CYBERSECURITY
by itwarelatam.com

Edición - Nº 10

La revista de Cloud Security

NOTA DE TAPA

Blockchain y ciberseguridad: una unión indivisible

INFORME ESPECIAL

¿Cómo funciona la ciberseguridad en la Nube?

MÁS TEMAS

Ventajas y desventajas de la autenticación biométrica

Una nueva póliza de Seguros: Riesgos de ciberseguridad

Cómo aumentar la seguridad en las bases de datos

CYBERARK®

PROTEJA LA IDENTIDAD EN LA NUBE

El 75 % de las empresas han sufrido un incidente o ataque de ciberseguridad en la nube* pues el perímetro ha migrado de la red a la identidad

Implemente el principio de menor privilegio gestione permisos y mejore la visibilidad agnóstica en ambientes de nube, sin interrupción al negocio

¡OBTENGA UNA PRUEBA GRATUITA Y CONOZCA MÁS!

cyberark.com/es/try-buy/cloud-entitlements-manager/

*FUENTE: 3 ESG Trends in Identity and Access Management: Libro electrónico «Cloud-driven Identities» de ESG, septiembre de 2020

EDICIÓN N°10

NOTA DE TAPA

BLOCKCHAIN Y CIBERSEGURIDAD: UNA UNIÓN INDIVISIBLE

06

SUMARIO

Blockchain no son sólo criptomonedas

Bienvenidxs a un nuevo número de Cybersecurity. Aunque no es posible agotarlo en pocas páginas, Ciberseguridad en Blockchain es un tema que se está haciendo rápidamente popular, a medida en que se van descubriendo nuevos usos, virtudes e inconvenientes en la tecnología de cadena de bloques. Y a eso es a lo que dedicamos nuestro tema de tapa.

El Informe especial está consagrado a la Ciberseguridad en la Nube. Con la cantidad de empresas que están migrando sus procesos a la nube, así como se aprovechan las ventajas de esta tecnología, también trae consigo diversos retos de seguridad que pueden afectar a toda la organización. De ahí que muchas empresas estén adoptando un enfoque híbrido de la infraestructura de TI.

Entre otras notas de esta revista, destacamos el nuevo estándar de ciberseguridad para criptomonedas, ventajas y desventajas de la autenticación biométrica; complementando el número anterior, hablamos de predicciones para el futuro de la gestión de identidades y accesos y, además, vemos que están apareciendo pólizas de seguro dedicadas a los riesgos de la seguridad informática. Y algo de tecnología con la seguridad en las bases de datos.

Aunque la pandemia no se ha ido del todo, los controles se han relajado, han vuelto las reuniones presenciales y, sobre todo, se está produciendo el retorno a las oficinas, con todo lo que eso implica. Algo que, seguramente, trataremos en futuros números.

Hasta la próxima.

Matías Perazzo
Director Editorial
mperazzo@mediaware.org

Ricardo Goldberger
Contenidos
rgoldberger@mediaware.org

Suscripciones:
info@itwarelatam.com

Para publicar en este medio:
ventas@mediaware.org
www.itwarelatam.com

Consultar por suscripción anual

Puede leer y descargar la versión digital de esta revista en www.itwarelatam.com.com

Edita, diseña, comercializa y distribuye Mediaware Marketing

itseller enfasys ITWARE LATAM.COM

mediaware MARKETING

Buenos Aires - Av. Jujuy 2073, 2°B, Distrito Tecnológico, Buenos Aires, Argentina
Tel.: +5411-4308-6642

Defenderse contra las amenazas actuales requiere la vigilancia constante de analistas calificados.

FALCON COMPLETE EN ACCIÓN

AUMENTE SU EQUIPO CON LA EXPERIENCIA MÁS PROFUNDA

La ciberseguridad no es solo un problema tecnológico, también requiere experiencia las 24 horas del día.

Falcon Complete le brinda experiencia enfocada para detener amenazas a través de una vigilancia continua.

PROTECCIÓN 24/7/365

ERRADICAR LAS AMENAZAS EN MINUTOS

Los adversarios suelen infligir daños en horas, pero las organizaciones pueden tardar días en responder.

Falcon Complete elimina quirúrgicamente las amenazas en minutos.

DETECTAR: <1 min
INVESTIGAR: <10 min
RESPONDER: <60 min

ELIMINE RIESGOS Y LIBERE ENORMES AHORROS

Defenderse de las amenazas actuales es un desafío continuo. Los equipos de seguridad siempre deben preguntarse: "¿Estoy haciendo lo suficiente?"

Falcon Complete ofrece resultados predecibles a una fracción del costo.

100% CONFIANZA
403% ROI

CrowdStrike® Falcon Complete TM es un servicio de detección y respuesta administradas (MDR) que ofrece **investigación especializada y respuesta quirúrgica 24x7x365.**

BLOCKCHAIN Y CIBERSEGURIDAD: UNA UNIÓN INDIVISIBLE

Por Ricardo Goldberger

Blockchain puede definirse como una estructura matemática para almacenar datos que es casi imposible de falsificar. Es un libro de contabilidad electrónico público que puede ser compartido por diferentes usuarios y crea un registro inmutable de sus transacciones.

Cada registro digital del hilo se denomina bloque (de ahí su nombre) y permite a un grupo abierto o controlado de usuarios participar en el libro electrónico. Cada bloque está a su vez vinculado a un participante concreto. La cadena de bloques sólo puede actualizarse por consenso entre los participantes en el sistema, y cuando se introducen nuevos datos, éstos nunca pueden borrarse. Cada entrada en el sistema se registra de forma veraz y verificable.

Como la información digital puede distribuirse, pero no copiarse, la tecnología blockchain es la columna vertebral de un nuevo tipo de Internet. Desarrollado originalmente para la moneda digital Bitcoin, la comunidad tecnológica está encontrando ahora otros usos.

Según la Cámara de Valencia, "no se puede definir blockchain sin hablar de seguridad. Uno de los mayores beneficios que aporta es su red ultrasegura. Debido a que los datos transmitidos están intrínsecamente encriptados, es mucho más seguro que el sistema de contraseña y nombre de usuario estándar.

"Los datos descentralizados almacenados usando blockchain hacen que sea extremadamente difícil hackearlos porque no existe un "único punto de falla". ¿Qué significa esto? Si todos los documentos se guardan en miles de discos duros diferentes, es poco probable que alguna vez se pierdan datos.

"En circunstancias normales, para entrar en una cadena de bloques, los hackers tendrían que abrumar a más del 50% de la red en menos tiempo de lo que lleva crear un nuevo bloque. La cantidad de potencia de cálculo requerida para hacer esto en la mayoría de las redes de blockchain es tremenda. Las más grandes son mucho más difíciles de hackear porque están más descentralizadas y tienen más ordenadores trabajando para verificar las transacciones.

"Además, es fácil detectar cuándo un bloque ha sido manipulado gracias a las funciones hash. Estos valores de un bloque se agregan a los datos en el siguiente. Cualquiera que intente alterar uno terminará cambiando el hash por completo, activando una bandera roja y deshabilitando el bloqueo por completo."

Una afirmación tan terminante debía ser confirmada. Por eso consultamos a varios especialistas en blockchain y ciberseguridad para ver qué hay de cierto en todo esto.

> **Como la información digital puede distribuirse, pero no copiarse, la tecnología blockchain es la columna vertebral de un nuevo tipo de Internet.**

Qué tan segura es la Blockchain

Arturo Busleiman, Coordinador de Ciberseguridad del Ministerio de Relaciones Exteriores, Comercio Internacional y Culto es tajante: "Tan seguro como cualquier cosa. Recordemos que la seguridad se construye en capas, y

Arturo Busieiman

no se puede garantizar. De hecho, ya existen ataques contra blockchain como, por ejemplo, el ataque del "51%", que lo podemos comparar con controlar el 51% o más de una empresa."
Pero seamos un poco más amplios en la explicación.

Claudio Avín, ACS Services Sales Representative de Oracle, amplía: "Blockchain es una tecnología que permite la transferencia de datos digitales con una codificación sofisticada y muy segura, permitiendo garantizar la integridad de los datos, así como su trazabilidad. Es, en síntesis, una cadena de confianza que descentraliza la validación de la información, haciendo que hackear dichos datos sea mucho más difícil que teniéndolos concentrados todos en un único servidor. De hecho, de acuerdo a una investigación desarrollada por Oracle y Enterprise Strategy Group (ESG), en la que se encuestaron a 700 profesionales del área de finanzas en todo el mundo, el 78% considera que Blockchain reducirá el fraude al menos a la mitad en los próximos 5 años."

Javier Ailbirt, CEO de TheEye relativiza: "Depende de la red a la que nos referimos, existen muchas redes o blockchains. Lo importante es entender el algoritmo de consenso y la cantidad de nodos. Entre mejor algoritmo y mayor cantidad de nodos, más segura es la red. Un nodo es una computadora conectada a otras, y éstas hacen a la red descentralizada. Cada nodo tiene una copia de toda la base de datos. El algoritmo de consenso sirve para prevenir que una persona simule virtualmente ser muchas, debido a que para escribir información es necesario que el consenso sea de más del 51% de los nodos, y así evitar el doble gasto. Existen varios algoritmos de consenso, el más conocido es el Proof of Work (Prueba de Trabajo), utilizada por ejemplo en la red blockchain de Bitcoin y que se basa en resolver algoritmos criptográficos para el cual es necesario potencia de cómputo. "

Claudio Avín

Javier Ailbirt

Maximiliano Hinz, Latam Operations Director de Binance agrega que "Blockchain es una tecnología que permite la descentralización de nodos. En el caso de las blockchains más conocidas, que son las de Bitcoin y la de Ethereum, estamos ante un producto de una seguridad superlativa. Esto es gracias a la característica de que para que algo se modifique en la blockchain, tiene que estar de acuerdo más del 50% de los nodos, con lo que un hackeo eficiente solo sucedería si hay más de 50% de nodos afectados. Las blockchains de ETH y BTC son las más seguras porque son las que más nodos tienen, y esto aumenta su complejidad. Si desarrollamos una nueva cadena de bloques, pero sólo con 3 nodos, entonces, atacando 2 de estos 3 nodos ya podríamos hackearla."

