BOLETÍN DE CIBERSEGURIDAD

JULIO 2023

ÍNDICE

NOTICIAS INTERNACIONALES 3

Hackers chinos usaron fallo en código para robar correos electrónicos de agencias de EU: Microsoft 4

IA podría vulnerar la seguridad de usuarios en pagos y criptomonedas 5

La filtración de datos de Roblox deja al descubierto datos de desarrolladores 7

Varios periódicos españoles sufren problemas por ataques informáticos prorrusos 8

NOTICIAS NACIONALES 10

La grave vulnerabilidad que puede vivir México, el INAI urgió Ley de Ciberseguridad 11

México, el más afectado por ciberataques en lo que va del año 13

VULNERAVILIDADES RELEVANTES 15

Tabla de vulnerabilidades relevantes: Julio 2023 16

Fabricantes y sus vulnerabilidades relevantes: Julio 2023 19

Empresas Multinacionales y sus vulnerabilidades: Julio 2023 20

CULTURA DE CIBERSEGURIDAD 21

Seguridad en la nube 22

REFERENCIAS 31

NOTICIAS INTERNACIONALES

HACKERS CHINOS USARON FALLO EN CÓDIGO PARA ROBAR CORREOS ELECTRÓNICOS DE AGENCIAS DE EU: MICROSOFT

MICROSOFT NO HA IDENTIFICADO EL OBJETIVO DEL ATAQUE, PERO HA RECONOCIDO QUE VARIAS VÍCTIMAS SE VIERON AFECTADAS, INCLUIDOS FUNCIONARIOS DEL DEPARTAMENTO DE ESTADO, EL DEPARTAMENTO DE COMERCIO Y LA CÁMARA DE REPRESENTANTES DE EE. UU.

IEl Economista. (2023, 15 julio). Hackers chinos usaron fallo en código para robar correos electrónicos de agencias de EU: Microsoft. El Economista. https://www.eleconomista.com.mx/tecnologia/Hackers-chinos-usaron-fallo-en-codigo-para-robar-correos-electronicos-de-agencias-de-EU-Microsoft-20230714-0067.html

Microsoft ha anunciado que los piratas informáticos chinos han aprovechado una vulnerabilidad de piratería. En una publicación de blog publicada el viernes, la compañía informó que los piratas informáticos del gigante asiático pudieron explotar una "falla de validación en el código de Microsoft" para lograr este efecto. El gobierno chino ha negado cualquier participación en espionaje.

Microsoft y funcionarios estadounidenses dijeron el miércoles por la noche que piratas informáticos del gobierno chino han accedido subrepticiamente a cuentas de correo electrónico de unas 25 organizaciones desde mayo. Esto incluyó al menos dos agencias gubernamentales.

Microsoft no ha identificado el objetivo del ataque, pero ha reconocido que varias víctimas se vieron afectadas, incluidos funcionarios del Departamento de Estado, el Departamento de Comercio y la Cámara de Representantes de EE. UU. El ministro de Relaciones Exteriores, Antony Brinken, le dijo al alto diplomático chino Wang Yi en una reunión en Yakarta el jueves que estaba "profundamente" preocupado por cualquier acción tomada contra el gobierno, las empresas y las personas de EE. UU., dijo.
"Tomaremos las medidas apropiadas para responsabilizar a los responsables", agregó, según un alto funcionario del Departamento de Estado.

Las prácticas de los servicios de seguridad de Microsoft están sujetas a un intenso escrutinio y son exigidas por funcionarios gubernamentales y legisladores. La empresa con sede en Redmond, Washington, crea un registro de auditoría digital de clase mundial, también conocido como registro, de libre acceso para todos los clientes.

IA PODRÍA VULNERAR LA SEGURIDAD DE USUARIOS EN PAGOS Y CRIPTOMONEDAS

LAS INSTITUCIONES FINANCIERAS DEBEN CREAR CONCIENCIA SOBRE LAS FALSIFICACIONES PROFUNDAS. EL ESTUDIO ENCUESTÓ A 8.055 USUARIOS DE MANERA UNIFORME EN EL REINO UNIDO, EE. UU., SINGAPUR Y MÉXICO. MÁS DEL 67% DIJO QUE CONOCÍA LAS HERRAMIENTAS DE IA GENERATIVA

Estrada, S. (2023, 5 julio). IA Podría vulnerar la seguridad de usuarios en pagos y criptomonedas. El Economista. https://www.eleconomista.com.mx/sectorfinanciero/IA-podria-vulnerar-la-seguridad-de-usuarios-en-pagos-y-criptomonedas-20230704-0094.html

Los avances tecnológicos, como las herramientas de inteligencia artificial (IA), están impulsando la innovación en el sector financiero. Sin embargo, también aumenta el riesgo de fraude digital.

La investigación realizada por Censuswide y Jumio muestra que la IA se usa para generar caras falsas, lo que compromete la identidad de los usuarios de servicios digitales (también conocidos como falsificaciones profundas). en tendencia ascendente. Según lo señalado existe una mayor presencia en los sectores de pagos y criptomonedas.

Ante la aplicación herramientas para el fraude, 52% de los encuestados cree que podría detectar un video creado con IA, sin embargo, el estudio señala que ello puede reflejar un exceso de confianza por parte de los usuarios, dado que los fraudes han alcanzado un nivel de sofisticación que impide su detección a simple vista.

"Las manipulaciones de videos, fotos que hablan o parpadean ese tipo de cosas son cada vez más importantes, las entidades financieras y las firmas de identidad digital tenemos que tomar un rol activo para concientizar de los riesgos", comentó Samer Atassi, vicepresidente para Latinoamérica de Jumio.

IA PODRÍA VULNERAR LA SEGURIDAD DE USUARIOS EN PAGOS Y CRIPTOMONEDAS

Según lo indicado por Atassi, las regulaciones existentes en el sector financiero obligan a la validación de cuentas para transaccionar, por lo que la entidad financiera debe capturar el rostro del usuario y validarlo con una fuente de datos oficial. Sin embargo, ello también puede conducir a una falsa seguridad, debido a que la validación sigue siendo vulnerable ante procesos como el deepfake. La encuesta reveló que, de las entidades del sector financiero, 43% preferían utilizar una identidad digital adicional a únicamente un documento de identidad físico.

"Las entidades financieras se tienen que asegurar que capturan información válida", dijo Atassi.

LA FILTRACIÓN DE DATOS DE ROBLOX DEJA AL DESCUBIERTO DATOS DE DESARROLLADORES

LOS ASISTENTES A LA CONFERENCIA DE DESARROLLADORES DE ROBLOX PUEDEN HABER EXPERIMENTADO UNA VIOLACIÓN DE DATOS ENTRE 2017 Y 2021. TROY HUNT, INVENTOR DEL SITIO WEB HAVE I BEEN PWNED, HA ANUNCIADO QUE LA NOTICIA DE UNA VIOLACIÓN DE DATOS EN X (ANTERIORMENTE TWITTER) SE HA VUELTO VIRAL.

Cyber Security Hub. (2023, 25 julio). Roblox data breach exposes developer data. https://www.cshub.com/attacks/news/roblox-developer-data-leak

Have I Been Pwned permite a los usuarios buscar su nombre e información para determinar si han estado expuestos a una violación de datos.

