BOLETÍN DE CIBERSEGURIDAD
NOVIEMBRE 2023

ÍNDICE

NOTICIAS INTERNACIONALES

MICROSOFT LANZA UNA NUEVA GENERACIÓN DE CIBERSEGURIDAD CON LA INICIATIVA DE FUTURO SEGURO

Microsoft lanza una nueva generación de ciberseguridad con la iniciativa de Futuro Seguro – Centro de Noticias. (2023, 3 noviembre). https://news.microsoft.com/es-es/2023/11/03/microsoft-lanza-una-nueva-generacion-de-ciberseguridad-con-la-iniciativa-de-futuro-seguro/

ESTA RECIENTE INICIATIVA CONVOCARÁ A TODAS LAS ÁREAS DE MICROSOFT CON EL OBJETIVO DE DESARROLLAR NUEVAS HERRAMIENTAS DE CIBERSEGURIDAD.

Se fundamenta en tres pilares: la ciberseguridad basada en inteligencia artificial, los avances en ingeniería de software y la defensa de una aplicación más extensa de los estándares internacionales. La empresa se compromete a crear un "ciberescudo" basado en IA diseñado para salvaguardar a clientes y países globalmente.

En los últimos meses, Microsoft ha llegado a la conclusión de que la velocidad, la magnitud y la creciente sofisticación de los ciberataques demandan una respuesta global renovada. Con este propósito, hoy lanzó la Iniciativa de Futuro Seguro (SFI), que se centrará en la próxima generación de protección cibernética. Los tres pilares principales se centran en la ciberseguridad basada en IA, avances en ingeniería de software y la defensa de una mayor aplicación de estándares internacionales para proteger a los civiles de amenazas cibernéticas.

Como se compartió en el Informe de Defensa Digital del mes pasado, implementar prácticas de ciberseguridad permite una protección efectiva contra la mayoría de los ataques cibernéticos. Sin embargo, dada la innovación agresiva y sofisticación de los atacantes, especialmente hacia infraestructuras críticas, Microsoft busca abordar estos desafíos mediante la SFI.

En el ámbito de la ciberseguridad basada en IA, Microsoft se compromete a desarrollar un "ciberescudo" que aproveche su red global de centros de datos y modelos avanzados de IA. Dentro de la SFI, el Centro de Inteligencia de Amenazas de Microsoft (MSTIC) y el Centro de Análisis de Amenazas de Microsoft (MTAC) están utilizando herramientas y técnicas avanzadas de IA. Microsoft Security Copilot, que combina modelos de lenguaje con competencias específicas de seguridad, aborda la escasez de profesionales especializados.

Además de la IA, la SFI impulsa nuevos avances en ingeniería de software, transformando el ciclo de vida de desarrollo de seguridad en un "SDL dinámico". Esto significa integrar continuamente la ciberseguridad contra patrones de amenazas emergentes durante todas las fases del desarrollo. Microsoft también mejorará las configuraciones predeterminadas de autenticación multifactor en el próximo año.

Finalmente, la SFI aborda la aplicación más efectiva de las normas internacionales en ciberseguridad. Microsoft busca fortalecer y elevar las normas necesarias para proteger a civiles en el ciberespacio, renovando esfuerzos para unir a gobiernos, sector privado y sociedad civil en la implementación de estándares internacionales de ciberseguridad.

RANSOMWARE CACTUS EXPLOTA VULNERABILIDADES EN QLIK SENSE EN ATAQUES DIRIGIDOS.

La campaña de ransomware CACTUS ha sido observada explotando recientemente vulnerabilidades de seguridad reveladas en una plataforma de análisis en la nube e inteligencia empresarial llamada Qlik Sense para obtener una posición en entornos específicos.

"ESTA CAMPAÑA MARCA LA PRIMERA INSTANCIA DOCUMENTADA DONDE ACTORES DE AMENAZAS QUE DESPLIEGAN EL RANSOMWARE CACTUS HAN EXPLOTADO VULNERABILIDADES EN QLIK SENSE PARA ACCEDER INICIALMENTE"

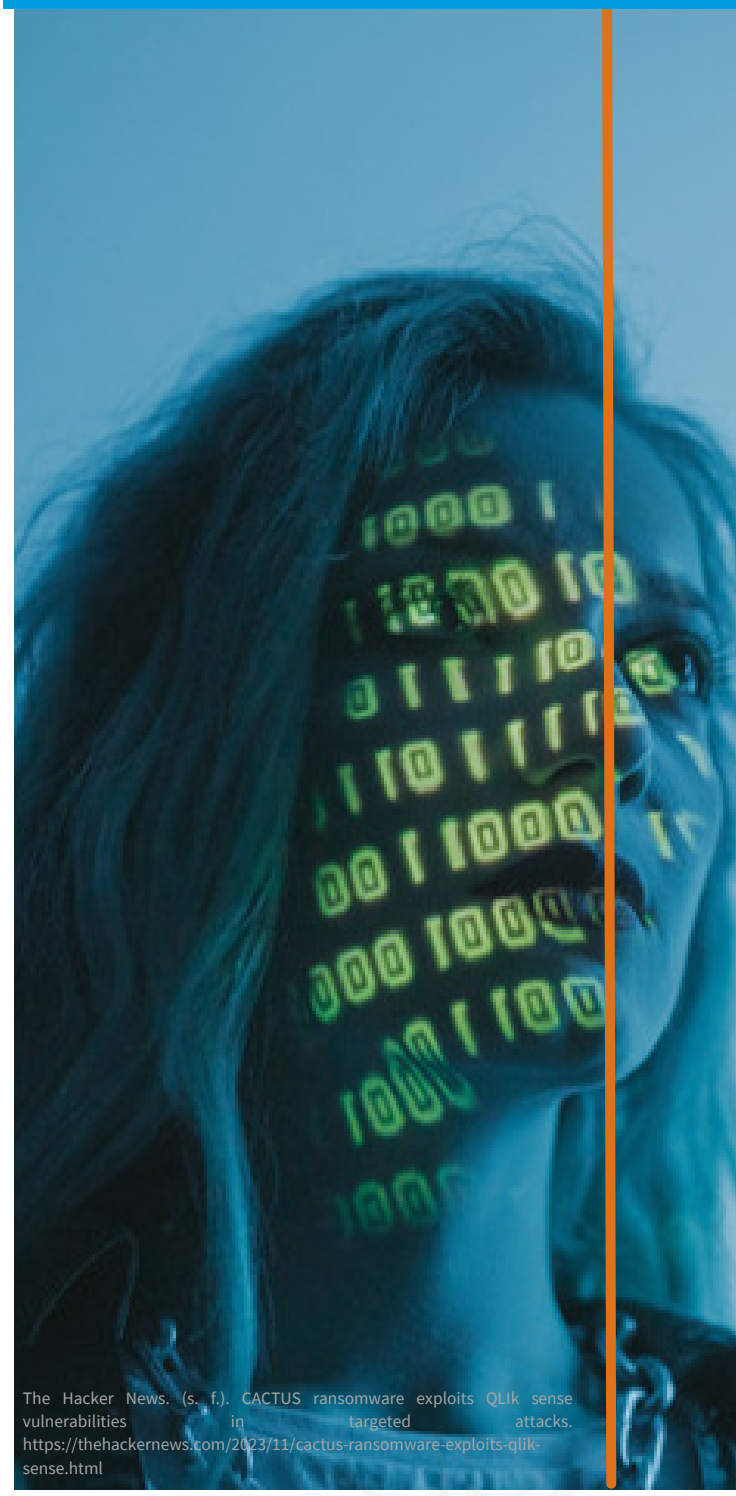
La empresa de ciberseguridad, que afirmó estar respondiendo a "varias instancias" de explotación del software, señaló que los ataques probablemente estén aprovechando tres fallas que se han revelado en los últimos tres meses:

- CVE-2023-41265 (puntuación CVSS: 9.9): una vulnerabilidad de túneles de solicitud HTTP que permite a un atacante remoto elevar sus privilegios y enviar solicitudes que son ejecutadas por el servidor backend que aloja la aplicación del repositorio.
- CVE-2023-41266 (puntuación CVSS: 6.5): una vulnerabilidad de travesía de ruta que permite a un atacante remoto no autenticado transmitir solicitudes HTTP a puntos finales no autorizados.
- CVE-2023-48365 (puntuación CVSS: 9.9): una vulnerabilidad de ejecución de código remoto no autenticado que surge debido a una validación incorrecta de encabezados HTTP, permitiendo a un atacante remoto elevar sus privilegios mediante el túnel de solicitudes HTTP.

Cabe destacar que CVE-2023-48365 es el resultado de un parche incompleto para CVE-2023-41265, que junto con CVE-2023-41266 fue revelado por Praetorian a finales de agosto de 2023. Se lanzó una corrección para CVE-2023-48365 el 20 de septiembre de 2023.

En los ataques observados por Arctic Wolf, la explotación exitosa de las fallas es seguida por el abuso del servicio Qlik Sense Scheduler para generar procesos diseñados para descargar herramientas adicionales con el objetivo de establecer persistencia y configurar control remoto.

Esto incluye ManageEngine Unified Endpoint Management and Security (UEMS), AnyDesk y Plink. También se ha observado a los actores de amenazas desinstalar el software Sophos, cambiar la contraseña de la cuenta de administrador y crear un túnel RDP a través de Plink.



The Hacker News. (s. f.). CACTUS ransomware exploits QLIk sense vulnerabilities in targeted attacks. https://thehackernews.com/2023/11/cactus-ransomware-exploits-qlik-sense.html

RANSOMWARE CACTUS EXPLOTA VULNERABILIDADES EN QLIK SENSE EN ATAQUES DIRIGIDOS.

Las cadenas de ataques culminan en el despliegue del ransomware CACTUS, con los atacantes también utilizando rclone para la extracción de datos.
El paisaje en constante evolución del ransomware.

La divulgación se produce en un momento en que el panorama de amenazas de ransomware se ha vuelto más sofisticado, y la economía subterránea ha evolucionado para facilitar ataques a gran escala a través de una red de intermediarios de acceso inicial y propietarios de botnets que revenden el acceso a sistemas de víctimas a varios actores afiliados.

Según datos recopilados por la firma de ciberseguridad industrial Dragos, el número de ataques de ransomware que afectan a organizaciones industriales disminuyó de 253 en el segundo trimestre de 2023 a 231 en el tercer trimestre. En contraste, se informaron 318 ataques de ransomware en todos los sectores solo en el mes de octubre de 2023.

A pesar de los esfuerzos continuos de los gobiernos de todo el mundo para abordar el ransomware, el modelo de negocio de ransomware como servicio (RaaS) ha seguido siendo un camino perdurable y lucrativo para extorsionar dinero de los objetivos.

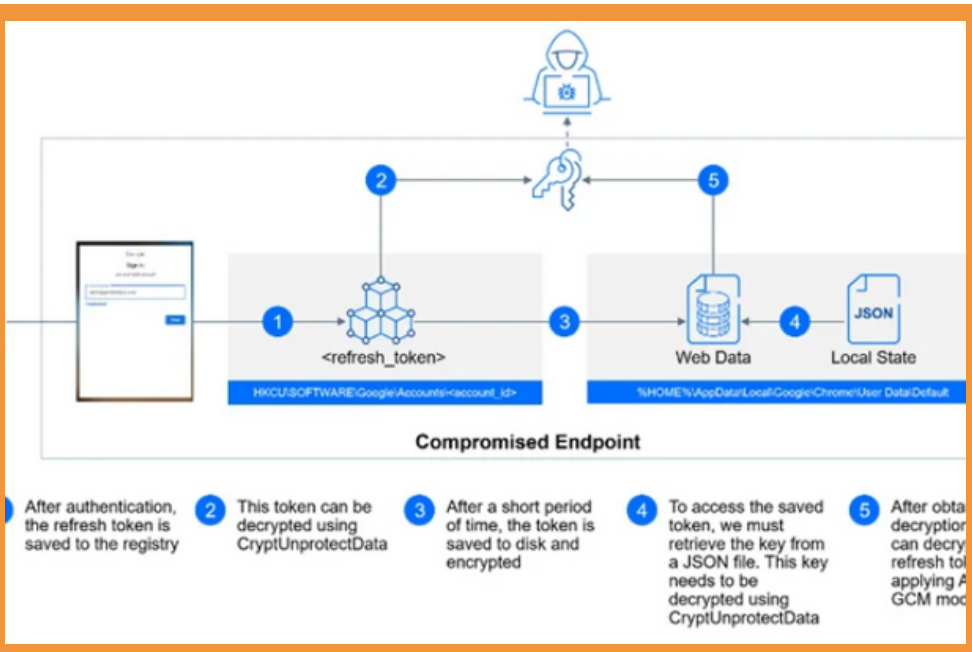
Se estima que Black Basta, un prolífico grupo de ransomware que apareció en abril de 2022, ha obtenido ganancias ilegales de al menos $107 millones en pagos de rescate en Bitcoin de más de 90 víctimas, según una nueva investigación conjunta publicada por Elliptic y Corvus Insurance.
La mayoría de estos ingresos fueron blanqueados a través de Garantex, un intercambio de criptomonedas ruso sancionado por el gobierno de EE. UU. en abril de 2022 por facilitar transacciones con el mercado negro Hydra.

Además, el análisis descubrió evidencia que vincula a Black Basta con el ahora desaparecido grupo de ciberdelincuentes rusos Conti, que se retiró alrededor del mismo tiempo que surgió el primero, así como con QakBot, que se utilizó para implementar el ransomware.

"Alrededor del 10% del monto del rescate se destinó a Qakbot, en casos en los que estuvieron involucrados en proporcionar acceso a la víctima", señaló Elliptic, agregando que "rastreó Bitcoin por valor de varios millones de dólares desde billeteras vinculadas a Conti hasta aquellas asociadas con el operador de Black Basta".