Américo de Paula, Líder de Arquitectura de Soluciones para Latinoamérica en AWS, utiliza una analogía: "En Blockchain los ataques cibernéticos son casi imposibles. Tenemos que pensar en la seguridad online como pensamos en la seguridad física. Nadie le da las llaves de su casa a un extraño; por lo contrario, las guarda en un lugar seguro para evitar robos. De igual manera, los usuarios y las empresas tienen que usar claves seguras y respetar todas las normas básicas de ciberseguridad para evitar que otros puedan entrar a su cuenta de Blockchain y hacer transacciones bajo su nombre."

Maximiliano Braga, CEO de CyberSecurity Defense ofrece otro enfoque distinto: "Las cryptomonedas se basan bajo un principio el cual se define como disuasivo. Esto significa que el costo del ataque es superior al beneficio que podemos obtener. Como ejemplo podríamos tomar el siguiente: Supongamos que podemos explotar una vulnerabilidad que hace que me pueda apoderar de todas las Bitcoins del mundo. Automáticamente su valor se convertiría en cero y nadie las querría, por lo cual el costo del ataque comparado al beneficio es nulo."

Una afirmación tan terminante debía ser confirmada. Por eso consultamos a varios especialistas en blockchain y ciberseguridad para ver qué hay de cierto en todo esto.

Atacar o no atacar

Uno de los principios generales de la ciberseguridad es que cuanto más popular se haga una aplicación o una tecnología, más susceptible será de ser atacada, ya que hay más posibilidades de afectar a mayor cantidad de gente, de usuarios y/o más empresas o más grandes.

Lo primero que habría que determinar es el grado de adopción de Blockchain. Avín nos acerca alguna información: "La confianza, la transparencia, la dependencia reducida de los intermediarios y la automatización hacen que el Blockchain sea atractivo para las empresas. Hoy, tanto el Blockchain como la Inteligencia Artificial, el Internet de las Cosas o los Chatbots ya son "mainstream" con el 84% de las organizaciones utilizando al menos una de estas cuatro nuevas tecnologías, según la investigación de Oracle y ESG (https://www.oracle.com/ar/scm/). La Encuesta Global Blockchain 2020 de Deloitte sugiere que las dudas iniciales sobre la utilidad de blockchain se están desvaneciendo, ya que los líderes empresariales ahora lo ven como parte integral de la innovación organizacional. Como resultado, están

Maximiliano Braga

Américo de Paula

invirtiendo dinero y recursos detrás de la tecnología de formas más significativas y tangibles."

De Paula añade: "Blockchain es una tecnología con popularidad creciente en una amplia variedad de industrias, especialmente banca y manufactura. De acuerdo con datos de IDC, en 2020 el gasto en soluciones de Blockchain fue un 50% más que en 2019. Esta tendencia seguirá creciendo a un ritmo sólido durante los próximos años, alcanzando una inversión global total de casi $17.9 mil millones de dólares para 2024."

"Las finanzas descentralizadas y las monedas/tokens basados en blockchain ya son accesibles tan fácilmente como usar m***pago —sostiene Busleiman—. Pero no confundamos un blockchain con una criptomoneda, como dirían en el Blockchain Federal Argentino, que recomiendo investigar. E incluso, si no fuese popular, la ventaja primaria de una entidad atacante (sea un individuo, un grupo bancado por una nación-estado, crimen organizado u otros) siempre se relacionará con ser los primeros en haber investigado una tecnología, así como la implementación de ataques a la misma."

> **"La confianza, la transparencia, la dependencia reducida de los intermediarios y la automatización hacen que el Blockchain sea atractivo para las empresas."**

Para Hinz, "sin duda, hay ataques constantes a cualquier tipo de infraestructura y la blockchain no es ajena a esto. Tengamos en cuenta que la recompensa por un hackeo bien hecho es conseguir Bitcoins que tienen un valor líquido inmediato. Por suerte, no se han reportado hackeos exitosos a la blockchain en la historia de Bitcoin."

Como bien dice Busleiman, es menester aclarar que una cosa es atacar la tecnología Blockchain y otra, muy distinta, es atacar a las billeteras virtuales. Algo que refrenda Pontiroli: "Según la Federación Latinoamericana de Bancos, Felaban: 'El uso de billeteras digitales en Latinoamérica incrementó en 180% en 2020, por ser una solución sumamente práctica para reemplazar el uso de efectivo'. Sin embargo, el uso de criptomonedas en la región no es tan fácil de cuantificar debido a los intercambios directos entre individuos o P2P. En 2020, los sistemas de detección de Kaspersky descubrieron un promedio de 360.000 nuevos archivos maliciosos por día, 18.000 más que el año anterior (un aumento del 5,2%) y más que los 346.000 en 2018. Esto se vio influenciado principalmente por un gran crecimiento en la cifra de troyanos, así como de puertas traseras: un aumento del 40,5% y 23%, respectivamente. Las principales amenazas para los tenedores de criptomonedas y tokens son los 'information stealers' o ladrones de información, que pueden capturar credenciales, frases semilla, o inclusive el archivo de la billetera directamente."

Maximiliano Hinz

A la hora de proteger

Continúa Pontiroli: “Por un lado, como usuarios finales, la seguridad de nuestras monedas o tokens puede asegurarse a través del uso de una billetera hardware, contraseñas robustas y segundo factor de autenticación. Por otro lado, la seguridad de la cadena de bloques depende del grupo de desarrollo que tiene la responsabilidad de auditar y controlar las amenazas para garantizar una red libre de manipulación, y en donde los participantes son parte activa de la seguridad a través de tareas como la minería de bloques.”

Avín alerta: “Las vulnerabilidades por lo general se encuentran en las aplicaciones clientes, por lo que se debe tener especial cuidado en su desarrollo seguro, utilizando factores de autenticación fuertes, como la biometría o doble factor de autenticación.”

Braga explica: “La persona que posee las claves privadas es la que decide cómo se gastan los activos criptográficos asociados; si no es el propietario de esto, está confiando su criptografía a un tercero. Si posee sus llaves, tiene control total sobre cómo usar sus fondos. La realidad es que uno como usuario no puede saber cuáles son los métodos de protección en materia de ciberseguridad utilizados por la aplicación, qué pasa en el backend, etc. Siempre es bueno estudiar la reputación de la misma y ver qué medidas mínimas de seguridad nos propone para iniciar sesión, transac-

Santiago Pontiroli

cionar, métodos de autenticación, etc. Otra buena práctica sería ver con qué certificaciones de seguridad cuenta la organización de tipo ISO, IEC, SOC, etc.”

En Blockchain —afirma de Paula—, cada transacción tiene un código propio. Usando la metáfora de la casa, podemos decir que en Blockchain las llaves no son accesibles para los atacantes y, por lo tanto, las aplicaciones ya están muy bien protegidas. Sin embargo, los usuarios tienen que respetar las mismas normas de seguridad que utilizan en otros casos: crear claves fuertes, no compartirlas con nadie y usar autenticación de factor múltiple, entre otras.”

Ailbirt precisa que “a diferencia de un sistema tradicional, La ventaja es que la información que ha sido grabada en la blockchain no se podrá modificar, con lo cual si un smart contract se ha desarrollado de manera correcta, no deberíamos preocuparnos por su seguridad. Además, si usamos la blockchain para registrar información, nunca podrán modificarla y fácilmente podremos recuperarla. En cambio, si atacan una base de datos tradicional, es muy probable que perdamos toda o gran parte de la información. “

> **“Los usuarios tienen que respetar las mismas normas de seguridad que utilizan en otros casos: crear claves fuertes, no compartirlas con nadie y usar autenticación de factor múltiple, entre otras.”**

Como siempre, Busleiman es tajante: “Si estamos hablando de aplicaciones descentralizadas basadas en contratos inteligentes, como aquellas en Ethereum programadas en Solidity, la vulnerabilidad es tanta como programadores hay en el mundo. Ya existen empresas y herramientas para realizar análisis de dichas “DApps” (Distributed Apps). Es una industria. ¿Prevenir? Como siempre: aprendiendo a programar EN FORMA SEGURA, y no intentar reinventar la rueda: usar patrones conocidos, bien evaluados.”

Para qué sirve, además

…

Además del boom de las criptomonedas, se vio que la tecnología Blockchain sirve para otras cosas como, por ejemplo, contratos inteligentes, logística o, como describe de Paula: “es una tecnología que permite crear aplicaciones en las que múltiples partes pueden registrar transacciones sin necesidad de que haya una autoridad central confiable que garantice que las transacciones estén verificadas y sean seguras. Blockchain permite esto mediante el establecimiento de una red peer-to-peer donde cada participante en la red tiene acceso a un libro de contabilidad compartido donde se registran las transacciones. Estas transacciones son por diseño, inmutables y verificables de forma independiente.” La blockchain es un libro de información descentralizado, por lo que su aplicabilidad es infinita. Pero, advierte Hinz, “la única limitación es el costo por utilizarla, donde a veces no es rentable pagar el costo operativo para escribir un bloque. Se pueden realizar controles de trazabilidad, manejo de stocks sensibles, incluso emitir certificados digitales. Un ejemplo de lo versátil que es la blockchain son los NFT’s, obras de arte con certificados de originalidad montados en blockchain”.

Ailbirt puntualiza: “Existen cientos de aplicaciones prácticas, recordemos que un blockchain es una base de datos descentralizada e inmodificable. En la actualidad hay Universidades que la

Crédito: www.freepik.com

utilizan para poder verificar la legitimidad de títulos, muchas empresas lo utilizan para guardar información crítica (como el estado de stock, resultados de balance, etc.) y para validar que cierta información existía en determinada fecha (timestamp), también existen casos en el sistema de salud para que el dueño del historial clínico sea el paciente y decida qué información, por cuanto tiempo y a quién se la comparte.”