En un mensaje anónimo a Hunt, una fuente afirma que todos en la Conferencia de desarrolladores de Roblox fueron testigos de la violación de datos. Las fuentes dijeron que los datos a los que se accedió durante el ataque cibernético incluían nombres, fechas de nacimiento, direcciones de correo electrónico, direcciones de casa e IP y números de teléfono. Las fuentes también afirmaron que los datos se filtraron a Internet.

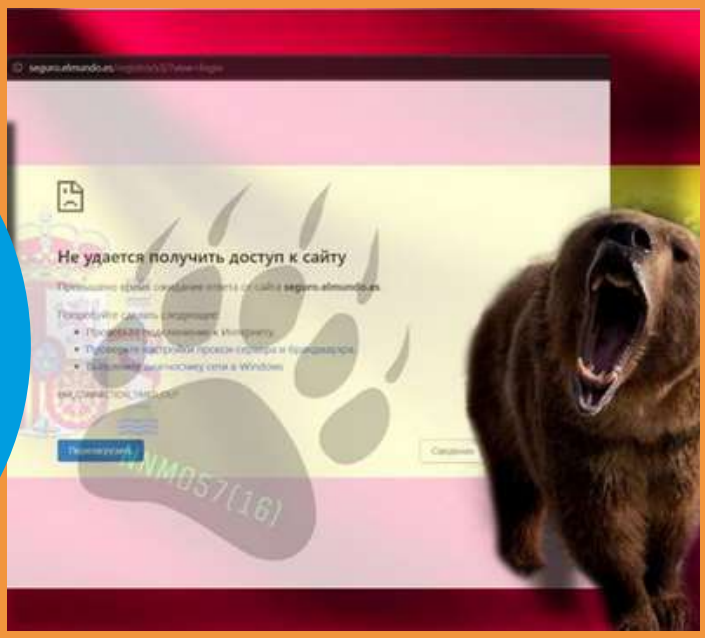
Las fuentes dijeron que descubrieron la filtración después de que un "turco" los contactó a través de WhatsApp después de buscar su nombre de usuario. Verificaron "Have I Been Pwned" para ver si fueron víctimas de una violación de datos, pero aparentemente no lo fueron. Luego, la fuente se puso en contacto con Hunt y le pidió que proporcionara detalles de la violación de datos en el sitio web.

Otra fuente se puso en contacto con Hunt y le notificó una violación de datos. Confirmando la información ya enviada a Hunt, las fuentes dicen que Roblox nunca reveló la violación de datos pública o internamente, y que los afectados no fueron informados del ciberataque.

La filtración se volvió a publicar recientemente en línea y recibió "considerable atención" de partes maliciosas y no maliciosas, según las fuentes. Las fuentes afirmaron que era cierto.

VARIOS PERIÓDICOS ESPAÑOLES SUFREN PROBLEMAS POR ATAQUES INFORMÁTICOS PRORRUSOS

VARIOS DIARIOS ESPAÑOLES, ENTRE ELLOS EL MUNDO, EXPANSIÓN Y ABC, HAN SUFRIDO ATAQUES INFORMÁTICOS EN LAS ÚLTIMAS HORAS QUE HAN DEJADO INACCESIBLES SUS SITIOS WEB Y CAUSADOS PROBLEMAS TÉCNICOS.



Arghire, I. (2023). 200,000 WordPress Sites Exposed to Attacks Exploiting Flaw in 'Ultimate Member' Plugin. SecurityWeek. https://www.securityweek.com/200000-wordpress-sites-exposed-to-attacks-exploiting-flaw-in-ultimate-member-plugin/?web_view=true

El sabotaje fue llevado a cabo por el grupo de hackers prorrusos NoName057, según el diario ABC, que experimentó un apagón la madrugada del martes que impidió a los usuarios identificarse con contraseñas. El Español también se quejó de que en la mañana los lectores sufrieron los mismos ataques que impidieron el acceso normal.

Este no es el primer caso de ataque informático registrado en los últimos días. El domingo durante las elecciones, el mismo grupo cerró las webs del Ministerio del Interior, INE, Junta Electoral y Moncloa, y eliminó temporalmente las páginas de las empresas de transporte Renfe y Sociobus.

El grupo NoName057 lleva varios días denunciando en su canal de Telegram estos ataques contra organizaciones y medios españoles. "El escudo de España dice Plus Ultra (más allá de las fronteras). "Lamentablemente, el Gobierno español ha malinterpretado el lema oficial de la patria, adoptado por Carlos V en 1492, y está más allá de los límites de la estupidez", escribió este martes el grupo junto al anuncio de que las webs de Casa Real también fueron hackeadas.

El mismo mensaje se refería al suministro de tanques y armas al ejército ucraniano. El apoyo del gobierno español a Ucrania es la razón por la que el grupo de hackers apunta a España. "Prorrusos" no significa que sean rusos, incluso podrían ser españoles que simpatizan con Putin. De hecho, comenzaron a actuar desde el comienzo de la guerra y, a menudo, hablaban de agresión en sus afirmaciones de autoría de los ataques", explica el experto en ciberseguridad Marcelino Madrigal. "Sus ataques cuestan dinero, así que no cobran dinero." Pequeño y fácil de controlar. El propósito es puramente ideológico", agregó.

VARIOS PERIÓDICOS ESPAÑOLES SUFREN PROBLEMAS POR ATAQUES INFORMÁTICOS PRORRUSOS

Este ataque consiste en un llamado DDos (abreviatura de Distributed Denial of Service Attack) y consiste en tráfico de inundación. Según ABC, se han dado a conocer los resultados de una investigación realizada por la Oficina de Coordinación de Ciberseguridad (OCC) y el Comisionado de Información General. Se dijo que el ciberataque fue llevado a cabo por el mismo grupo de piratas informáticos que paralizó varios periódicos el martes.

Actualmente, el Ministerio del Interior aún tiene que revelar el error, pero el Ministerio del Interior culpa del error al trabajo de mantenimiento. El mismo día, el grupo también reivindicó un ataque informático contra el Banco Cooperativo España contra la plataforma de compra de billetes de autobús de Moveria y el diario Expanción.

NOTICIAS NACIONALES

LA GRAVE VULNERABILIDAD QUE PUEDE VIVIR MÉXICO, EL INAI URGIÓ LEY DE CIBERSEGURIDAD

COMISIONADOS DEL INSTITUTO NACIONAL DE TRANSPARENCIA ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES (INAI) REITERARON AL PODER LEGISLATIVO LA URGENCIA DE LA CREACIÓN DE UNA LEY DE CIBERSEGURIDAD, ASÍ COMO LA ACTUALIZACIÓN DE LA NORMATIVIDAD DE PROTECCIÓN A DATOS PERSONALES.

País, E., País, E., & País, E. (2023b, julio 25). Varios periódicos españoles sufren problemas por ataques informáticos prorrusos. El País. https://elpais.com/tecnologia/2023-07-25/varios-periodicos-espanoles-sufren-problemas-por-ataques-informaticos.html

Blanca Lilia Ibarra, comisionada presidenta del INAI, defendió que este órgano actúa con autonomía, imparcialidad y criterios técnico (@INAImexico). Desde Tlaxcala y durante la Jornada Regional de Transparencia Municipal, Ciudadanía Digital y Rendición de Cuentas, la comisionada de la institución Norma Julieta del Río Venegas, aseguró que actualmente el marco normativo en la materia está desactualizado.