LOS HACKERS PODRÍAN APROVECHAR GOOGLE WORKSPACE Y LA PLATAFORMA EN LA NUBE PARA LLEVAR A CABO ATAQUES DE RANSOMWARE.

Se ha demostrado un conjunto de métodos de ataque novedosos contra Google Workspace y la Plataforma en la Nube de Google que podrían ser potencialmente aprovechados por actores de amenazas para llevar a cabo ataques de ransomware, exfiltración de datos y recuperación de contraseñas.



The Hacker News. (s.f.-b). Hackers could exploit Google workspace and cloud platform for ransomware attacks. https://thehackernews.com/2023/11/hackers-could-exploit-google-workspace.html

Se ha demostrado un conjunto de métodos de ataque novedosos contra Google Workspace y la Plataforma en la Nube de Google que podrían ser potencialmente aprovechados por actores de amenazas para llevar a cabo ataques de ransomware, exfiltración de datos y recuperación de contraseñas.

"Partiendo de una única máquina comprometida, los actores de amenazas podrían avanzar de varias maneras: podrían pasar a otras máquinas clonadas con GCPW instalado, obtener acceso a la plataforma en la nube con permisos personalizados o descifrar contraseñas almacenadas localmente para continuar su ataque más allá del ecosistema de Google", dijo Martin Zugec, director de soluciones técnicas en Bitdefender, en un nuevo informe.

Un requisito previo para estos ataques es que el actor malicioso ya haya obtenido acceso a una máquina local a través de otros medios, lo que llevó a Google a marcar el error como no apto para corrección "ya que está fuera de nuestro modelo de amenaza y el comportamiento está alineado con las prácticas de Chrome de almacenar datos locales".

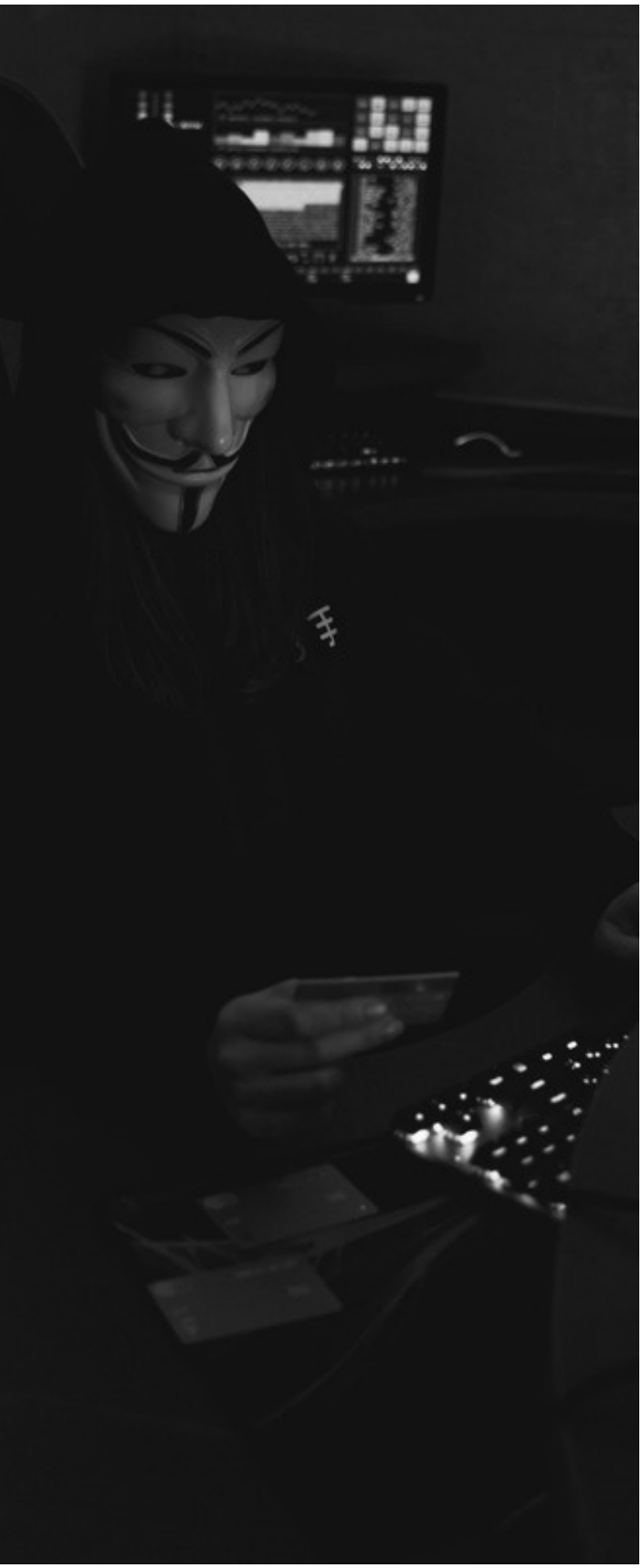
Sin embargo, la firma rumana de ciberseguridad ha advertido que los actores de amenazas pueden aprovechar tales lagunas para ampliar una única vulnerabilidad de un punto final a una violación de toda la red.

En resumen, los ataques se basan en el uso del Proveedor de Credenciales de Google para Windows (GCPW) por parte de una organización, que ofrece capacidades tanto de gestión de dispositivos móviles (MDM) como de inicio de sesión único (SSO).

Esto permite a los administradores gestionar y controlar de forma remota los dispositivos Windows dentro de sus entornos de Google Workspace, así como permite a los usuarios acceder a sus dispositivos Windows utilizando las mismas credenciales que se utilizan para iniciar sesión en sus cuentas de Google.

GCPW está diseñado para utilizar una cuenta de servicio privilegiada local llamada Administración de Cuentas e ID de Google (GAIA) para facilitar el proceso de manera transparente en segundo plano conectándose a las API de Google para verificar las credenciales del usuario durante el paso de inicio de sesión y almacenar un token de actualización para evitar la necesidad de una nueva autenticación.

LOS HACKERS PODRÍAN APROVECHAR GOOGLE WORKSPACE Y LA PLATAFORMA EN LA NUBE PARA LLEVAR A CABO ATAQUES DE RANSOMWARE.



Con esta configuración, un atacante con acceso a una máquina comprometida puede extraer los tokens de actualización de OAuth de una cuenta, ya sea del registro de Windows o del directorio de perfil de Chrome del usuario, y eludir las protecciones de autenticación multifactor (MFA).

El token de actualización se utiliza posteriormente para construir una solicitud POST HTTP al punto final "https://www.googleapis[.]com/oauth2/v4/token" para obtener un token de acceso, que, a su vez, puede ser abusado para recuperar, manipular o eliminar datos sensibles asociados con la cuenta de Google.