“Algunos usos que puede tener la tecnología Blockchain —desgrana Avín— son los contratos inteligentes, que puede aplicarse tanto a contratos gubernamentales como de seguros de automóviles y hasta las hipotecas. En un proceso estándar en papel los contratos requieren la firma de varias partes a medida que avanzan. Esto puede ralentizar el proceso y presentar problemas como costos de envío, riesgos de seguridad debido a copias o impresiones y problemas de programación. Los contratos inteligentes eliminan todos estos problemas al ser precisos, transparentes, permanentes y convenientes. Por ejemplo, debido a que blockchain crea un registro ordenado permanente de cada transacción, los contratos inteligentes garantizan que las firmas se recopilen en el orden adecuado necesario para ejecutar el acuerdo. Además, blockchain representa la única fuente del documento por lo que nunca hay confusión sobre su estado.”

A lo que dice Ailbirt, Avín agrega: “También, el Blockchain es utilizado en salud. Para la atención médica en particular, los beneficios inherentes de permanencia, precisión y accesibilidad de esta tecnología la convierten en una opción muy práctica para impulsar un mundo de registros digitales y dispositivos conectados. Desde registros

médicos individuales más rápidos y fáciles, hasta decisiones de personal hospitalario basadas en datos, la industria de la salud tiene muchos casos de uso valiosos para el Blockchain y, en muchos casos, opciones prácticas de Blockchain empresariales existentes para hacerla realidad."

Pontiroli abre el panorama: "Existen infinidad de usos para la cadena de bloques, siendo las criptomonedas el más evidente y popular hoy día. Sin embargo, proyectos relacionados a una Internet descentralizada y libre de censura, resolución de dominios, almacenamiento de archivos, sistemas de votación o consenso, certificación de documentos, mensajería segura, e inclusive almacenar nuestro ADN, son todas opciones e investigaciones en curso para aprovechar todo el potencial que tiene blockchain."

Otras alternativas serían:

Industria Farmacéutica: Las nuevas reglas para garantizar la integridad de los medicamentos desde la fabricación hasta el consumo podrían salvar hasta un millón de vidas cada año. Las ciencias de la vida y las compañías de atención médica crean números de serie únicos para las unidades de medicamentos y equipos, que se escanean, capturan y verifican en su punto de origen, según Scott Allison, presidente de atención médica en el gigante de logística DHL. Aplicado de la manera correcta, Blockchain puede llevar la serialización de seguimiento y rastreo a un siguiente nivel, reduciendo costos, elevando la seguridad y la confianza, eliminando los movimientos de datos propensos a errores y permitiendo la transparencia de la cadena de suministro en tiempo real.

"Proyectos relacionados a una Internet descentralizada y libre de censura, resolución de dominios, almacenamiento de archivos, sistemas de votación o consenso, certificación de documentos, mensajería segura, e inclusive almacenar nuestro ADN, son todas opciones e investigaciones en curso"

Seguridad alimentaria. IBM se está asociando con proveedores de alimentos, incluidos Dole, Nestlé y Walmart, para regular mejor la seguridad alimentaria utilizando Blockchain. En la industria de la cadena global de suministro de alimentos, esto significa que todos los productores, proveedores, procesadores, distribuidores, minoristas, reguladores y consumidores pueden obtener acceso autorizado a información sobre el origen y el estado de los alimentos en sus transacciones. Todos los miembros del ecosistema pueden usar la red de Blockchain para rastrear los alimentos contaminados hasta su fuente en un corto período de tiempo, para asegurar que sean retirados rápidamente de los estantes de las tiendas.

Crisis humanitarias. Las Naciones Unidas (ONU) están explorando cómo se puede utilizar Blockchain interna y externamente para abordar cuestiones humanitarias actuales, como el tráfico de niños, según Mahrinah von Schlegel, directora ejecutiva de la organización sin fines de lucro Embassy 2.0. La ONU utiliza actualmente Blockchain en 16 agencias, incluido el Programa Mundial de Alimentos (para ayudar a los refugiados a comprar alimentos) y la Oficina de Coordinación de Asuntos Humanitarios (para mejorar el financiamiento de los donantes, asegurar y monitorear las cadenas de suministro y datos protección).
Como sintetiza Busleiman: "Cualquier cosa que valga la pena ser almacenado y procesado: trámites, documentos, contratos, asistencia social, cuestiones electorales, escribanía, etc."

En suma, hay Blockchain para rato y, seguramente, cada vez se le encontrarán más usos.

El Futuro de Blockchain: predicciones para 2030

Por Toshendra Kumar Sharma - blockchain-council.org

Desde hace más de una década, las criptomonedas y la tecnología blockchain han tomado el mundo por asalto. Algunos afirman que esto es sólo el principio. Con la rápida adopción de blockchain por parte de numerosas empresas de diversos sectores, es evidente que el blockchain se está transformando en un movimiento y avanza con paso firme hacia la siguiente fase de la revolución. La cadena de bloques se está convirtiendo en un fenómeno inevitable debido a las tecnologías básicas y a las importantes oportunidades que ofrece a las empresas digitales.

Predicciones de Blockchain para 2030

1. Blockchain se aprovechará para la mayoría del comercio mundial

La cadena de suministro mundial es uno de esos ámbitos prometedores en los que blockchain puede aportar un importante valor empresarial. Actualmente, hay muchas ineficiencias, fraudes y errores en el comercio mundial, ya que se lleva a cabo a través de un conjunto caótico de relaciones comerciales entre partes que no son de confianza. Una lista de los problemas de la cadena de suministro en el mundo real que deben ser resueltos son:

- Falsificación de autopartes.
- Medicamentos falsificados.
- Adulteración en la cadena de suministro de alimentos.
- Ropa de moda falsa y artículos de lujo.
- Falsificación de equipos electrónicos, incluidos los dispositivos médicos.

Estos problemas de la cadena de suministros son una amenaza para la vida. Esto se debe principalmente a que los ecosistemas empresariales están fragmentados, sólo parcialmente automatizados, y carecen de una autoridad central de confianza que certifique la autenticidad y rastree la procedencia. La cadena de bloques es una de esas tecnologías que traerá consigo la lucha contra la disrupción: pondrá orden y actuará como una fuerza de unificación. Blockchain desempeñará un papel fundamental en la mejora del rendimiento, la flexibilidad, la eficiencia y la madurez.

2. Flujos sin fricción y activos digitales

En 2030 habrá más tokens de un billón de dólares que empresas de un billón de dólares. Actualmente, hay una carrera entre las cuatro empresas mundiales más valoradas, que son Google, Apple, Microsoft y Amazon. Éstas alcanzan un valor de un billón de dólares. Blockchain tendrá un impacto positivo en los negocios digitales, y también aumentará el valor en los mercados de valores. Blockchain reduce drásticamente el costo de las transacciones y los flujos de información. Favorece los flujos sin fricción de tokens y otros activos. En la futura era blockchain, los tokens de un billón de dólares desempeñarán un papel importante. Se trata de tokens que apoyan un ecosistema descentralizado de entidades.

3. Identidad Blockchain para todos

En 2030, o incluso antes, todos los individuos y sus activos virtuales o físicos tendrán identidades blockchain. Blockchain ayudará a mejorar los sistemas aportando muchas soluciones de identidad. Dado que los sistemas de identidad actuales son disfuncionales e inseguros, la tecnología blockchain actuará como fuente única de verificación tanto para los individuos como para los activos. Esto ayudará a:

- Aumentar la privacidad y la eficiencia.
- Descentralizar y verificar los datos recogidos.
- Almacenar la información en un solo libro de contabilidad.
- Reducir el riesgo de violaciones de la seguridad.
- Crear una nueva plataforma de identidad distribuida y no controlada por una autoridad central. Esto aumenta la transparencia.

Algunos casos de uso de blockchain en el ámbito de la identidad son los registros de empleo, los registros de identificación fiscal, los registros gubernamentales, los certificados y registros sanitarios y las puntuaciones de reputación.

4. Mejoras considerables en el nivel de vida global

Hoy en día, la pobreza y la diferencia de ingresos son los problemas más duros a los que se enfrenta la humanidad. Más del 10% de la población mundial total, que asciende a más de 750 millones de personas, vive su vida con menos de 2 dólares al día. Más de 2.000 millones de personas no tienen acceso a los servicios financieros y se consideran no bancarizadas. Blockchain tiene el potencial de reducir considerablemente la brecha de la pobreza. Esto se consigue de tres maneras, que son:

a) Reducción de la corrupción - Blockchain crea transparencia en los registros oficiales. Los detalles de todos los activos, incluidos los terrenos, se registrarán en un libro de contabilidad digital inmutable (a prueba de manipulaciones), transparente y seguro, que estará completamente abierto al público. La incertidumbre asociada a cualquier activo reduce su potencial de trazabilidad y su precio. La creación de un sistema distribuido de seguimiento de activos ayudará a aumentar la riqueza mundial. Resolver este problema tendrá importantes implicaciones financieras positivas en la economía mundial.

b) Inclusión financiera - Este es un beneficio obvio de las criptodivisas como el Bitcoin. Las criptodivisas y el blockchain ayudan a la población no bancarizada a bancarizarse y, por lo tanto, a cobrar. Mediante el uso de la tecnología Blockchain, no hay necesidad de depender de una institución centralizada como un banco o el gobierno, para proporcionar el permiso para abrir una cuenta bancaria. Proporcionará un fácil acceso a una bolsa de criptomonedas en la que la gente puede comprar y vender utilizando sus teléfonos inteligentes. Dado que muchos comerciantes de todo el mundo ya aceptan las criptodivisas, éstas se convertirán en un estándar de facto en 2030, como el dólar estadounidense, que es ampliamente aceptado en la actualidad.

c) Tokenización de activos generadores de valor - La tokenización se refiere a demostrar la propiedad de activos reales mediante el uso de tokens digitales. Blockchain ayuda a la tokenización de activos a gran escala. Esto significa que incluso un agricultor de una zona rural puede convertirse en propietario fraccionario de un activo generador de ingresos, como un hotel o una mina de oro. Esto ayudará a abrir una base de inversores potenciales a un mercado más amplio, a reducir el tiempo de negociación y a aumentar la liquidez en comparación con los valores tradicionales.