En este sentido aseguró que este es uno de los puntos que se suma a la lista de trabajo contemplada en el Senado de la República.

“Hay que decirlo como es, necesitamos actualizarlo; necesitamos una Ley de Ciberseguridad. Hay muchos proyectos en el Senado no los han sacado porque están viendo los nombramientos del INAI; entonces, cuando salgan los nombramientos, seguramente van a salir esas leyes”, comentó.

De acuerdo con Julieta del Río Venegas actualmente desde el instituto se aplican “soluciones integrales” que contemplan tanto software como hardware para garantizar la seguridad de las innovaciones tecnológicas empleadas por el Instituto.

Entre los desarrollos tecnológicos empleados por el órgano autónomo se encuentra la aplicación de la

LA GRAVE VULNERABILIDAD QUE PUEDE VIVIR MÉXICO, EL INAI URGIÓ LEY DE CIBERSEGURIDAD

Inteligencia Artificial para el desarrollo del CAVI (asistente virtual) así como para la Plataforma Nacional de Transparencia. De acuerdo con el Índice de Ciberseguridad Global (ICG) de la Unión Internacional de Telecomunicaciones, México ocupa el lugar 63 de 175 países en materia de preparación de seguridad cibernética.

Si bien en el país se contempla la protección de activos digitales, con la Ley Federal de Protección de Datos Digitales, aún existen lagunas en el marco normativo debido al rezago sobre la regulación en la materia. Y es que, el territorio mexicano es uno de los países de América Latina que, según el Reporte de Ciberseguridad 2020 del BID, no cuenta con un marco legal sobre delitos informáticos.

Bajo este sentido, apenas en abril de este 2023 presentó la iniciativa de Ley Federal de Ciberseguridad, misma que tiene como objetivo el “el aumentar la seguridad cibernética bajo un esquema de corresponsabilidad, prevención, combate y persecución de los delitos cibernéticos o ciberdelitos, a su vez la protección de datos personales y el respeto a los derechos humanos”.

Dentro de la iniciativa se detalla que la ciberseguridad implica el uso de herramientas informáticas, como firewalls, software antivirus, autenticación y cifrado de datos, por mencionar algunas.

MÉXICO, EL MÁS AFECTADO POR CIBERATAQUES EN LO QUE VA DEL AÑO

LA ORGANIZACIÓN INTERNACIONAL DE HACKERS Y EXPERTOS EN CIBERSEGURIDAD (OIHEC), ENCABEZADA Y FUNDADA POR HÉCTOR LÓPEZ, FUE ÚNICO DE LA COMPAÑÍA CONSULTADOS DURANTE EL PRIMER TROTE DE CIBERSEGURIDAD LEGISLATIVA Y DE POLÍTICA PÚBLICA

Pérez, Á. L. (2023). México, el más afectado por ciberataques en lo que va del año | Ventas de seguridad. https://www.ventasdeseguridad.com/2023072523481/noticias/empresas/mexico-el-mas-afectado-por-ciberataques-en-2023.html

El informe precisó, además, que las empresas mexicanas enfrentan amenazas a la ciberseguridad de dos clases: una es el daño directo a su infraestructura y la segunda es el ataque a los colaboradores (usuarios finales). De este modo, los criminales buscan comprometer las redes internas de las empresas, así como la conectividad de los usuarios internos y externos, los servidores y páginas web del negocio.

Principales estrategias para cometer crímenes en línea

- Ataques de correo electrónico o phishing.
- Ataques a la red.
- Ataques a la nube.
-

Ataques de ransomware a aplicaciones, dispositivos, puntos de conexión, a terceros o eslabones de la cadena de suministro.

Retos y oportunidades

De acuerdo con Ricardo Pulgarín, arquitecto senior de Soluciones de seguridad de Cirion Technologies, muchas empresas están adquiriendo cierta madurez en temas de ciberseguridad. Sin embargo, falta profundizar en cuanto a cultura y medidas para neutralizar los ataques.

“La recapacitación es fundamental y debe estar respaldada por una correcta implementación de políticas y protocolos de ciberseguridad. El enfoque debe ponerse en lo operacional y en la seguridad de la información”, señala él.

Otra de las apreciaciones de Pulgarín es que aunque cualquier implementación para contrarrestar la problemática requiera una inversión, no realizarla probablemente resulte más costoso si se llega a recibir un ataque que alcance a los usuarios o a las infraestructuras propias.

“Se vuelve fundamental que las empresas comiencen a tener planes de ciberseguridad que permitan establecer políticas, definir las herramientas, controles y procesos idóneos que deben aplicarse. Adicionalmente, es necesario que cada organización elija un socio estratégico que la apoye para implementar este tipo de plan”, agrega.

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: JULIO 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-3956	07/27/2023	The InstaWP Connect plugin for WordPress is vulnerable	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-3956

Descripción: The InstaWP Connect plugin for WordPress is vulnerable to unauthorized access of data, modification of data and loss of data due to a missing capability check on the 'events_receiver' function in versions up to, and including, 0.0.9.18. This makes it possible for unauthenticated attackers to add, modify or delete post and taxonomy, install, activate or deactivate plugin, change customizer settings, add or modify or delete user including administrator user.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-35087	07/21/2023	It is identified a format string vulnerability	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-35087

Descripción: This vulnerability is caused by lacking validation for a specific value when calling cm_processChangedConfigMsg in ccm_processREQ_CHANGED_CONFIG function in AiMesh system. An unauthenticated remote attacker can exploit this vulnerability without privilege to perform remote arbitrary code execution, arbitrary system operation or disrupt service. This issue affects RT-AX56U V2: 3.0.0.4.386_50460; RT-AC86U: 3.0.0.4_386_51529.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-3859	07/23/2023	A vulnerability was found in phpscriptpoint Car Listing	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-3859

Descripción: This issue affects some unknown processing of the file /search.php of the component GET Parameter Handler. The manipulation of the argument brand_id/model_id/car_condition/car_category_id/body_type_id/fuel_type_id/transmission_type_id/year/mileage_start/mileage_end/country/state/city leads to sql injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-235211. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-3850	07/23/2023	A vulnerability has been found in SourceCodes	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-3850

Descripción: Affected by this vulnerability is an unknown functionality of the file /classes/Master.php?f=delete_category of the component HTTP POST Request Handler. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The identifier VDB-235201 was assigned to this vulnerability.

TABLA DE VULNERABILIDADES RELEVANTES: JULIO 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-37466	07/13/2023	vm2 is an advanced vm/sandbox for Node.js.	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-37466

Descripción: The maintenance of the project has been discontinued. In vm2 for versions up to 3.9.19, `Promise` handler sanitization can be bypassed with `@@species` accessor property allowing attackers to escape the sandbox and run arbitrary code. Remote Code Execution, assuming the attacker has arbitrary code execution primitive inside the context of vm2 sandbox.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-37278	07/13/2023	GLPI is a Free Asset and IT Management Software	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-37278

Descripción: An administrator can trigger SQL injection via dashboards administration. This vulnerability has been patched in version 10.0.9.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-3624	07/13/2023	A vulnerability classified as critical has been found in Nesote	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-3624

Descripción: This affects an unknown part of the file /index.php/coins/update_marketboxslider of the component POST Parameter Handler. The manipulation of the argument marketcurrency leads to sql injection. It is possible to initiate the attack remotely. The identifier VDB-233577 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-33150	07/11/2023	Microsoft Office Security Feature Bypass Vulnerability	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-33150

Descripción: Exploitation of the vulnerability requires the victim to open a specially crafted file and click through Office Security Prompt(s). An attacker would have no way to force users to open the file. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability.