Un segundo exploit se refiere a lo que se llama el movimiento lateral de la imagen dorada, que se centra en implementaciones de máquinas virtuales (VM) y aprovecha el hecho de que crear una máquina clonando otra máquina con GCPW preinstalado hace que la contraseña asociada con la cuenta GAIA también se clone.

"Si conoces la contraseña de una cuenta local, y las cuentas locales en todas las máquinas comparten la misma contraseña, entonces conoces las contraseñas de todas las máquinas", explicó Zugec.

"Este desafío de contraseña compartida es similar a tener la misma contraseña de administrador local en todas las máquinas, algo que ha sido abordado por la Solución de Contraseña de Administrador Local (LAPS) de Microsoft."

El tercer ataque implica el acceso a credenciales en texto plano aprovechando el token de acceso adquirido mediante la técnica mencionada anteriormente para enviar una solicitud GET HTTP a un punto final de API no documentado y obtener la clave privada RSA necesaria para descifrar el campo de contraseña.

"Tener acceso a credenciales en texto plano, como nombres de usuario y contraseñas, representa una amenaza más grave", dijo Zugec. "Esto se debe a que permite a los atacantes suplantar directamente a usuarios legítimos y obtener acceso ilimitado a sus cuentas, lo que podría llevar a la toma completa de la cuenta".

SE PUEDE APROVECHAR LA "AUTENTICACIÓN FORZADA" PARA ROBAR TOKENS NTLM DE WINDOWS.

The Hacker News. (s. f.-b). Hackers can exploit «Forced authentication» to steal Windows NTLM tokens. https://thehackernews.com/2023/11/hackers-can-exploit-forced.html

INVESTIGADORES EN CIBERSEGURIDAD HAN DESCUBIERTO UN CASO DE "AUTENTICACIÓN FORZADA" QUE PODRÍA SER EXPLOTADO PARA FILTRAR LOS TOKENS NT LAN MANAGER (NTLM) DE UN USUARIO DE WINDOWS AL ENGAÑAR A LA VÍCTIMA PARA QUE ABRA UN ARCHIVO DE MICROSOFT ACCESS ESPECIALMENTE DISEÑADO.

El ataque aprovecha una característica legítima en la solución del sistema de gestión de bases de datos que permite a los usuarios vincularse a fuentes de datos externas, como una tabla remota de SQL Server.

"Esta característica puede ser abusada por los atacantes para filtrar automáticamente los tokens NTLM del usuario de Windows a cualquier servidor controlado por el atacante, a través de cualquier puerto TCP, como el puerto 80", dijo el investigador de seguridad de Check Point, Haifei Li. "El ataque puede lanzarse siempre que la víctima abra un archivo .accdb o .mdb. De hecho, cualquier tipo de archivo de Office más común (como un .rtf) puede funcionar igualmente bien".

NTLM, un protocolo de autenticación introducido por Microsoft en 1993, es un protocolo de respuesta a desafíos que se utiliza para autenticar a los usuarios durante el inicio de sesión. Con el tiempo, se ha descubierto que es vulnerable a ataques de fuerza bruta, pase de hash y de relay.

En resumen, el último ataque abusa de la función de tabla vinculada en Access para filtrar los hashes NTLM a un servidor controlado por un actor al incrustar un archivo .accdb con un vínculo de base de datos de SQL Server remota dentro de un documento de MS Word utilizando un mecanismo llamado Object Linking and Embedding (OLE).

Un atacante puede configurar un servidor que controla, escuchando en el puerto 80, y poner su dirección IP en el campo 'alias de servidor' mencionado anteriormente", explicó Li. "Luego pueden enviar el archivo de base de datos, incluida la tabla vinculada, a la víctima".

Si la víctima abre el archivo y hace clic en la tabla vinculada, el cliente de la víctima se pone en contacto con el servidor controlado por el atacante para la autenticación, lo que permite a este último llevar a cabo un ataque de relay lanzando un proceso de autenticación con un servidor NTLM objetivo en la misma organización.
El servidor malintencionado luego recibe el desafío, lo transmite a la víctima como parte del proceso de autenticación y obtiene una respuesta válida, que se transmite finalmente al servidor NTLM.

Aunque Microsoft ha lanzado mitigaciones para el problema en la versión de Office/Access (Canal Actual, versión 2306, compilación 16529.20182) después de una divulgación responsable en enero de 2023, 0patch ha lanzado correcciones no oficiales para Office 2010, Office 2013, Office 2016, Office 2019 y Office 365.
Este desarrollo también se produce cuando Microsoft anunció planes para discontinuar NTLM en Windows 11 a favor de Kerberos para mejorar la seguridad.

NOTICIAS NACIONALES

BANXICO EMITE NUEVAS REGLAS DE CIBERSEGURIDAD PARA SPEI Y SPID

EL SISTEMA DE PAGOS INTERBANCARIOS EN DÓLARES (SPID), EL BANCO DE MÉXICO HA INTRODUCIDO NUEVAS REGLAS QUE FUERON PREVIAMENTE SOMETIDAS A CONSULTA PARA QUE LOS PARTICIPANTES DE AMBOS SISTEMAS PUDIERAN EXPRESAR SUS OPINIONES AL RESPECTO.

Recientemente, en el Diario Oficial de la Federación (DOF), Banxico publicó tres circulares relacionadas con el fortalecimiento de las pautas de ciberseguridad, tanto para SPEI como para SPID. Entre las disposiciones destacadas emitidas por el banco central se encuentra el requisito, según la Circular 11/2023, para que las entidades participantes en el SPID cuenten con un Oficial de Seguridad de la Información (CISO).

Gutiérrez, F. (2023, 23 noviembre). Banxico emite nuevas reglas de ciberseguridad para SPEI y SPID. El Economista. https://www.eleconomista.com.mx/sectorfinanciero/Banxico-emite-nuevas-reglas-de-ciberseguridad-para-SPEI-y-SPID-20231123-0011.html

Este CISO tendrá la responsabilidad de llevar a cabo verificaciones regulares para asegurar el cumplimiento de sus funciones y realizar revisiones periódicas de los requisitos de seguridad en la infraestructura tecnológica, incluyendo terceros que puedan afectar la operación.

Las entidades participantes deberán proporcionar al CISO un listado actualizado de personas con acceso a información crítica. La fecha de entrada en vigor de esta circular es el 4 de abril de 2024.

Adicionalmente, mediante la Circular 12/2023, el Banco de México busca fortalecer la seguridad, clarificar elementos técnicos y agregar medidas para mejorar la ciberresiliencia de los participantes en el SPEI. Se introducen definiciones clave, como "Ciberresiliencia", que se refiere a la capacidad del participante para prevenir, adaptarse, responder o recuperar su operación en el SPEI ante ciberataques. Esta circular incluye controles adicionales, intensificación de medidas de control de acceso y gestión de vulnerabilidades en la tecnología de la información (IT).