Conclusión

Blockchain es una de esas potentes tecnologías que no se pueden ignorar, ya que está afectando a una amplia gama de empresas. Aunque el panorama de la cadena de bloques es confuso y cambia constantemente, la promesa es real. Ofrece capacidades que van desde las mejoras incrementales hasta las alteraciones radicales de los modelos de negocio que ayudan a las empresas a extraer valor empresarial para realizar las inversiones adecuadas en el momento oportuno.

Blockchain blanco de ataques

Por Patricio López - Instructor Blockchain Academy Chile y Arquitecto Blockchain

Un blockchain público, como Bitcoin o Ethereum, son tecnologías altamente seguras, debido a su alto grado de descentralización y al gasto que estas redes hacen en su propia seguridad para evitar fraudes y doble consumo de activos. Han existido redes blockchain que han sufrido vulneraciones mediante un ataque llamado 51%, como Ethereum Classic y Bitcoin Satoshi Vision. Por otro lado, la identificación de una persona para hacer una transacción se basa en criptografía que, hasta ahora, no ha podido ser vulnerada y es muy segura.

Los ataques

En general hay dos grandes tipos de ataques a las redes blockchain. Uno consiste en obtener acceso a llaves privadas de una cuenta que tenga privilegios sobre una aplicación, por ejemplo, para poder retirar fondos. Aparte de tener las máximas medidas de seguridad posible sobre las mismas, es aconsejable que cualquier operación sobre un contrato inteligente que tenga privilegios administrativos se haga mediante, o bien una billetera multifirma que necesite de varias llaves, o bien usando un mecanismo de ejecución diferida, de modo de poder reaccionar y evitar ataques antes de que el contrato ejecute las instrucciones.

El otro tiene que ver con explotar bugs o vulnerabilidades de un contrato inteligente.

Existen ataques con principios similares a los que caen en la tecnología web tradicional, tales como el phishing, la suplantación de identidad o los sim card attacks. Otros son específicos para la toma de control de llaves, tal como la venta de llaves seguras adulteradas, o el ataque de aplicaciones de almacenamiento de llaves.

Incluso han habido ataques tremendamente novedosos y originales sobre aplicaciones DeFi, basados en pedir gran cantidad de criptomonedas prestadas para incidir sobre el precio de un token y lograr, mediante una combinación de compras y ventas, obtener un gran beneficio económico. Varios discuten incluso si esto puede considerarse un ataque o es más bien un uso muy inteligente e inesperado de las reglas del juego.

Otros usos

Los usos de esta tecnología están por lo general asociado a los contratos inteligentes, que es programación de códigos auto-ejecutables. Esto se ha usado para casos de uso como trazabilidad, tokenización de activos, medios de pagos, bonos, garantías, seguros, entre muchos otros.

Por el lado más innovador, se han estado creando ecosistemas basados en la tecnología aplicada a la industria financiera llamada Finanzas Descentralizadas, cuyas aplicaciones buscan acercar nuevos productos y servicios financieros basados en la inclusión, transparencia e interoperabilidad. En esta misma línea, este año se ha dado a conocer el ecosistema de NFT o arte digital asociado a blockchain o coleccionables.

Patricio López

BLOCKCHAIN ACADEMY CHILE

Blockchain Academy Chile
https://www.blockchainacademy.cl
https://aula.blockchainacademy.cl
https://beacons.page/blockacademycl

> **Ataques específicos son la venta de llaves seguras adulteradas, o el ataque de aplicaciones de almacenamiento de llaves.**


¿Cómo funciona la ciberseguridad en la Nube?

Por Rocío Bravo

La seguridad de los servicios en la nube es un tema que cobra cada vez más relevancia por la cantidad de empresas que deciden migrar a servicios cloud. A pesar de las ventajas que esta tecnología implica, también trae consigo diversos retos de seguridad que pueden afectar a toda la organización. ¿Cómo afrontarlos? ¿Es posible pensar en un entorno cloud 100% seguro?

En la actualidad muchas empresas están adoptando un enfoque híbrido de la infraestructura de TI, ampliando su infraestructura local tradicional para incluir recursos en la nube, ya sean privados, públicos o multinube. Las ventajas de desplegar una infraestructura en la nube y ejecutar aplicaciones empresariales en la nube incluyen más flexibilidad empresarial, ahorro económico gracias a operaciones más eficientes y automatizadas y escalabilidad de pago por uso.

Sin embargo, el dinamismo y la interconexión de dispositivos que caracteriza al cloud computing también imponen nuevos retos para la seguridad de los datos, aplicaciones e infraestructuras de personas y empresas. Por esta razón, es necesario adoptar medidas de seguridad muy estrictas como la del cifrado de datos, el uso de contraseñas sólidas y la autenticación de doble factor, así como el uso exclusivo de interfaces de programación de aplicaciones (API) que sean seguras.

“La nube ha cumplido un rol clave en permitir la continuidad del trabajo en la respuesta a los desafíos planteados por la pandemia”, plantea Omar Alcalá, Director de Ingeniería para Tenable América Latina y el Caribe. Según el estudio “Más allá de los límites: El Futuro de la ciberseguridad en el nuevo mundo del trabajo”, comisionado por Tenable a Forrester, el 80% de las empresas trasladaron sus funciones críticas a la nube gracias a su capacidad de permitirnos servicios ubicuos disponibles en cualquier parte del mundo a un clic de distancia. “Es también por esto que ahora podemos tener atacantes del otro lado del mundo intentando acceder a nuestra información, servicios, usuarios y todo lo que tengamos en la nube. Ya si no ganan acceso, pueden también buscar negar los servicios, con los consecuentes impactos por indisponibilidad”.

Hugo Giampietri

La nube ha demostrado ser un gran aliado de las empresas a nivel operacional, hecho que se ha potenciado durante el último año, con la crisis desatada por la pandemia. Pero este recurso, además de proveer a las organizaciones de mayor agilidad en el Time to Market y de mayor capacidad de almacenamiento de datos e información, también se ha convertido en un agente esencial en torno a la protección y seguridad frente a las amenazas cibernéticas. De acuerdo con **Jesús Mauricio López,** Consultor de Cloud Solutions de TIVIT Colombia, "la primera industria en migrar completamente a lo digital fue la ciberdelincuencia. Es por esto por lo que las principales compañías proveedoras de nube como Amazon Web Services (AWS), Azure y Google Cloud, se han esforzado por desarrollar productos y servicios Cloud capaces de hacerle frente a estas amenazas, optimizando la seguridad digital de los ambientes de nube y mejorando su respuesta ante los diversos incidentes que pueden ocurrir".

Según datos de Fortinet, América Latina ha sido blanco de más de 7 mil millones de intentos de ciberataques tan solo en el primer trimestre de 2021. Comprendiendo ese escenario tan desafiante, en los últimos años, la estrategia de ciberseguridad en la nube se ha convertido en un requisito imprescindible para cualquier empresa, ya que, debido a la digitalización de los sistemas de almacenamiento y gestión de datos y archivos confidenciales, es fundamental desarrollar mecanismos de protección robustos y eficientes.

De acuerdo con **Hugo Giampietri,** Principal Corporate Account Manager en Citrix, en la actualidad, las plataformas de servicios en la nube son la preferencia digital para las compañías por la seguridad que la misma brinda para el resguardo de los datos y el beneficio que esto conlleva para el trabajo móvil, Sin embargo, aclara, esto no significa que el uso de la nube no pueda enfrentarse a algunas amenazas, según el servicio contratado y la estrategia. En este sentido, enumera las siguientes amenazas:

- **Violaciones de datos:** El robo de datos puede ser provocado por un ataque, error humano, vulnerabilidades de una aplicación o malas prácticas de seguridad. Este riesgo no es exclusivo de la nube, pero se clasifica constantemente como una de las principales preocupaciones de los clientes porque depende de la configuración correcta al acceso a los datos, sin dejar una puerta abierta para los cibercriminales.

- **Gestión de identidad y accesos deficientes:** Una mala gestión de identidad y claves de acceso puede generar que un atacante acceda a las infraestructuras con resultados desastrosos. Estos delincuentes informáticos pueden hacerse pasar por usuarios legítimos para modificar, eliminar datos, robar información o inyectar códigos maliciosos.

- **APIs inseguras:** Los proveedores de la nube ponen a disposición un conjunto de APIs que los clientes utilizan para administrar e interactuar con los servicios. Estas deberían estar diseñadas para evitar cualquier intento de sobrepasar la seguridad.

- **Vulnerabilidades de los sistemas operativos:** Los piratas informáticos pueden sacar provecho de ello para infiltrarse en el sistema, poniendo en riesgo la seguridad.

- **Amenazas persistentes avanzadas (APT):** Son una forma de ataque que se infiltra en los sistemas para comprometerlos y robar datos. Las APT persiguen a sus objetivos de forma sigilosa durante largos periodos de tiempo.

- **Ataques de denegación de servicio (DoS):** Los ataques DoS se han diseñado para evitar que los usuarios puedan acceder a sus datos o aplicaciones, y se encuentran entre las principales amenazas de la nube.

Gabriel Bergel

Gabriel Bergel, Líder de Consultoría en Telefónica Tech Chile, agrega: "La principal amenaza es la popularidad, rapidez e intensidad con que están migrando las personas y empresas a la nube, empujados principalmente por la pandemia del Covid-19, lo que la convierte en un activo muy preciado para los ciberdelincuentes y a la vez exige una debida diligencia por parte de las personas y empresas antes de decidir migrar".