TABLA DE VULNERABILIDADES RELEVANTES: JULIO 2023

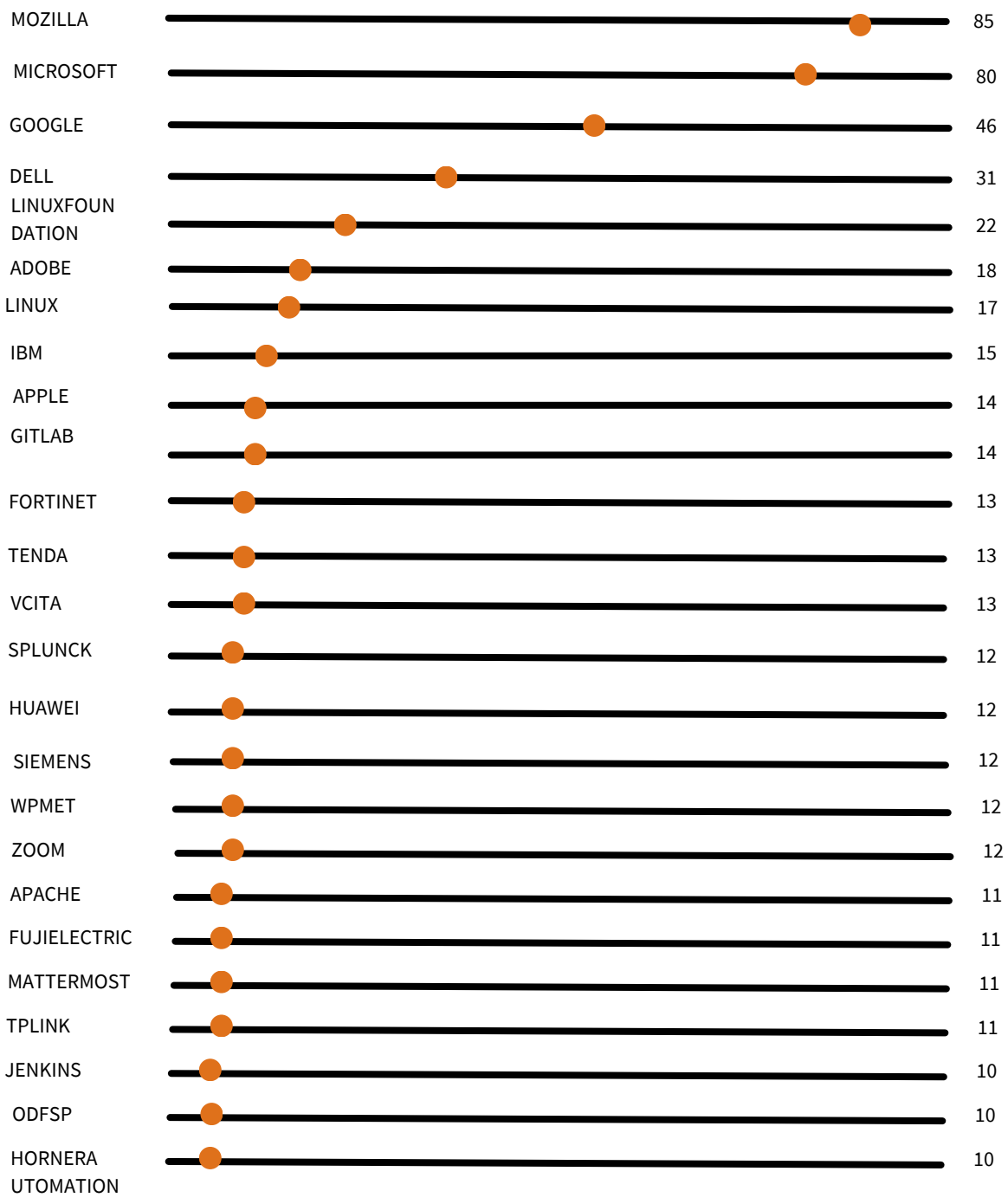
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-26258	07/03/2023	Arcserve UDP through 9.0.6034 allows authentication	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-26258

Descripción: The method getVersionInfo at WebServiceImpl/services/FlashServiceImpl leaks the AuthUUID token. This token can be used at /WebServiceImpl/services/VirtualStandbyServiceImpl to obtain a valid session. This session can be used to execute any task as administrator.

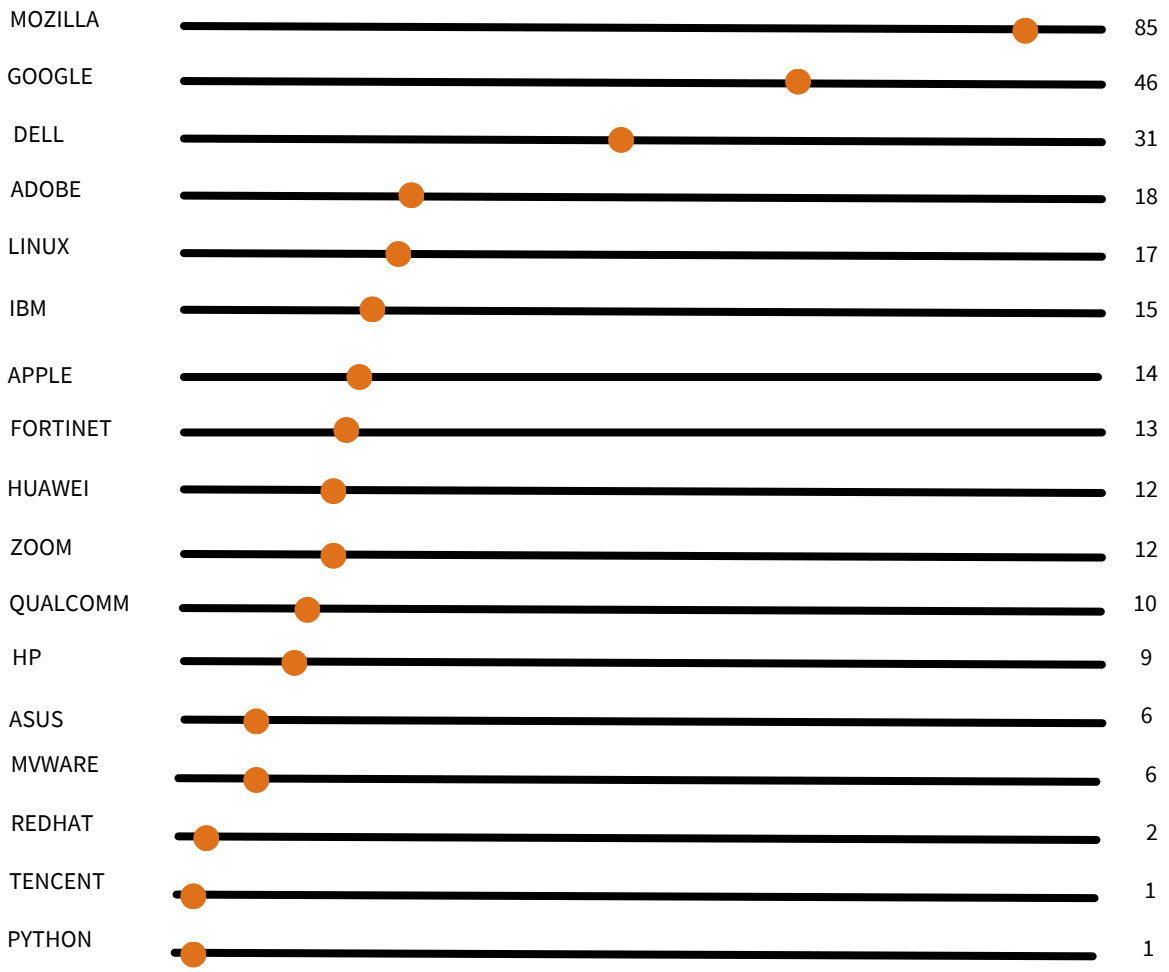
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-35797	07/03/2023	Improper Input Validation vulnerability	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-35797