En cuanto a la Circular 13/2023, esta modifica algunas reglas del SPID con el objetivo de garantizar la seguridad y el buen funcionamiento de los sistemas de pagos interbancarios en dólares. Se añaden definiciones, como la de "Aplicativo SPID", y se establece la obligatoriedad de implementar políticas para el desarrollo seguro del Aplicativo SPID, incluyendo pruebas de penetración y controles de acceso. Algunas disposiciones de esta circular entrarán en vigor a partir del 19 de diciembre próximo.

Es importante destacar que tanto el SPEI como el SPID son sistemas operados por Banxico para facilitar transferencias de fondos electrónicos entre los participantes, cada uno con sus propias características y funciones específicas.

LO QUE SE SABE DEL CIBERATAQUE AL AEROPUERTO INTERNACIONAL DE QUERÉTARO

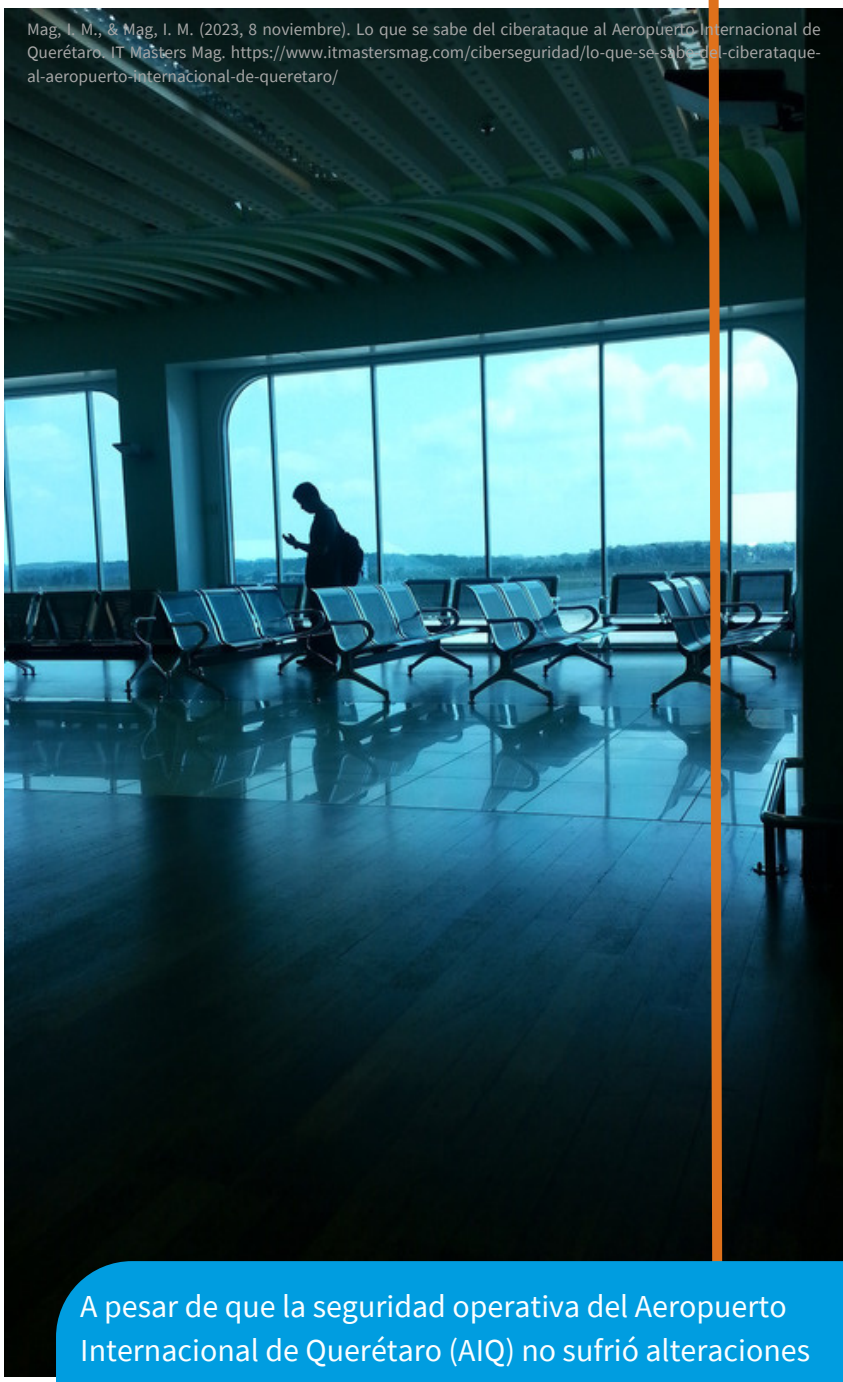
El aeródromo, que opera en colaboración entre el Gobierno estatal y Aeropuertos y Servicios Auxiliares (ASA), confirmó el ciberataque el 31 de octubre a través de su cuenta oficial en X.

En su declaración, el AIQ aseguró: "Informamos que tuvimos un incidente de ciberataque y estamos trabajando con expertos para abordar esta situación. Los sistemas AIQ están funcionando con normalidad. La seguridad de nuestros pasajeros y operaciones sigue siendo nuestra principal prioridad".

La confirmación se produjo después de que el grupo de ciberdelincuentes LockBit incluyera al AIQ en su foro en la dark web, según informes de usuarios en redes, incluida la plataforma Venarix.

LockBit, catalogado como el grupo de ransomware más activo en el primer trimestre de 2023 con más de 1,500 registros de anuncios de víctimas en la plataforma SOCRadar, estableció el próximo 27 de noviembre como fecha límite para la publicación de todos los datos obtenidos. Ante esto, el AIQ respondió indicando que toda la información en su posesión, por su naturaleza, es de dominio público.

El incidente de ciberseguridad, según el AIQ, fue resultado de "un acto involuntario de personal de la organización al interactuar con un archivo con software malicioso". Aunque no ha proporcionado actualizaciones adicionales, el aeropuerto afirmó que el equipo de seguridad cibernética y expertos han actuado diligentemente, aplicando medidas de contención y aislamiento.



Mag, I. M., & Mag, I. M. (2023, 8 noviembre). Lo que se sabe del ciberataque al Aeropuerto Internacional de Querétaro. IT Masters Mag. https://www.itmastersmag.com/ciberseguridad/lo-que-se-sabe-del-ciberataque-al-aeropuerto-internacional-de-queretaro/

A pesar de que la seguridad operativa del Aeropuerto Internacional de Querétaro (AIQ) no sufrió alteraciones debido a un ciberataque ocurrido el 30 de octubre pasado, persiste la amenaza de una posible filtración de datos.

Dada la naturaleza frecuente de ciberataques en la industria de la aviación, con casos recientes que involucran a Air Canada y Air Europa, así como incidentes de denegación de servicio distribuido (DDoS) en los sitios web de aeropuertos estadounidenses, el AIQ se encuentra en proceso de investigación en colaboración con las autoridades pertinentes para determinar la naturaleza, alcance y responsabilidades del incidente.