En este sentido, sigue el vocero, "el principal atractivo es el volumen de información disponible en este tipo de plataformas, donde una debilidad podría impactar a muchas empresas de una vez y la débil jurisprudencia internacional en caso de incidentes o cometer un ciberdelito, ya que dependerá del país donde están las plataformas alojadas y los datos, y si existe o no normativas legales aplicables, luego si existen acuerdos o tratados internacionales entre el país desde donde se cometió el incidente o delito y el país donde está implementada la nube".

Para abordar las estrategias de Cloud en una organización desde la mirada de la ciberseguridad, primero, la nube debe verse como una extensión de la empresa. "Es un error considerar que al ir a la nube, la seguridad es tarea de ellos", destaca el ejecutivo de Tenable. "Podrán ser responsables de la seguridad del Datacenter, de sus servidores físicos, del enlace, o dependiendo del servicio, de la aplicación arrendada o del sistema operativo, sin embargo, la información y los usuarios que nosotros depositamos ahí, siempre será responsabilidad del dueño de estos".

La naturaleza elástica de los entornos en la nube permite que los activos en la nube sean provisionados y retirados de forma dinámica, a menudo por personal que no está en el área de seguridad como los equipos de DevOps, web y comercio electrónico. Es por ello que las estrategias de seguridad no aplican de la misma manera. "Entender conceptos que si bien no son nuevos como elasticidad, redes definidas por software (SDN), posturas de seguridad en la nube (CSPM), Frontera de servicios para acceso seguro(SASE), o Zero Trust, ayudan a adoptar tecnologías distribuidas como lo son los servicios de nube de forma segura.

Adicionalmente, la creación de mejores prácticas de seguridad que puedan seguir el ritmo de la nube es otro paso fundamental para proteger sus activos en ese entorno.

Sonnia Reyes Jairala

En suma, considerar siempre seguridad alrededor del usuario y de la información que se maneja", sentencia Alcalá.

Sonnia Reyes Jairala, Territory Sales Manager South of LatinAmerica en WatchGuard Technologies, agrega: "Hay que abrirse un camino hacia la transformación digital, por ejemplo, estandarizar una figura de la red consolidada con refuerzos importantes como Autenticación Multifactor en una plataforma en la nube fácil en despliegue y aprendizaje, una robusta solución que cubra la red empresarial con servicios siempre activos, alineado con herramientas de visibilidad cronológicas, donde logremos atender incidentes inmediatos, cubriendo visibilidad para todos los parámetros del core".

Por su parte, **María Florencia Martin,** directora de ventas regional para Argentina, Chile y Uruguay de Appgate sostiene: "Existe una

relación importante entre el valor que genera o no el hacer uso de servicios, plataformas o infraestructura cloud, uno de los principales focos que debe tener en cuenta una organización es la seguridad, teniendo claridad de los riesgos y los controles que pueden ayudar a mitigar y hacer gestión eficiente. Por ello, es importante tener una visión y estrategia de ciberseguridad tanto a nivel de proveedor cloud como de organización, pero se puede decir que el nivel de seguridad cloud se convierte en una percepción de acuerdo al riesgo y control que se tengan definidos, algo que puede ser fácilmente gestionado".

Las estrategias de migración o modelos de servicio en la nube deben considerar la seguridad como un pilar fundamental, esto implica administrar y mitigar los riesgos o amenazas que se pudieran presentar de una manera adecuada, proporcionar visibilidad, trazabilidad y protección en los diferentes entornos y accesos es mandatorio, para evitar accesos no autorizados y conexiones no permitidas. "Una buena forma de establecer seguridad y control puede ser el despliegue de una solución que mitigue riesgos en el acceso, esto se logra fácilmente al implementar un esquema de postura de seguridad al autenticar y condiciones de conexión para llegar a los recursos alojados en la nube sin que esto implique un impacto en la operación de los clientes", complementa la vocera.

¿Es posible pensar en un entorno cloud 100% seguro?

Durante el 2021 hemos sido protagonistas en la consolidación del modelo de trabajo híbrido en la región. Para 2022, expresa el

María Florencia Martin

ejecutivo de Critrix, "esperamos ver más inversión en la nube, sobre todo pensando en datacenters híbridos con una mayor adopción cloud. Este tipo de inversiones aportará agilidad, flexibilidad y escalabilidad para responder a las necesidades de las empresas hoy en día, pero también mirando hacia el futuro".

Según él, "es posible alcanzar un estadío seguro, siempre y cuando se reciba el asesoramiento adecuado de un proveedor de Cloud. Es necesario tener en cuenta muchos factores y vulnerabilidades de la empresa, antes de brindar un servicio. Sin embargo, sabemos que las amenazas siempre seguirán existiendo y algo tan simple como un error humano es difícil de prevenir. Un nuevo mundo laboral deja expuestas nuevas vulnerabilidades, por lo cual hoy más que nunca es importante poder adelantarse a posibles ataques, a través de soluciones completas de seguridad inteligente y entregadas en la nube, que mantengan protegidos a los usuarios y a la organización, sin las complejidades y el gasto que implica un centro de datos".

En la misma línea, Bergel enfatiza: "La seguridad absoluta no existe, como tampoco existe la plataforma tecnológica 100% segura. A medida que la tecnología avanza, existen nuevas debilidades que se descubren. En seguridad y ciberseguridad trabajamos en base modelos de amenazas y riesgos donde el objetivo principal es disminuir las probabilidades de que una amenaza explote alguna debilidad con un impacto negativo. Así el riesgo se materializa, pero nunca será cero. Los entornos más utilizados son entornos híbridos donde cierta información o plataformas más críticas mantienen un esquema tradicional y plataformas menos críticas, pero masivas se migran a la nube".

Por último, la ejecutiva de Watchguard remarca: "Todos sabemos que la seguridad es un gran desafío en la actualidad, pero la educación de los usuarios debería ser la primera línea de defensa para el Team de TI".

Omar Alcalá

Las principales amenazas que enfrenta la computación en la nube

La cantidad y variedad de datos que se manejan a través de la nube, pero también la baja madurez en seguridad que tienen muchas organizaciones que hacen la transición al modelo resultan muy atractivo para los ciberatacantes. En este sentido, dice Gastón Gualdoni, Regional Sales Manager en CrowdStrike, "si no hay estrategias pensadas para las características específicas de la nube, los atacantes pueden obtener mucha información con poco esfuerzo".

La primera y principal amenaza es la visibilidad reducida, ya que las cargas de trabajo y muchas responsabilidades pasan al proveedor del servicio. Luego, el aumento en la complejidad de las regulaciones, especialmente en organizaciones que operan desde múltiples países. En tercer lugar, los ataques sin malware son una amenaza también. "Este tipo de ataques ha aumentado del 49% a un 68% en los últimos 3 meses según el reporte de nuestro equipo de búsquedas de amenazas Overwatch", dice el ejecutivo. Por último, los agentes internos. "Estos incidentes suelen ser perpetrados con credenciales de acceso autorizadas, lo que dificulta su detección", explica Gualdoni.

Como primer paso para abordar las estrategias de Cloud en una organización desde la mirada de la ciberseguridad, aconseja: "Es importante conocer las características y necesidades de su organización para implementar la nube con precisión, compartiendo responsabilidades con el proveedor y entendiendo las limitaciones del modelo. Esto es lo que permite diseñar estrategias de seguridad verdaderamente eficientes".

Y sigue: "Nosotros creemos firmemente que la unión entre inteligencia artificial e inteligencia humana es la clave. La IA permite analizar altos volúmenes de datos y patrones con rapidez, mientras que los humanos analizan el contexto de las actividades, implementan soluciones y ofrecen insights para mejorar la seguridad".

En términos de costos, "la seguridad en la nube es mucho más eficiente", asegura el experto. "Esto se debe a que no es necesario que una organización detenga sus operaciones para implementarla, ni realizar traslados de equipo, por lo que se evitan así los costos "ocultos" de los modelos de seguridad tradicionales".

Por otro lado, "la seguridad física limita el acceso directo a los datos, lo que es impráctico en el mundo moderno, donde tener información en el momento adecuado puede determinar el éxito de un negocio. La seguridad en la nube ofrece la capacidad de acceder a los datos de forma segura, ya que no se trata de obstáculos, sino de herramientas para controlar el tráfico", concluye Regional Sales Manager en CrowdStrike.

Gastón Gualdoni,
Regional Sales Manager
en CrowdStrike

/www.crowdstrike.com/latam/

Filtración de datos: la principal amenaza en la nube

Adam McCord,
Vice President Latin America Caribbean de Cyberark

www.cyberark.com

Adam McCord, Vice President Latin America and Caribbean de Cyberark, comparte datos de la Cloud Security Alliance (CSA) en donde figura que la filtración de datos es la principal amenaza que sufren las soluciones en la nube. "A medida que más y más información se traslada a la nube, su protección efectiva comienza recién con la pregunta tan básica "¿quién tiene acceso a esto?", reflexiona el vocero.

El costo promedio de una filtración de datos es de 3,92MM. "Mediante métodos de phishing, la explotación de vulnerabilidades o el robo de credenciales, los delincuentes buscan formas de acceder a cuentas con privilegios elevados en la nube, como las cuentas de servicios", detalla. "El secuestro de cuentas supone el control total de la cuenta, sus servicios y los datos que contiene. Esto permite a los agentes maliciosos utilizar cargas de trabajo en la nube para la criptominería, robar datos y atacar otros objetivos".

Las consecuencias de tales compromisos pueden ser graves, desde interrupciones operativas y empresariales significativas hasta la eliminación completa de los activos, datos y capacidades de la organización. Para contrarrestar ese impacto, "aunque el camino hacia la nube de cada organización es único, es recomendable aplicar y mantener políticas de gestión del acceso con privilegios uniformes en toda la empresa", sostiene el vocero. "No es recomendable tener múltiples herramientas y procesos de acceso con privilegios únicos para múltiples escenarios de despliegue en la nube, ya que esto conlleva una mayor complejidad operativa".