Descripción: This issue affects Apache Airflow Apache Hive Provider: before 6.1.1. Before version 6.1.1 it was possible to bypass the security check to RCE via principal parameter. For this to be exploited it requires access to modifying the connection details. It is recommended updating provider version to 6.1.1 in order to avoid this vulnerability.

FABRICANTES Y SUS VULNERABILIDADES RELEVANTES: JULIO DE 2023



EMPRESAS MULTINACIONALES Y SUS VULNERABILIDADES: JULIO DE 2023



CULTURA DE CIBERSEGURIDAD

SEGURIDAD EN LA NUBE

La seguridad en la nube es una disciplina de la ciberseguridad dedicada a asegurar los sistemas informáticos en la nube. Incluye mantener los datos privados y seguros a través de la infraestructura, las aplicaciones y las plataformas en línea. Asegurar estos sistemas implica los esfuerzos de los proveedores de la nube y de los clientes que los utilizan, bien se trate de una persona, una pequeña o mediana empresa o una organización.

En su núcleo, la seguridad en la nube se compone de las siguientes categorías:

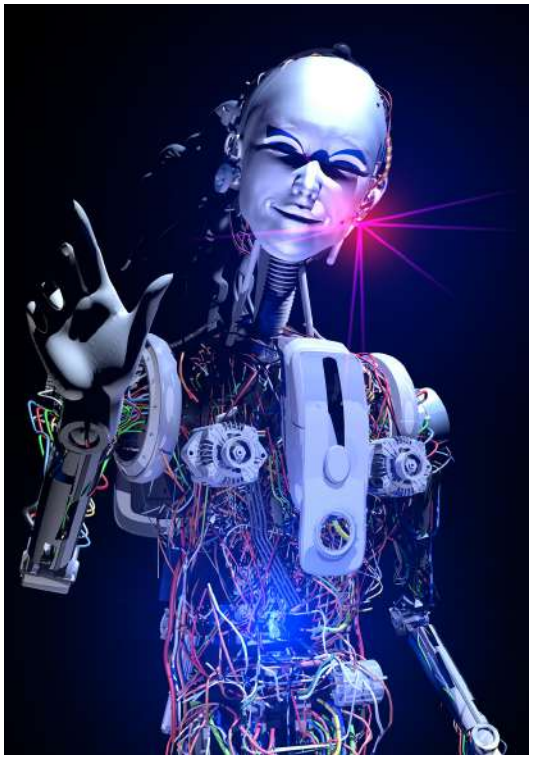
- Seguridad los datos
- Gestión de identidades y accesos (IAM, por sus siglas en inglés)
- Gobernanza (políticas de prevención, detección y mitigación de amenazas)
- Planificación de la retención de datos (DR) y la continuidad del negocio (BC)
- Cumplimiento legal

La seguridad en la nube puede parecer como la seguridad informática heredada, pero esta plataforma exige en realidad un enfoque diferente.
La seguridad en la nube es toda la tecnología, los protocolos y las buenas prácticas que protegen los entornos informáticos en la nube, las aplicaciones que se ejecutan en la nube y los datos almacenados en ella. La seguridad de los servicios en la nube comienza por comprender qué se está asegurando exactamente, así como los aspectos del sistema que se deben administrar.

El alcance total de la seguridad en la nube está diseñado para proteger lo siguiente, independientemente de sus responsabilidades:

- **Redes físicas:** enrutadores, energía eléctrica, cableado, controles de clima, etc.
- **Almacenamiento de datos:** discos duros, etc.
- **Servidores de datos:** hardware y software informáticos de la red central
- **Plataformas de virtualización de equipos informáticos:** software de máquinas virtuales, máquinas anfitrionas y máquinas invitadas
- **Sistemas operativos (OS):** software que soporta todas las funciones informáticas
- **Middleware:** gestión de la interfaz de programación de aplicaciones (API),
- **Entornos de ejecución:** ejecución y mantenimiento de un programa en ejecución
- **Datos:** toda la información almacenada, modificada y a la que se ha accedido
- **Aplicaciones:** servicios tradicionales de software (correo electrónico, software de impuestos, paquetes de productividad, etc.)
- **Hardware de usuario final:** ordenadores, dispositivos móviles, dispositivos de Internet de las cosas (IoT), etc.

LOS TIPOS DE SERVICIOS EN LA NUBE



- **El núcleo de cualquier servicio de la nube de terceros** implica que el proveedor administre la red física, el almacenamiento de datos, los servidores de datos y las plataformas de virtualización de los ordenadores. El servicio se almacena en los servidores del proveedor y se virtualiza a través de su red administrada internamente para entregarse a los clientes para su acceso remoto. Esto transfiere los costes de hardware y otras infraestructuras para proporcionar a los clientes acceso a sus necesidades informáticas desde cualquier lugar a través de su conexión a Internet.

- **Los servicios en la nube de software como servicio (SaaS)** proporcionan a los clientes acceso a aplicaciones que están puramente alojadas y se ejecutan en los servidores del proveedor. Los proveedores administran las aplicaciones, los datos, el tiempo de ejecución, el middleware y el sistema operativo. Los clientes solamente se encargan de obtener y utilizar las aplicaciones. Algunos ejemplos de SaaS incluyen Google Drive, Slack, Salesforce, Microsoft 365, Cisco WebEx y Evernote.

- **Los servicios en la nube de plataforma como servicio** proporcionan a los clientes un host para el desarrollo de sus propias aplicaciones, que se ejecutan dentro del propio espacio “sandbox” del cliente en los servidores del proveedor. Los proveedores administran el tiempo de ejecución, el middleware y el sistema operativo. Los clientes se encargan de gestionar sus aplicaciones, datos, acceso de usuarios, dispositivos de usuarios finales y redes de usuarios finales. Algunos ejemplos de PaaS incluyen Google App Engine y Windows Azure.