CIBERATAQUES CONTRA SECTOR FINANCIERO SE INCREMENTAN EN MÉXICO: INDUSTRIA

La frecuencia de ataques cibernéticos dirigidos a instituciones del sistema financiero mexicano está en aumento, enfocándose cada vez más en los clientes de bancos y otras entidades financieras, según revelan entrevistas con profesionales de la industria consultados por El Economista.

Hasta agosto de 2023, cuatro instituciones financieras en México reportaron incidentes cibernéticos, según datos del Banco de México (Banxico), con pérdidas económicas que alcanzan los 67.61 millones de pesos. De estos incidentes, tres afectaron a instituciones bancarias y uno a la Sociedad Cooperativa de Ahorro y Préstamo (Socap) Caja Popular Mexicana.

En comparación, durante 2022, solo un banco, una casa de bolsa y una Sociedad de Información Crediticia informaron haber sufrido un incidente cibernético que causó pérdidas por 25.5 millones de pesos.

Luis Rodríguez, vicepresidente senior de Tecnologías, Operaciones y Digital en Scotiabank México, señala que los ciberataques en México y América Latina, particularmente en México, han aumentado en paralelo con las medidas implementadas por las instituciones financieras, especialmente en perjuicio de sus clientes. Rodríguez destaca que los ataques de phishing y vishing, que emplean tecnología y técnicas de ingeniería social, son las amenazas más perjudiciales para los clientes, ya que buscan engañarlos para robar datos y credenciales.

Rodríguez enfatiza que Scotiabank, al igual que la mayoría de las instituciones financieras mexicanas, no solicita información confidencial a sus clientes, como contraseñas y datos personales. Además, destaca que la estrategia de ciberseguridad de Scotiabank incluye un enfoque global de prevención de incidentes, con un Centro de Operaciones de Seguridad en Toronto para monitorear posibles ataques o intrusiones en sus redes, y la oferta de herramientas y recursos educativos a los clientes para protegerse contra fraudes cibernéticos.

Nubank, el neobanco brasileño, sigue una estrategia similar, según Jag Duggal, director global de Producto de la fintech. La compañía utiliza "equipos rojos" a nivel global y de forma continua para identificar vulnerabilidades en su infraestructura, adoptando un enfoque global en el diseño de productos y plataformas tecnológicas, aunque adaptando un pequeño porcentaje al entorno local.

Riquelme, R. (2023, 13 noviembre). Ciberataques contra sector financiero se incrementan en México: industria. El Economista. https://www.eleconomista.com.mx/sectorfinanciero/Ciberataques-contra-sector-financiero-se-incrementan-en-Mexico-industria-20231112-0001.html

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: NOVIEMBRE 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-37924	11/22/2023	Apache Software Foundation Apache Submarine has an SQL injection vulnerability when a user logs in.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-37924

Descripción: This issue can result in unauthorized login. Now we have fixed this issue and now user must have the correct login to access workbench. This issue affects Apache Submarine: from 0.7.0 before 0.8.0. We recommend that all submarine users with 0.7.0 upgrade to 0.8.0, which not only fixes the issue, supports the oidc authentication mode, but also removes the case of unauthenticated logins. If using the version lower than 0.8.0 and not want to upgrade, you can try cherry-pick PR https://github.com/apache/submarine/pull/1037 https://github.com/apache/submarine/pull/1054 and rebuild the submarine-server image to fix this**.**

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-44324	11/17/2023	Adobe FrameMaker versions 2022 and earlier are affected by an Improper Authentication vulnerability that could result in a Security feature bypass.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-44324

Descripción: An unauthenticated attacker can abuse this vulnerability to access the API and leak default admin's password. Exploitation of this issue does not require user interaction.

TABLA DE VULNERABILIDADES RELEVANTES: NOVIEMBRE 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-34060	11/14/2023	VMware Cloud Director Appliance contains an authentication bypass vulnerability in case VMware Cloud Director Appliance was upgraded to 10.5 from an older version.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-34060

Descripción: On an upgraded version of VMware Cloud Director Appliance 10.5, a malicious actor with network access to the appliance can bypass login restrictions when authenticating on port 22 (ssh) or port 5480 (appliance management console) . This bypass is not present on port 443 (VCD provider and tenant login). On a new installation of VMware Cloud Director Appliance 10.5, the bypass is not present. VMware Cloud Director Appliance is impacted since it uses an affected version of sssd from the underlying Photon OS. The sssd issue is no longer present in versions of Photon OS that ship with sssd-2.8.1-11 or higher (Photon OS 3) or sssd-2.8.2-9 or higher (Photon OS 4 and 5).

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-5913	11/08/2023	Incorrect Privilege Assignment vulnerability in opentext Fortify ScanCentral DAST.	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-5913

Descripción: The vulnerability could be exploited to gain elevated privileges.This issue affects Fortify ScanCentral DAST versions 21.1, 21.2, 21.2.1, 22.1, 22.1.1, 22.2, 23.1.

TABLA DE VULNERABILIDADES RELEVANTES: NOVIEMBRE 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-4699	11/06/2023	Insufficient Verification of Data Authenticity vulnerability in Mitsubishi Electric Corporation	CVSS v3.1:9.1 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-4699

Descripción: MELSEC-F Series main modules and MELSEC iQ-F Series CPU modules allows a remote unauthenticated attacker to reset the memory of the products to factory default state and cause denial-of-service (DoS) condition on the products by sending specific packets.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-46817	11/03/2023	An issue was discovered in phpFox before 4.8.14.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-46817

Descripción: The url request parameter passed to the /core/redirect route is not properly sanitized before being used in a call to the unserialize() PHP function. This can be exploited by remote, unauthenticated attackers to inject arbitrary PHP objects into the application scope, allowing them to perform a variety of attacks, such as executing arbitrary PHP code.

TABLA DE VULNERABILIDADES RELEVANTES: NOVIEMBRE 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-42802	11/02/2023	GLPI is a free asset and IT management software package. Starting in version 10.0.7 and prior to version 10.0.10, an unverified object instantiation allows one to upload malicious PHP files to unwanted directories.	CVSS v3.1:9.8[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-42802

Descripción: The url request parameter passed to the /core/redirect route is not properly sanitized before being used in a call to the unserialize() PHP function. This can be exploited by remote, unauthenticated attackers to inject arbitrary PHP objects into the application scope, allowing them to perform a variety of attacks, such as executing arbitrary PHP code.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-20048	11/01/2023	A vulnerability in the web services interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute certain unauthorized configuration commands on a Firepower Threat Defense (FTD) device that is managed by the FMC Software.	CVSS v3.1:9.9[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-20048

Descripción: This vulnerability is due to insufficient authorization of configuration commands that are sent through the web service interface. An attacker could exploit this vulnerability by authenticating to the FMC web services interface and sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to execute certain configuration commands on the targeted FTD device. To successfully exploit this vulnerability, an attacker would need valid credentials on the FMC Software.