En este sentido, desde Cyberark recomiendan las siguientes prácticas que permitirán aplicar sistemáticamente controles de acceso con privilegios y gestión de identidades en toda organización, desde entornos híbridos hasta multinube:

- Protección de las cuentas "root" y de la consola de gestión en la nube ya que éstas permiten la gestión integral de los recursos en la nube de una organización.

- Protección de la infraestructura dinámica en la nube de su organización. Una gran ventaja de la infraestructura basada en la nube es que los nuevos servidores virtuales, el almacenamiento, los contenedores y otros recursos se pueden aprovisionar de forma dinámica según sea necesario.

- Protección de aplicaciones nativas en la nube y procesos de DevOps. Las prácticas recomendadas abogan por una menor dependencia de las credenciales codificadas de forma rígida o "quemadas en código". Eliminar todas las credenciales incluidas en el código es una de las mejores y más relevantes prácticas.

- Protección de aplicaciones SaaS. El primer paso para proteger estas aplicaciones es implementar un servicio de inicio de sesión único (SSO), siempre protegido con autenticación robusta, moderna y adaptativa. El SSO se sirve de un proveedor de identidades central para gestionar la autenticación de usuarios y permitir el acceso a las aplicaciones SaaS a través de un único conjunto de credenciales de inicio de sesión.

Seguridad en la nube: la clave para valorizar el trabajo híbrido

Cecilia Pastorino,
Investigadora de Seguridad Informática de ESET Latinoamérica

www.welivesecurity.com

"La computación en la nube es cada vez más la norma en lugar de la excepción para las empresas", dice Cecilia Pastorino, Investigadora de Seguridad Informática de ESET Latinoamérica. En promedio, hoy en día el 92% de las organizaciones tienen servicios o infraestructura en la nube.

Como correlato, surgen ataques por varias razones que van desde cuestiones económicas hasta prácticas. "Evitar comprar equipamiento que luego se vuelve obsoleto o pierde su valor, evitar gastos de mantenimiento o energía, o simplificar las tareas del área de TI", ejemplifica la vocera. Incluso, sigue, "desde la perspectiva de la pequeña empresa, agregar un servidor o contratar un servicio específico con solo apretar un botón. Mientras que esta solución ha hecho que las cosas sean mucho más sencillas para pequeñas y grandes empresas, también ha llevado a nuevos debates y consideraciones en materia de seguridad".

La nube implica una mayor complejidad, lo cual puede crear brechas de seguridad, especialmente si las organizaciones utilizan múltiples plataformas y nubes híbridas (servidores o servicios locales y tercerizados conectados entre sí). Esto expande significativamente la superficie de ataque corporativo para los ciberatacantes, proporcionando más oportunidades a las que apuntar como cuentas y sistemas mal configurados, contraseñas débiles y vulnerabilidades.

"Con la gran variedad de servicios de cloud computing que existen hoy en el mercado, el primer paso es decidir a quién vamos a confiar la información y sistemas de la compañía", plantea. En este sentido, "es muy importante leer atentamente las condiciones de contratación y tener en claro qué responsabilidades recaen sobre el proveedor y cuales dependen de la propia organización".

Si bien no hay una fórmula única en materia de seguridad, una buena gestión ayudará a mitigar el riesgo, adaptando prácticas seguras de trabajo. Por ejemplo, cifrar los datos almacenados en la nube, y también los datos en tránsito. Si bien puede demandar un esfuerzo extra y aumentar la complejidad de las operaciones, añade una capa adicional de seguridad a toda la información confidencial. Además, asegura Pastorino "es indispensable controlar y limitar el acceso a los servicios en la nube y a la información con contraseñas fuertes y múltiple factor de autenticación".

También es importante contar con soluciones de seguridad en los servidores. Así como existen códigos maliciosos pensados para atacar plataformas de virtualización, como Venom, también hay que considerar al resto de las amenazas que continúan propagándose por los sistemas operativos ya conocidos.

"Las nubes no tienen que traer opacidad o inquietud", dice la experta de ESET. "La capacidad de acceder a archivos y servicios desde cualquier lugar es poderosa, y puede introducir nuevos riesgos para el entorno, o bien puede ser una oportunidad para obtener servicios de confianza y mejorar la productividad general", concluye.

El futuro de la ciberseguridad está en la nube

Tomando como fuente el reporte de Nube y Amenazas de Netskope (Julio del 2021), el cual se enfoca en un análisis profundo sobre las tendencias de amenazas y riesgos de la nube, se han identificado como principales tendencias de amenazas para este año:

- Aplicaciones nube de almacenamiento como Google Drive y Microsoft Drive de uso personal, representando el mayor riesgo asociado a la seguridad de los datos, por ser las más utilizadas en el movimiento no autorizado de datos por parte de usuarios que dejan la organización durante sus últimos 30 días de trabajo.

- Los App Plugins de terceros se han convertido en una amenaza importante para la seguridad de los datos, aprobando el acceso a datos sensibles. La estadística muestra que el 97% de los usuarios de Google Workspace han autorizado al menos a una aplicación de terceros el acceso a su cuenta de Google corporativa.

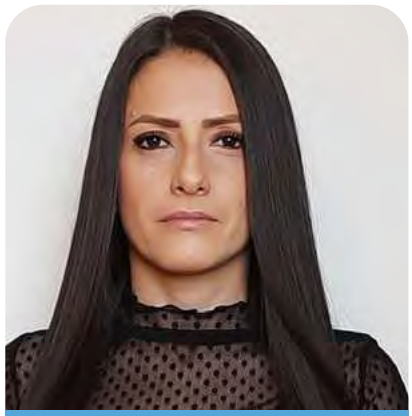
- El acceso público de ambientes en la nube continúa siendo un vector importante de infiltración para los atacantes. El estudio muestra que más del 35% de cargas de trabajo en las principales nubes públicas están expuestas a Internet.

- Incremento en el abuso de aplicaciones nube populares para la entrega de malware y evasión de listas de bloqueo o reputación por parte de los ciberatacantes.

- Persistencia en el modelo de trabajo remoto reportando a finales de junio del 2021 un 70% de usuarios que continúan bajo este escenario, lo cual indudablemente incrementa los vectores de riesgo para una organización.

La adopción de la nube está exigiendo una reestructuración en la actual estrategia de ciberseguridad, la cual en la mayoría de los casos fue pensada y diseñada para arquitecturas y necesidades del pasado. Es así, como también lo ha identificado y plasmado Gartner en diferentes investigaciones, haciendo mención de que el futuro de la ciberseguridad está en la nube. La consultora propone, además, un modelo arquitectónico de servicios nube denominado SASE (Secure Access Service Edge) que busca gestionar de forma eficiente los retos y necesidades propios del proceso de transformación digital en el cual se encuentran en la actualidad las organizaciones.

"Es imposible hablar de la ciberseguridad en la nube sin mencionar el término SASE



Karen Espitia,
Channel Sales Engineer
Netskope Latam

www.netskope.com

y su propuesta de convergencia entre las capacidades del mundo de networking y seguridad entregadas bajo un modelo de servicio en nube", dice Karen Espitia, Channel Sales Engineer Netskope Latam. "SASE se ha convertido en un marco de referencia para articular la estrategia de ciberseguridad en la nube, permitiendo consolidar las tecnologías de la información como un habilitador de optimización y agilidad para el negocio".

En la medida que las organizaciones sean conscientes de la necesidad de transformar su estrategia de ciberseguridad para no solo tener visibilidad sino también control de los riesgos asociados a la adopción de la nube, este proceso de convergencia a un modelo de referencia como SASE será la ruta más acertada para afrontar los actuales retos de seguridad.

Dmitri Zaroubine,
Presales Manager para
Latam en Veeam Software

www.veeam.com

La importancia de una estrategia de disponibilidad

Los modelos y arquitecturas de almacenamiento de datos han evolucionado mucho, desde los servidores físicos a centros de datos, pasando por el SaaS en VM y la nube, la multi-nube o las soluciones híbridas. Todos ellos presentan sus propias ventajas y puntos débiles, planteando una serie de retos en términos de seguridad, habilidades y optimización de costos que las empresas deben conocer antes de invertir fuertemente en esta estrategia.

"Las estrategias de copia de seguridad fiables son fundamentales en un mundo de la nube múltiple", dice Dmitri Zaroubine, Presales Manager para Latam en Veeam Software. "Las agencias deben implementar y seguir un enfoque de protección de datos consistente, simple y fácil de entender".

Una estrategia que es fácil de seguir y recordar, dice el vocero, es la regla 3-2-1-1-0. "Cada número representa una política de copia de seguridad crucial", explica. Para empezar, esto significa mantener tres copias de los datos, aunque es totalmente posible que al final haya más de 3 copias (algunos datos críticos pueden albergar 4 o incluso 5 copias de los datos). De este modo, aunque se destruyan dos copias, los datos del organismo siguen estando protegidos en otras copias. De estas tres copias, los datos deben estar alojados en dos tipos de soportes diferentes. "Gracias a Veeam las empresas pueden tener no solo varias copias, si no un resguardo inmutable frente los ataques de ransomware, teniendo la posibilidad de validar los respaldos y estar 100% seguro que el dato es accesible en caso de ser necesario", asegura el ejecutivo.

Se puede llegar a tener niveles muy altos en ambientes clouds, sin embargo, siempre va existir el riesgo, por lo que se debe implementar una estrategia de protección donde se involucren herramientas y procesos para asegurar los activos de la organización de acuerdo a los requerimientos definidos. "Pero esto no debe ser lo único, todo estos esfuerzos deben estar acompañados por una estrategia de disponibilidad donde, si algún riesgo llegase a materializar, se puedan activar diferentes acciones para recuperar cada uno de los componentes del servicio para estar en línea lo más pronto posible y así minimizar el impacto sobre los SLA establecidos", destaca Zaroubine.

La IT basada en la nube es inevitable para casi todas las organizaciones aunque, a diferencia de todas las generaciones de IT anteriores, no existe una única arquitectura "moderna". En el pasado, casi todo el mundo se estandarizó en Midrange, luego NetWare, pasando por Windows, hasta llegar a la virtualización con VMware. Esta vez, dice el ejecutivo, "hay varios escenarios "modernos" como IaaS, SaaS, PaaS y contenedores, cada uno con distintas ventajas y con diferentes requisitos de protección de datos".

