu-ayuda-ciberseguridad-incibe-protagonista-nueva-campana

¿Qué es el email spoofing y cómo se puede identificar?

El boletín de ciberseguridad de INCIBEe recoge información, a través de una historia real, sobre Fortnite, un videojuego online multijugador de combate armado 'todos contra todos', con distintos modos de juego (con y sin posibilidades de construcción, creativo y cooperativo), que está dirigido a usuarios mayores de 13 años.

Enlace: https://www.incibe.es/sala-prensa/notas-prensa/el-email-spoofing-y-se-puede-identificar

A Visual Summary of SANS Pen Test HackFest Summit 2022

Ashton Rodenhiser de Mind's Eye Creative creó grabaciones gráficas de las presentaciones de la Cumbre SANS Pen Test HackFest. Si te perdiste una charla o quieres ver la Cumbre a través de una lente visual puedes hacerlo en el siguiente link:

Enlace: https://www.sans.org/blog/a-visual-summary-of-sans-pen-test-hackfest-summit-2022/


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