TABLA DE VULNERABILIDADES RELEVANTES: NOVIEMBRE 2023

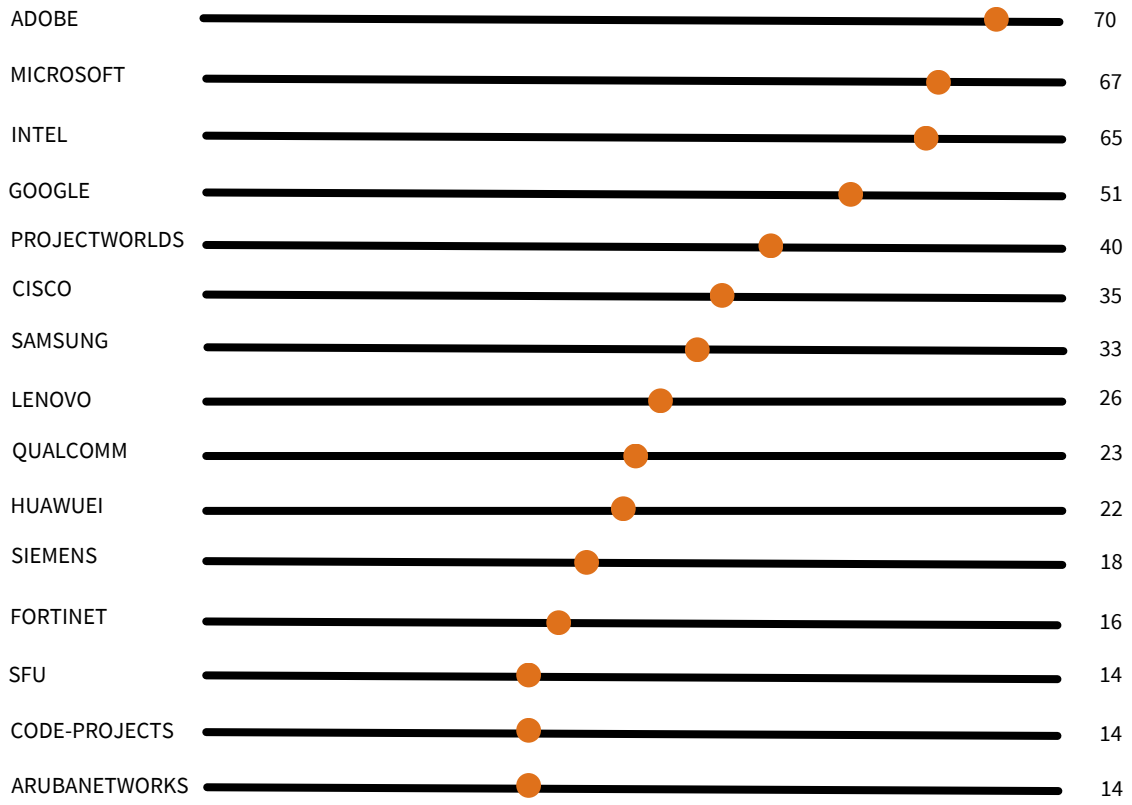
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-1716	11/01/2023	Cross-site scripting (XSS) vulnerability in Invoice Edit Page in Bitrix24	CVSS v3.1:9.6[critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-1716

Descripción: Bitrix24 22.0.300 allows attackers to execute arbitrary JavaScript code in the victim's browser, and possibly execute arbitrary PHP code on the server if the victim has administrator privilege.

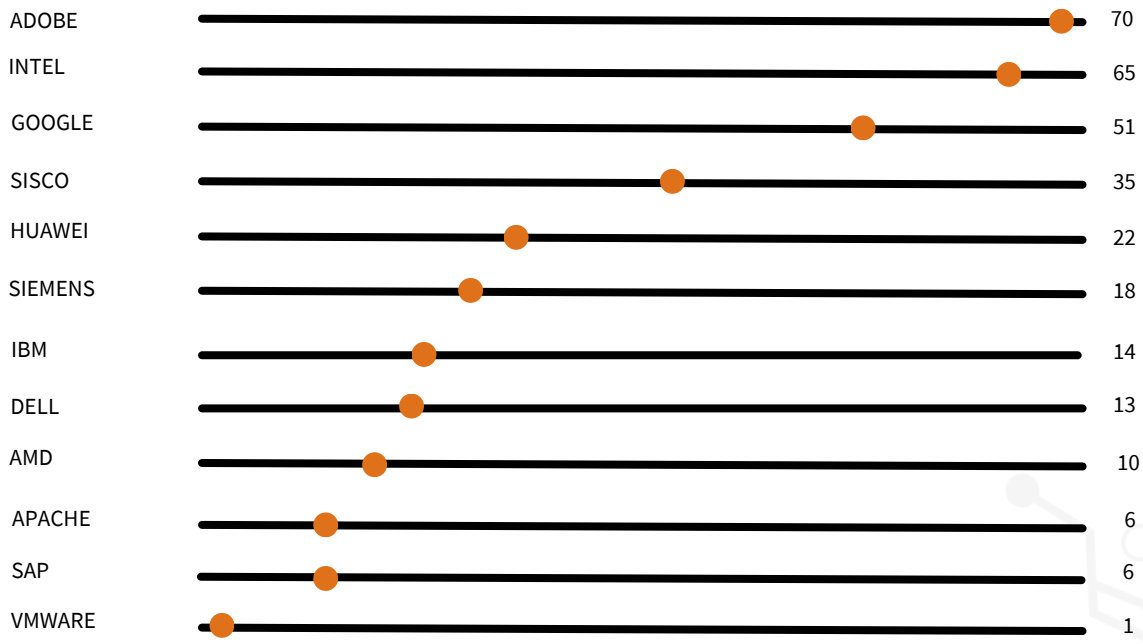
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-5766	11/01/2023	A remote code execution vulnerability in Remote Desktop Manager	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-5766

Descripción: In Remote Desktop Manager 2023.2.33 and earlier on Windows allows an attacker to remotely execute code from another windows user session on the same host via a specially crafted TCP packet.

FABRICANTES CON VULNERABILIDADES RELEVANTES: NOVIEMBRE DE 2023



EMPRESAS MULTINACIONALES CON VULNERABILIDADES: NOVIEMBRE DE 2023



CULTURA DE CIBERSEGURIDAD

BACKUPS

DEFINICIÓN.

Backup, respaldo, copia de seguridad o copia de reserva es una copia de los datos originales de un sistema de información o de un conjunto de software (archivos, documentos, etc.) que se almacena en un lugar seguro, con el fin de poder volver a disponer de su información en caso de que alguna eventualidad, accidente ocasione su pérdida del sistema.

El propósito principal de hacer copias de seguridad es garantizar la disponibilidad y la integridad de los datos en caso de pérdida, daño o eliminación accidental.

COMO FUNCIONA.