El reciente informe sobre las tendencias para la protección de la nube 2021 de Veeam, muestra que aunque la IT central sigue estableciendo la mayoría de las veces la estrategia general de protección de datos, algo especialmente importante para la coherencia de la gestión y el cumplimiento en la conservación de los mismos, puede resultar más resistente en la nube nativa. Sin embargo, es necesario conservarlo", concluye el Presales Manager para Latam de la compañía.

CryptoCurrency Security Standard (CCSS)

Por Leonardo Devia

El estándar de seguridad de criptomonedas (CCSS) es un conjunto de requisitos para todos los sistemas de información que utilizan criptomonedas, incluidos los intercambios, las aplicaciones web y las soluciones de almacenamiento de criptomonedas. Al estandarizar las técnicas y metodologías utilizadas por los sistemas en todo el mundo, los usuarios finales podrán tomar decisiones informadas sobre qué productos y servicios utilizar y con qué empresas desean alinearse.

CCSS está diseñado para complementar los estándares de seguridad de la información existentes (es decir, ISO 27001:2013) mediante la introducción de una guía para las mejores prácticas con relación a las criptomonedas como Bitcoin.

CCSS no está diseñado para sustituir o reemplazar estos estándares; de hecho, seguir la CCSS al pie de la letra e ignorar estándares como ISO 27001:2013 probablemente conducirá a un compromiso. CCSS es un estándar de criptomonedas que aumenta las prácticas estándar de seguridad de la información. Al igual que con cualquier estándar, los profesionales de seguridad y/o auditores con conocimientos y experiencia son necesarios al implementar cualquier sistema de información, para garantizar la cobertura de todas las clases de ataques, así como el manejo adecuado de todos los riesgos potenciales.

Diez aspectos

CCSS cubre una lista de 10 aspectos de seguridad de un sistema de información que almacena, realiza transacciones o acepta criptomonedas. Un sistema de información es una colección de tecnologías (hardware y/o software), personal, políticas y procedimientos que trabajan juntos para proporcionar un entorno seguro. El valor mínimo de los 10 aspectos determina el puntaje general de un sistema de información dentro de tres (3) niveles de seguridad creciente: el nivel I es el más bajo y ofrece fuertes medidas de seguridad, mientras que el nivel III es el más alto y ofrece la seguridad más completa.

> “CCSS está diseñado para complementar los estándares de seguridad de la información existentes (es decir, ISO 27001:2013) mediante la introducción de una guía para las mejores prácticas con relación a las criptomonedas como Bitcoin.”

El CCSS cubre los controles que aumentan la seguridad de la porción de criptomonedas de un sistema de información, sin embargo, no cubre los estándares y prácticas comunes para aumentar la seguridad cibernética de un sistema de información. Por esta razón, CCSS debe considerarse como un conjunto separado de recomendaciones que se aplican por encima de las prácticas de seguridad estándar en otros dominios, incluida la continuidad del negocio, la recuperación de desastres, la prevención de intrusiones en la red, la seguridad física y la gestión de vulnerabilidades.

La CCSS se aplica a cualquier sistema de información que utilice criptomonedas. Esto incluye (pero no se limita a):

- Intercambios de criptomonedas (es decir, sistemas de información que permiten a sus usuarios intercambiar criptomonedas por otras formas de dinero)
- Mercados de criptomonedas (es decir, sistemas de información que permiten a sus usuarios intercambiar criptomonedas por otros bienes y servicios)
- Juegos de criptomonedas (es decir, sistemas de información que permiten a los usuarios apostar sus criptomonedas para tener la oportunidad de ganar más)
- Procesadores de criptomonedas (es decir, sistemas de información que automatizan la aceptación de criptomonedas para el pago)
- Almacenamiento de criptomonedas (es decir, sistemas de información que facilitan la recepción y transmisión de criptomonedas entre otros actores)
- Cualquier sistema de información que maneje criptomonedas como parte de su lógica empresarial.

Clasificación

CCSS se divide en tres (3) niveles de seguridad creciente:

Nivel I

Un sistema de información que ha alcanzado el nivel I de seguridad ha demostrado mediante una auditoría que protege sus activos de información con altos niveles de seguridad. La mayoría de los riesgos para los activos de información del sistema se han abordado mediante controles que cumplen con las pautas de la industria. Si bien este es el nivel más bajo dentro de CCSS, aún representa una gran seguridad.

Nivel II

Un sistema de información que ha alcanzado el nivel de seguridad II ha demostrado mediante una auditoría que superan los fuertes niveles de seguridad con controles mejorados adicionales. Además de cubrir la mayoría de los riesgos para los activos del sistema de información, se ha empleado el uso de tecnologías de seguridad descentralizadas, como firmas múltiples, que exceden las pautas de la industria y brindan redundancia si alguna clave o persona no está disponible o se ve comprometida.

Nivel III

Un sistema de información que ha alcanzado el nivel de seguridad III ha demostrado mediante auditorías que superan los niveles mejorados de seguridad con políticas y procedimientos formalizados que se aplican en cada paso de sus procesos comerciales. Se requieren múltiples actores para todas las acciones críticas, los mecanismos de autenticación avanzados garantizan la autenticidad de todos los datos y los activos se distribuyen geográfica y organizativamente de tal manera que sean resistentes al compromiso de cualquier persona u organización. En este sitio web se puede acceder al Framework completo: https://cryptoconsortium.github.io/CCSS/Details/

Ventajas y desventajas de la autenticación biométrica

La autenticación biométrica y sus usos en la tecnología moderna y las aplicaciones digitales tiene una serie de ventajas: una alta seguridad y garantía, experiencia de usuario cómoda y rápida, es intransferible y a prueba de falsificaciones.

Una alta seguridad y garantía

La biometría proporciona mayores niveles de garantía a los proveedores de que una persona es real, al verificar un rasgo tangible del mundo real como algo que el usuario tiene y algo que es. La mayoría de las contraseñas y PIN y la información de identificación personal, probablemente se hayan visto comprometidas con una filtración de datos, lo que significa que los estafadores pueden acceder a miles de millones de cuentas que conservan las respuestas a los métodos de autenticación tradicionales.

La introducción de la autenticación biométrica en el proceso, agrega un obstáculo para los estafadores que sólo un usuario real y autorizado puede circunnavegar. Por más de que un estafador pueda saber que una persona usa el nombre de su perro y algunos números de la suerte para la mayoría de sus cuentas en línea, no puede usar su huella digital para desbloquear una cuenta si no pueden proporcionarse en el acto. La biometría sólo puede ser proporcionada por personas vivas que respiran; en este momento, un robot tendría dificultades para pasar un escaneo de iris.

La experiencia del usuario es conveniente y rápida

Si bien los procesos internos para la autenticación biométrica son técnicos, desde el punto de vista del usuario es increíblemente fácil y rápido. Colocar un dedo en un escáner y desbloquear una cuenta en segundos es más rápido que escribir una contraseña larga que tiene varios caracteres especiales. Además, olvidar una contraseña es un error común de la mayoría de los usuarios. ¿Las probabilidades de que olvide sus propios datos biométricos?

> “La introducción de la autenticación biométrica en el proceso, agrega un obstáculo para los estafadores que sólo un usuario real y autorizado puede circunnavegar.”

Intransferible

La autenticación biométrica requiere que su entrada esté presente tras la autorización. No puede transferir o compartir un biométrico físico de forma digital; la única forma de utilizar la mayoría de los sistemas de autenticación biométrica es con una aplicación física.

Casi a prueba de falsificaciones

Rasgos biométricos como patrones faciales, huellas dactilares, escaneo de iris y otros,

son muy difíciles de replicar con la tecnología actual. Existe una probabilidad entre 64 mil millones de que su huella digital coincida exactamente con la de otra persona. Dicho de otra manera, tiene más chances de ganar la lotería que tener la misma huella digital que un pirata informático que intenta acceder a su cuenta protegida por datos biométricos.

Desventajas de la autenticación biométrica

Por más de contar con una mayor seguridad, eficiencia y conveniencia, la autenticación biométrica y sus usos en la tecnología moderna y las aplicaciones digitales también tienen desventajas:

Costos

No es de extrañar que la implementación de un sistema de seguridad más avanzado requiera inversiones y costos importantes. Uno de los aspectos a tener presente, como "la principal razón para no adoptar la autenticación biométrica", es el costo. La transición a una autenticación biométrica no sería lo único por lo que una empresa tendría que pagar, esto conlleva la necesidad de actualizar sistemas para admitir un cambio a la autenticación biométrica en sus dispositivos.

Filtraciones de datos

Las empresas y los gobiernos que recopilan y almacenan los datos personales de los usuarios se encuentran bajo la amenaza constante de los piratas informáticos. Debido a que los datos biométricos son insustituibles, las organizaciones deben tratar los datos biométricos confidenciales con mayor seguridad y precaución, algo que es costoso y técnicamente difícil para mantenerse a la vanguardia de los avances en materia de fraude. Si una contraseña o un PIN están comprometidos, siempre existe la posibilidad de cambiarlos. No se puede decir lo mismo de la biometría fisiológica o conductual de una persona.

Seguimiento

En la medida que el mundo aumenta el uso de sistemas de autenticación biométrica como la tecnología de reconocimiento facial y otras medidas de se-

guridad biométrica, se debe tener en cuenta la privacidad de los usuarios. Cuando los datos biométricos se convierten en datos y se almacenan, particularmente en lugares o países que tienen grandes medidas de vigilancia, un usuario corre el riesgo de dejar un registro digital permanente que potencialmente puede ser rastreado por actores nefastos. En muchos casos, las organizaciones y los gobiernos han utilizado software de reconocimiento facial para rastrear e identificar a las personas con una precisión aterradora que inhibe significativamente la privacidad. A medida que aumenta la vigilancia, los datos biométricos pueden convertirse en una etiqueta digital permanente que se puede utilizar para rastrear a alguien, con y sin su conocimiento.