- **Los servicios en la nube de infraestructura como servicio (IaaS)** ofrecen a los clientes hardware y plataformas de conectividad remota para alojar la mayor parte de sus tareas informáticas, incluido el sistema operativo. Los proveedores solo administran los servicios básicos en la nube. Los clientes se encargan de asegurar todo lo que se apila en un sistema operativo, incluidas las aplicaciones, los datos, los tiempos de ejecución, el middleware y el propio sistema operativo. Además, los clientes deben gestionar el acceso de los usuarios, los dispositivos de usuarios finales y las redes de usuarios finales. Algunos ejemplos de IaaS incluyen Microsoft Azure, Google Compute Engine (GCE) y Amazon Web Services (AWS).

LOS ENTORNOS DE LA NUBE

LOS ENTORNOS DE LA NUBE

- **Entornos de nubes públicas,** compuestos por servicios en la nube de varios usuarios en los que un cliente comparte los servidores de un proveedor con otros clientes, como un edificio de oficinas o un espacio de trabajo. Se trata de servicios de terceros dirigidos por el proveedor para dar acceso a los clientes a través de la web.
- **Entornos de nubes privadas de terceros,** que se basan en el uso de un servicio en la nube que proporciona al cliente el uso exclusivo de su propia nube. Estos entornos de un solo usuario normalmente son propiedad de un proveedor externo, y se administran y operan fuera del sitio.
- **Entornos de nubes privadas internas**, que también se componen de servidores de servicios en la nube de un solo usuario, pero se operan desde su propio centro de datos privado. En este caso, este entorno de la nube es gestionado por las propias empresas para permitir la configuración completa de cada elemento.
- **Entornos de varias nubes**, que incluyen el uso de dos o más servicios en la nube de proveedores independientes. Estos pueden ser cualquier combinación de servicios públicos o privados en la nube.
- **Entornos de nubes híbridas**, que consisten en el uso de una combinación de nube privada de terceros o centro de datos de nubes privadas in situ con una o más nubes públicas.

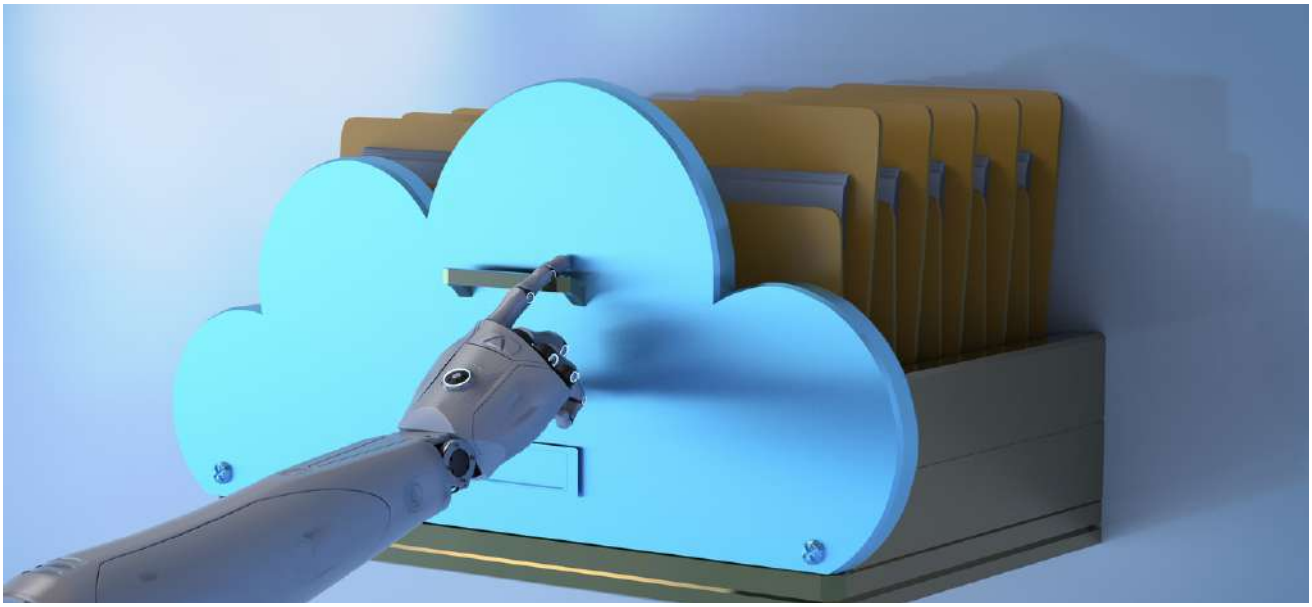
Al enfocarlo desde esta perspectiva, podemos entender que la seguridad basada en la nube puede ser un poco diferente según el tipo de espacio de nubes en el que trabajen los usuarios. No obstante, los efectos se sienten tanto en los clientes individuales como en las empresas.

¿CÓMO FUNCIONA LA SEGURIDAD EN LA NUBE?

Cada medida de seguridad en la nube funciona para lograr uno o más de los siguientes objetivos:

- Permitir la recuperación de datos en caso de pérdida de datos
- Proteger el almacenamiento y las redes contra el robo de datos malicioso
- Evitar los errores humanos o negligencias que causan la fuga de datos
- Reducir el impacto de cualquier compromiso de datos o sistemas

SEGURIDAD EN LA NUBE



La seguridad de los datos es un aspecto de la seguridad en la nube que implica el fin técnico de la prevención de amenazas. Existen herramientas y tecnologías que permiten a los proveedores y los clientes insertar barreras entre el acceso y la visibilidad de los datos confidenciales. Entre ellas, el cifrado es una de las herramientas más potentes disponibles. El cifrado codifica los datos para que solo los pueda leer alguien que tenga la clave de cifrado. En caso de pérdida o robo de los datos, no será posible leerlos ni interpretarlos. Las protecciones para el tráfico de datos, tales como las redes privadas virtuales (VPN), también ganan importancia en las redes de la nube.

La gestión de identidades y accesos (IAM) se refiere a los privilegios de acceso que se ofrecen a las cuentas de los usuarios. La gestión de la autenticación y la autorización de las cuentas de usuario también se aplica aquí. Los controles de acceso son fundamentales para restringir a los usuarios, tanto a los legítimos como a los maliciosos, el acceso y el compromiso de los datos confidenciales y sistemas. La gestión de contraseñas, la autenticación de varios factores y otros métodos entran en el alcance de la IAM.

La gobernanza se centra en las políticas de prevención, detección y mitigación de amenazas. Con PYMES y empresas, aspectos como la información sobre amenazas pueden ayudar a rastrear y priorizar las amenazas para mantener los sistemas esenciales vigilados cuidadosamente. Sin embargo, incluso los clientes individuales de la nube podrían beneficiarse de la valoración de las políticas y la formación sobre el comportamiento seguro del usuario. Estas se aplican sobre todo en los entornos empresariales, pero las normas para el uso seguro y la respuesta a las amenazas pueden ser útiles para cualquier usuario.

La planificación de la retención de datos (DR) y la continuidad del negocio (BC) implica medidas técnicas de recuperación de desastres en caso de pérdida de datos. Los métodos para la redundancia de datos, como las copias de seguridad, son fundamentales para cualquier plan de DR y BC. Además, disponer de sistemas técnicos para garantizar la continuidad de las operaciones puede ser de gran ayuda. Las plataformas para probar la validez de las copias de seguridad y las instrucciones detalladas de recuperación de los empleados son igual de valiosas para un plan de BC completo.