Identificación de Datos Críticos: Antes de realizar un backup, es crucial identificar qué datos son críticos y necesitan ser respaldados. Esto puede incluir archivos importantes, documentos, configuraciones de sistema, bases de datos, correos electrónicos, y más.
Selección del Método de Backup: Existen diferentes métodos de backup, y la elección depende de diversos factores, como la cantidad de datos, la frecuencia de cambio y la importancia de la información. Algunos métodos:

- Backup Completo: Se copian todos los datos seleccionados en cada ejecución.
- Backup Incremental: Se copian solo los datos que han cambiado desde la última copia de seguridad, reduciendo así el tiempo y los recursos necesarios. Sin embargo, la restauración puede ser más compleja ya que se necesitan todas las copias incrementales desde la última copia completa.
- Backup Diferencial: Se copian todos los datos que han cambiado desde la última copia completa. Aunque puede requerir más espacio de almacenamiento que un backup incremental, la restauración suele ser más rápida porque solo se necesitan la última copia completa y la copia diferencial más reciente.
- Ejecución del Backup: Una vez que se ha seleccionado el método de backup, se ejecuta el proceso. Esto puede hacerse manualmente o de manera programada, según las necesidades y la configuración del sistema.
- Almacenamiento Seguro: Las copias de seguridad se almacenan en un lugar seguro que está separado de los datos originales. Esto puede ser en dispositivos de almacenamiento externo, servidores remotos, servicios en la nube u otros medios seguros.
- Verificación: Después de realizar un backup, es recomendable verificar su integridad para asegurarse de que los datos se copiaron correctamente y están disponibles para su restauración.
- Periodicidad: Los backups deben realizarse de forma regular, dependiendo de la importancia de los datos y la frecuencia de cambio.
- Restauración: En caso de pérdida de datos, el proceso de restauración implica recuperar los datos desde las copias de seguridad.

RIESGOS / IMPORTANCIA DE CONOCER

La falta de realizar backups puede exponer a individuos y organizaciones a varios riesgos significativos. Entre alguno de ellos destacan:

- Pérdida de Datos Irreversible: Si no se realizan copias de seguridad, la pérdida de datos debido a factores como fallos de hardware, errores humanos, ataques de malware, Ransomware o desastres naturales puede resultar en la pérdida irreversible de información crítica. como documentos legales, registros financieros, proyectos de investigación, entre otros, lo que puede tener consecuencias graves para individuos y organizaciones.
- Impacto en la Continuidad del Negocio: La pérdida de datos puede tener un impacto grave en la continuidad del negocio. La falta de acceso a información vital puede interrumpir las operaciones normales y afectar la productividad.
- Costos de Recuperación Elevados: En caso de pérdida de datos, la recuperación puede ser costosa y llevar mucho tiempo. Los servicios de recuperación de datos especializados pueden ser costosos, y en algunos casos, la pérdida de datos puede ser irreversible.
- Daño a la Reputación: La pérdida de datos, especialmente si involucra información confidencial de clientes o socios, puede dañar la reputación de una organización. La pérdida de la confianza del cliente puede tener consecuencias a largo plazo.
- Incumplimiento de Regulaciones: En muchos sectores, existen regulaciones que exigen la protección y retención de datos. La falta de cumplimiento con estas regulaciones puede resultar en sanciones legales y multas significativas.

ALGÚN CASO CONOCIDO

Ataque de Ransomware a la Ciudad de Baltimore (2019):

En 2019, la ciudad de Baltimore fue víctima de un ataque de ransomware llamado RobbinHood que paralizó sus sistemas de tecnología de la información. El ransomware cifró archivos y sistemas, afectando servicios esenciales y bloqueando el acceso a datos críticos. Aunque la ciudad tenía algunos sistemas respaldados, la falta de una estrategia de backup integral complicó la recuperación sin pagar un rescate sustancial. Este incidente destaca la importancia de contar con medidas de seguridad sólidas y estrategias de backup efectivas para hacer frente a amenazas cibernéticas como el ransomware.

CÓMO EVITARLO

Evitar la pérdida de datos por falta de backup es esencial para garantizar la integridad y disponibilidad de la información crítica. A continuación, se enlistan unas recomendaciones:

Diversifica la Ubicación de los Backups:

- Almacena copias de seguridad en ubicaciones separadas de los datos originales para protegerte contra eventos catastróficos como incendios, inundaciones o robos.

Automatiza el Proceso de Backup:

- Configura sistemas automáticos de backup para reducir la posibilidad de errores humanos y garantizar la consistencia en la realización de copias de seguridad.

Realiza Pruebas de Recuperación:

- De manera periódica, realiza pruebas de recuperación para asegurarte de que las copias de seguridad sean efectivas y puedas restaurar los datos cuando sea necesario.

Monitorea y Audita Regularmente:

- Implementa herramientas de monitoreo para supervisar la integridad de los backups y realiza auditorías periódicas para garantizar el cumplimiento de las políticas de backup.

CÓMO DETECTARLO

Para detectar una pérdida de backups se podrían aplicar las siguientes medidas:

- Implementa herramientas de monitoreo que supervisen la integridad y disponibilidad de los backups de manera regular.
- Registro de Actividades (Logs).
- Configura alertas automáticas para notificar a los administradores en caso de errores o fallas en el proceso de backup.
- Revisa los registros de acceso y autorización para asegurarte de que solo personal autorizado tenga acceso a los backups.

CÓMO CONTENERLO

Implementa un Plan de Recuperación ante Desastres (DRP):

Desarrolla y sigue un plan de recuperación ante desastres que aborde cómo recuperar datos en caso de pérdida, incluida la pérdida de backups. Esto puede incluir estrategias para reconstruir o recuperar datos de fuentes alternativas.

CÓMO SOLUCIONARLO/REMEDIARLO

Implementa un Sistema de Backup Regular:

- Realiza backups de manera regular según la criticidad y la frecuencia de cambio de tus datos.
- Utiliza diferentes tipos de backups, como completos, incrementales o diferenciales, según sus necesidades y recursos.

CÓMO PUEDE AYUDAR ADV-IC

ADV Integradores y Consultores S.A de C.V es una empresa dedicada a la Ciberseguridad que, mediante el monitoreo continuo, la prevención de amenazas se minimiza el riesgo de infección de equipos por Ransware, borrado de bases de datos por acceso no autorizado de usuarios privilegiados.

REFERENCIAS

REFERENCIAS

- Equipo editorial, Etecé. (2023, 19 noviembre). Backup - concepto, usos y cómo hacer backups. Concepto. https://concepto.de/backup/#ixzz8K9v94nzi
- Grustniy, L. (2019, 22 noviembre). Baltimore cifrada. Kaspersky. Recuperado 29 de noviembre de 2023, de https://www.kaspersky.es/blog/baltimore-encrypted/18554/
- Microsoft recupera la mayor a de los datos de Sidekick. | Noticias - CSI -. (s. f.). https://www.cert.unam.mx/historico/noticias/index.html-noti=3463

ZERU

Cybersecurity Services

Security Operation Center - SOC by

ADV

+52 81 2011 8604

contacto@adv-ic.com

Av. Melchor Ocampo 193, Torre Privanza, Piso 11 Oficina 11D
Colonia Veronica Anzures. Delegación Miguel Hidalgo CP 11300