SEGURIDAD EN LA NUBE

El cumplimiento legal gira en torno a la protección de la privacidad del usuario, tal como lo establecen los órganos legislativos. Los gobiernos asumieron la importancia de proteger la información de los usuarios privados para que no sea explotada con fines de lucro. Por lo tanto, las empresas deben seguir los reglamentos para cumplir con estas políticas. Uno de los enfoques es el uso del enmascaramiento de datos, que oculta la identidad dentro de los datos mediante métodos de cifrado.

¿QUÉ HACE QUE LA SEGURIDAD EN LA NUBE SEA DIFERENTE?

La seguridad informática tradicional ha experimentado una inmensa evolución debido al cambio a la informática basada en la nube. Si bien los modelos de la nube permiten una mayor comodidad, la conectividad siempre activa requiere nuevas consideraciones para mantenerlas seguras. La seguridad en la nube, como una solución de ciberseguridad modernizada, se distingue de los modelos informáticos heredados en algunos aspectos.

Almacenamiento de datos: la mayor distinción es que los modelos antiguos de TI dependían en gran medida del almacenamiento de datos in situ. Las empresas han descubierto desde hace mucho tiempo que la creación de todas las plataformas informáticas internas para los controles de seguridad detallados y personalizados es costosa y rígida. Las plataformas basadas en la nube han ayudado a transferir los costes de desarrollo y mantenimiento de los sistemas, pero también a eliminar cierto control de los usuarios.

Velocidad de escalada: de manera similar, la seguridad en la nube exige una atención única al escalar los sistemas de TI de la empresa. La infraestructura y las aplicaciones centradas en la nube son muy modulares y se movilizan rápidamente. Si bien esta capacidad mantiene los sistemas uniformemente ajustados a los cambios empresariales, también plantea problemas cuando la necesidad de mejoras y comodidad de una empresa supera su capacidad para mantenerse al día en materia de seguridad.

Interfaz del sistema de usuarios finales: tanto para las empresas como para los usuarios individuales, los sistemas de nubes también se conectan con muchos otros sistemas y servicios que se deben asegurar. Los permisos de acceso deben mantenerse desde el nivel de dispositivo de usuario final hasta el nivel de software e incluso el nivel de red. Además, tanto proveedores como usuarios deben estar atentos a las vulnerabilidades que pueden causar a través de comportamientos de configuración y acceso al sistema inseguros.

Proximidad a otros datos y sistemas en red: dado que los sistemas en la nube son una conexión persistente entre los proveedores de la nube y todos sus usuarios, esta importante red puede comprometer incluso al propio proveedor. En los entornos de redes, un solo dispositivo o componente débil se puede explotar para infectar al resto. Los proveedores de la nube se exponen a las amenazas de muchos usuarios finales con los que interactúan, bien sea que estén proporcionando almacenamiento de datos u otros servicios. Las responsabilidades adicionales en materia de seguridad de la red recaen en los proveedores cuyos productos entregados de otro modo se basarían exclusivamente en los sistemas de los usuarios finales y no en los propios.

SEGURIDAD EN LA NUBE

El cumplimiento legal gira en torno a la protección de la privacidad del usuario, tal como lo establecen los órganos legislativos. Los gobiernos asumieron la importancia de proteger la información de los usuarios privados para que no sea explotada con fines de lucro. Por lo tanto, las empresas deben seguir los reglamentos para cumplir con estas políticas. Uno de los enfoques es el uso del enmascaramiento de datos, que oculta la identidad dentro de los datos mediante métodos de cifrado.

¿QUÉ HACE QUE LA SEGURIDAD EN LA NUBE SEA DIFERENTE?

La seguridad informática tradicional ha experimentado una inmensa evolución debido al cambio a la informática basada en la nube. Si bien los modelos de la nube permiten una mayor comodidad, la conectividad siempre activa requiere nuevas consideraciones para mantenerlas seguras. La seguridad en la nube, como una solución de ciberseguridad modernizada, se distingue de los modelos informáticos heredados en algunos aspectos.

Almacenamiento de datos: la mayor distinción es que los modelos antiguos de TI dependían en gran medida del almacenamiento de datos in situ. Las empresas han descubierto desde hace mucho tiempo que la creación de todas las plataformas informáticas internas para los controles de seguridad detallados y personalizados es costosa y rígida. Las plataformas basadas en la nube han ayudado a transferir los costes de desarrollo y mantenimiento de los sistemas, pero también a eliminar cierto control de los usuarios.

Velocidad de escalada: de manera similar, la seguridad en la nube exige una atención única al escalar los sistemas de TI de la empresa. La infraestructura y las aplicaciones centradas en la nube son muy modulares y se movilizan rápidamente. Si bien esta capacidad mantiene los sistemas uniformemente ajustados a los cambios empresariales, también plantea problemas cuando la necesidad de mejoras y comodidad de una empresa supera su capacidad para mantenerse al día en materia de seguridad.

Interfaz del sistema de usuarios finales: tanto para las empresas como para los usuarios individuales, los sistemas de nubes también se conectan con muchos otros sistemas y servicios que se deben asegurar. Los permisos de acceso deben mantenerse desde el nivel de dispositivo de usuario final hasta el nivel de software e incluso el nivel de red. Además, tanto proveedores como usuarios deben estar atentos a las vulnerabilidades que pueden causar a través de comportamientos de configuración y acceso al sistema inseguros.

Proximidad a otros datos y sistemas en red: dado que los sistemas en la nube son una conexión persistente entre los proveedores de la nube y todos sus usuarios, esta importante red puede comprometer incluso al propio proveedor. En los entornos de redes, un solo dispositivo o componente débil se puede explotar para infectar al resto. Los proveedores de la nube se exponen a las amenazas de muchos usuarios finales con los que interactúan, bien sea que estén proporcionando almacenamiento de datos u otros servicios. Las responsabilidades adicionales en materia de seguridad de la red recaen en los proveedores cuyos productos entregados de otro modo se basarían exclusivamente en los sistemas de los usuarios finales y no en los propios.

Resolver la mayoría de los problemas de seguridad en la nube significa que tanto los usuarios como los proveedores de la nube, tanto en entornos personales como en empresariales, deben ser proactivos en cuanto a sus propias funciones en la ciberseguridad. Este doble enfoque significa que los usuarios y los proveedores deben abordar lo siguiente:

- Configuración y mantenimiento seguros del sistema.
- Educación sobre seguridad del usuario, tanto a nivel de comportamiento como a nivel técnico.

Por último, los proveedores y los usuarios de la nube deben tener transparencia y responsabilidad para garantizar que ambas partes estén seguras.

RIESGOS DE SEGURIDAD EN LA NUBE

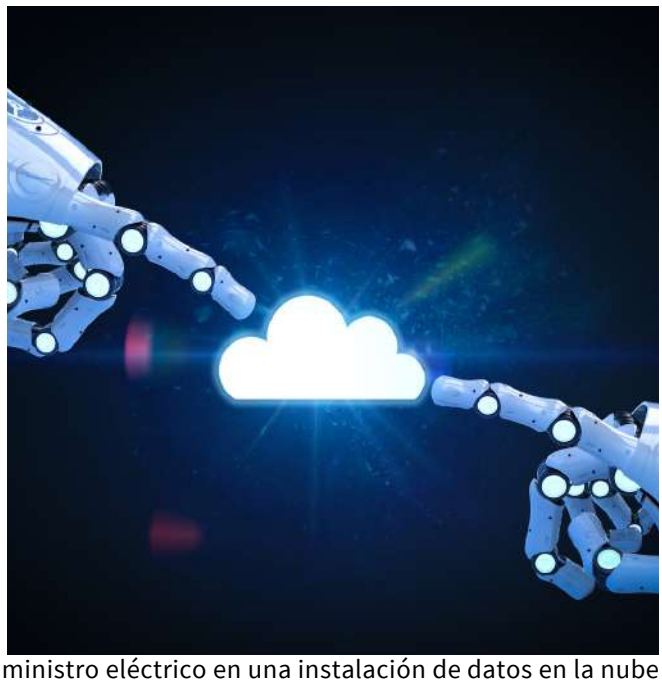
¿Cuáles son los problemas de seguridad en la informática en la nube? Si no es consciente de su existencia ¿cómo se supone que va a tomar las medidas adecuadas? Después de todo, una seguridad débil en la nube puede exponer a los usuarios y proveedores a todo tipo de amenazas de ciberseguridad. Algunas amenazas comunes a la seguridad en la nube incluyen:

- Riesgos de la infraestructura basada en la nube, incluidas las plataformas informáticas heredadas incompatibles y las interrupciones de los servicios de almacenamiento de datos de terceros.
- Amenazas internas debidas a errores humanos como, por ejemplo, la mala configuración de los controles de acceso de los usuarios.
- Amenazas externas causadas casi exclusivamente por actores maliciosos, como malware, phishing y ataques de DDoS.

SEGURIDAD EN LA NUBE

El mayor riesgo que plantea la nube es que no existe un perímetro. La ciberseguridad tradicional se centraba en proteger el perímetro, pero los entornos en la nube están altamente conectados, lo que conlleva que las interfaces de programación de aplicaciones (API) sean inseguras y los secuestros de cuentas puedan plantear problemas reales. Frente a los riesgos para la seguridad que afectan a la computación en la nube, los profesionales de la ciberseguridad deben adoptar un planteamiento más centrado en los datos.

La interconexión también plantea problemas para las redes. Los actores maliciosos a menudo acceden las redes debido a credenciales comprometidas o débiles. Una vez que un hacker consigue acceder a una red, puede propagarse fácilmente y utilizar las interfaces mal protegidas de la nube para localizar datos en diferentes bases de datos y nodos. Incluso puede utilizar sus propios servidores en la nube como destino donde exportar y almacenar los datos robados. La seguridad tiene que estar en la nube y no servir como elemento exclusivo para proteger frente al acceso a los datos que allí se almacenan.



El almacenamiento de los datos por parte de terceros y el acceso a través de Internet también plantean sus propias amenazas. Si, por algún motivo, estos servicios se interrumpen, podría perderse el acceso a los datos. Por ejemplo, un corte en la red telefónica podría significar que no se puede acceder a la nube en un momento esencial. Alternativamente, un corte de energía podría afectar al centro de datos donde se almacenan los datos, lo que podría conllevar una pérdida de datos permanente.

Dicho tipo de interrupciones podrían tener repercusiones a más largo plazo. Un reciente corte del suministro eléctrico en una instalación de datos en la nube de Amazon resultó en la pérdida de los datos de algunos clientes debido a los desperfectos que se ocasionaron en el hardware de los servidores. Este es un buen ejemplo de por qué conviene tener copias de seguridad locales de al menos algunos de sus datos y aplicaciones.

SEGURIDAD EN LA NUBE

¿POR QUÉ ES IMPORTANTE LA SEGURIDAD EN LA NUBE?

En la década de 1990, los datos comerciales y personales se almacenaban y gestionaban a nivel local, y la seguridad también era local. Los datos se encontraban en el almacenamiento interno de un PC en casa, y en los servidores de la empresa, si trabajaba para una empresa.

La introducción de la tecnología de la nube ha obligado a todos a reevaluar la ciberseguridad. Los datos y aplicaciones pueden estar flotando entre sistemas locales y remotos, y estar siempre accesibles por Internet. Si accede a Google Docs desde el teléfono móvil o si utiliza el software Salesforce para gestionar a sus clientes, esos datos pueden guardarse en cualquier parte. De ahí que protegerlos sea más difícil que cuando solo se trataba de impedir que usuarios no deseados accedieran a su red. La seguridad en la nube requiere ajustar algunas prácticas informáticas previas, pero se ha vuelto más esencial por dos razones clave:

1. Comodidad por encima de la seguridad. La informática en la nube está creciendo de forma exponencial como método principal tanto para el lugar de trabajo como para el uso individual. La innovación ha permitido que la nueva tecnología se implemente más rápido de lo que avanzan las normas de seguridad de la industria, lo que hace que los usuarios y los proveedores tengan más responsabilidad a la hora de considerar los riesgos de la accesibilidad.
2. Centralización y almacenamiento para múltiples usuarios. Cada componente, desde la infraestructura básica hasta pequeños datos como correos electrónicos y documentos, puede ahora localizarse y accederse de forma remota e ininterrumpida a través de conexiones basadas en la web. Toda esta recopilación de datos en los servidores de unos pocos proveedores de servicios importantes puede ser muy peligrosa. Los actores de amenazas pueden atacar ahora a grandes centros de datos de varias empresas y causar importantísimas filtraciones de datos.

Lamentablemente, los actores maliciosos se dan cuenta del valor de los objetivos basados en la nube y los investigan cada vez más para encontrar sus vulnerabilidades de seguridad. A pesar de que los proveedores de la nube asumen muchas funciones de seguridad de los clientes, no lo gestionan todo. Esto deja incluso a los usuarios no técnicos con el deber de auto educarse sobre la seguridad en la nube.

Dicho esto, los usuarios no están solos en lo que respecta a las responsabilidades de seguridad en la nube. Ser consciente del alcance de sus deberes de seguridad ayudará a que todo el sistema esté mucho más seguro.

REFERENCIAS

REFERENCIAS

- https://www.eleconomista.com.mx/tecnologia/Hackers-chinos-usaron-fallo-en-codigo-para-robar-correos-electronicos-de-agencias-de-EU-Microsoft-20230714-0067.html
- https://www.eleconomista.com.mx/sectorfinanciero/IA-podria-vulnerar-la-seguridad-de-usuarios-en-pagos-y-criptomonedas-20230704-0094.html
- https://www.cshub.com/attacks/news/roblox-developer-data-leak
- https://elpais.com/tecnologia/2023-07-25/varios-periodicos-espanoles-sufren-problemas-por-ataques-informaticos.html
- https://elpais.com/tecnologia/2023-07-25/varios-periodicos-espanoles-sufren-problemas-por-ataques-informaticos.html
- https://www.ventasdeseguridad.com/2023072523481/noticias/empresas/mexico-el-mas-afectado-por-ciberataques-en-2023.html
- https://www.kaspersky.es/resource-center/definitions/what-is-cloud-security

ZERU

Cybersecurity Services

Security Operation Center - SOC by

ADV

+52 55 6178 9397

contacto@adv-ic.com

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