> “En la medida que el mundo aumenta el uso de sistemas de autenticación biométrica, se debe tener en cuenta la privacidad de los usuarios.”

Parcialidad

Minimizar el sesgo demográfico en biometría, mientras se verifican las identidades de los solicitantes durante la incorporación digital, es un desafío para los proveedores. La mala implementación de la tecnología, o el mal uso deliberado, pueden resultar en discriminación y exclusión. Sin una solución comprobada de prueba de identidad centrada en documentos, el rendimiento entre demográficos puede ser poco confiable y limitar el acceso de los clientes a elementos esenciales como el crédito y la gama en expansión de servicios digitales.

Falsos positivos e inexactitud

Los métodos de autenticación biométrica más comunes se basan en información parcial para autenticar la identidad de un usuario. Por ejemplo, un dispositivo biométrico móvil escaneará una huella digital completa durante la fase de inscripción y la convertirá en datos. Sin embargo, la autenticación biométrica futura de la huella digital solo utilizará partes de las impresiones para verificar la identidad, por lo que es más rápido. En 2018, se creó una plataforma de inteligencia artificial que pudo descifrar, de manera fraudulenta, la autenticación de huellas dactilares con una tasa de éxito del 20% al hacer coincidir las similitudes de las impresiones parciales con los datos biométricos completos.

Crédito: Art Rachen on Unsplash

ESET PROTECT

Máxima seguridad digital para empresas

Soluciones escalables en prevención, detección y respuesta para endpoints con la plataforma ESET PROTECT, que protege datos comerciales y usuarios de su empresa con tecnología en múltiples niveles.

- Visibilidad en tiempo real
- Reportes avanzados y personalizables
- Gestión centralizada en una pantalla
- Consola en la nube muy fácil de usar

Encuentre la mejor solución para su empresa haciendo **clic aquí**

TUX SOLUTIONS

www.tux-solutions.com

www.nexsysla.com

NEXSYS WHATSAPP FOR BUSINESS

Predicciones para el futuro de la gestión de identidades y accesos

El COVID-19 tuvo un impacto dramático en casi todas las funciones dentro de la empresa, y la administración de identidad y acceso no es una excepción. En una era de mayor trabajo remoto, los enfoques tradicionales para la administración de acceso están luchando para administrar los dispositivos y las identidades de los usuarios que ahora existen fuera de la empresa.

Muchas organizaciones ya no poseen las habilidades y los recursos internos para abordar de manera efectiva la creciente complejidad de los desafíos de administración de identidad y acceso (IAM) que enfrentan. A medida que el panorama de IAM continúa evolucionando rápidamente, los líderes de seguridad y riesgo deben mejorar sus enfoques para la prueba de identidad, desarrollar habilidades de administración de proveedores más sólidas y mitigar los riesgos de una fuerza laboral cada vez más remota.

Para ayudarlos a abordar de manera eficaz esta nueva era, se han realizado cinco predicciones estratégicas para el futuro de IAM y la detección de fraudes. Estas predicciones se centran en las tendencias actuales en identidad descentralizada, gestión de acceso, servicios profesionales de IAM y pruebas de identidad.

Predicción # 1:

La malla de ciberseguridad admitirá más del 50% de las solicitudes de IAM para 2025.

El antiguo modelo de seguridad de "adentro significa confiable" y "afuera significa no confiable" se ha roto durante mucho tiempo. La mayoría de los activos y dispositivos digitales están fuera de la empresa, al igual que la mayoría de las identidades.

El modelo de malla de ciberseguridad proporciona un enfoque más integrado, escalable, flexible y confiable para el control de acceso a activos digitales que los controles perimetrales de seguridad tradicionales. Para 2025, la malla de ciberseguridad admitirá más de la mitad de todas las solicitudes de IAM, lo que permitirá un modelo de gestión de acceso unificado más explícito, móvil y adaptable.

> "Para 2025, la malla de ciberseguridad admitirá más de la mitad de todas las solicitudes de IAM, lo que permitirá un modelo de gestión de acceso unificado más explícito, móvil y adaptable."

Predicción # 2:

Para 2023, el 40% de la convergencia de aplicaciones de IAM estará impulsada principalmente por los MSSP que se centran en la entrega de las mejores soluciones en un enfoque integrado.

Las organizaciones carecen de los recursos y las habilidades calificadas para planificar, desarrollar, adquirir e implementar soluciones integrales de IAM. Como resultado, están contratando empresas

de servicios profesionales para que brinden el apoyo necesario, particularmente cuando es necesario abordar múltiples funciones simultáneamente.

Cada vez más, las organizaciones dependerán de las empresas de proveedores de servicios de seguridad gestionados (MSSP) para obtener asesoramiento, orientación y recomendaciones de integración. Para 2023, el 40% de la convergencia de aplicaciones de IAM estará impulsada principalmente por los MSSP que se centran en la entrega de las mejores soluciones en un enfoque integrado, cambiando la influencia de los proveedores de productos a los socios de servicios.

Predicción # 3

Para 2024, el 30 por ciento de las grandes empresas implementarán Soluciones de verificación de identidad para abordar las debilidades comunes en los procesos del ciclo de vida de la identidad de la fuerza laboral.

Históricamente, los flujos de trabajo de inscripción y recuperación proporcionados por los proveedores para la autenticación multifactor han incorporado "señales de verficación" débiles, como direcciones de correo electrónico y números de teléfono. Como resultado, la implementación de una "corroboración de mayor confianza" se ha dejado como un ejercicio para la empresa. Todo esto tiene que ver con el ejercicio de diferenciación de falsos negativos en la gestión de los productos de IDM.

Debido al aumento masivo de las interacciones remotas con los empleados, los procedimientos de inscripción y recuperación más sólidos son un requisito urgente, ya que es más difícil diferenciar entre atacantes y usuarios legítimos. Los productos de prueba de identidad se implementarán cada vez más dentro del ciclo de vida de la identidad de la fuerza laboral para abordar tales debilidades.

Predicción # 4

En 2024 comenzará a surgir un estándar de identidad global, portátil y descentralizado.

Los enfoques centralizados para administrar los datos de identidad, comunes en el mercado actual, luchan por brindar beneficios en las tres áreas clave: privacidad, garantía y seudoanonimato. Un enfoque descentralizado utiliza la tecnología blockchain para ayudar a garantizar la privacidad, lo que permite a las personas validar las solicitudes de información al proporcionar al solicitante solo la cantidad mínima de información requerida.

Predicción # 5

Para 2022, el 95 por ciento de las organizaciones requerirán que los proveedores de pruebas de identidad demuestren que están minimizando el "sesgo demográfico".

Los sesgos con respecto a la raza, la edad, el género y otras características

"Un enfoque descentralizado utiliza la tecnología blockchain para ayudar a garantizar la privacidad, lo que permite a las personas validar las solicitudes de información"

llamaron la atención de manera significativa en 2020, coincidiendo con el mayor interés en la prueba de identidad centrada en documentos en casos de uso en línea. Este proceso de "identificación más selfie" utiliza algoritmos de reconocimiento facial para comparar las selfies de los clientes con la foto de su documento de identidad.

Siempre ha habido conciencia de posibles sesgos en los procesos de reconocimiento facial, con implicaciones en la experiencia del cliente, daño a la marca y la responsabilidad legal. Como resultado, para 2022, la mayoría de las organizaciones requerirán que los proveedores de pruebas de identidad demuestren que están minimizando el sesgo demográfico, un aumento significativo de menos del 15% actual.

Una nueva póliza de Seguros: Riesgos de ciberseguridad

El delito cibernético se ha intensificado en los últimos años, en particular el ransomware. En 2019, se estima que hubo pérdidas por más de 5.000 millones de dólares, por causa de ese ataque. El compromiso del correo electrónico empresarial y los ataques de phishing también han aumentado a medida que los piratas informáticos utilizan cualquier vulnerabilidad en los procesos de validación u otras prácticas recomendadas para intentar acceder a los sistemas informáticos de una organización.

“Una póliza de seguro cibernético brinda cobertura al asegurado en caso de un ataque cibernético que resulte en la pérdida de datos y/o la violación de información confidencial.”

La amenaza es más real que nunca. Desde que comenzó la pandemia de COVID-19, los delincuentes han acelerado el ritmo alcanzando nuevos ataques en múltiples industrias, incluidas organizaciones de atención médica, agencias gubernamentales e instituciones educativas. Buscan interrumpir las operaciones comerciales, robar datos personales, la propiedad intelectual y causar daños a la reputación.

Con el incremento del delito cibernético, el cual se ha vuelto más lucrativo para los piratas informáticos, las organizaciones están considerando recursos adicionales para ayudar a proteger a sus empleados, clientes y clientes y cubrir los altos costos asociados con la recuperación. Una de estas opciones es el seguro de riesgos de ciberseguridad.

¿De qué se trata la póliza de riesgo de ciberseguridad?

El seguro es un método de transferencia de riesgos que coloca riesgos específicos a otra persona o entidad por parte o la totalidad de la pérdida financiera asociada. Una póliza de seguro transfiere el riesgo a través de una obligación contractual de un asegurado a un proveedor de seguros, sujeto a los términos y condiciones de la póliza de seguro.

Una póliza de seguro cibernético brinda cobertura al asegurado en caso de un ataque cibernético que resulte en la pérdida de datos y/o la violación de información confidencial. Dependiendo de los términos y condiciones de la póliza de ciberseguro, el asegurado podría recuperar el costo de:

- Restaurar las identidades personales de los clientes afectados
- Restauración de datos
- Interrupción del negocio que resulta en la pérdida de ingresos.
- Comunicarse con clientes, clientes, empleados y otras partes interesadas
- Multas y sanciones

- Responsabilidad de seguridad y privacidad
- Extorsión cibernética
- Interrupción de la red

¿Es adecuado para la empresa?

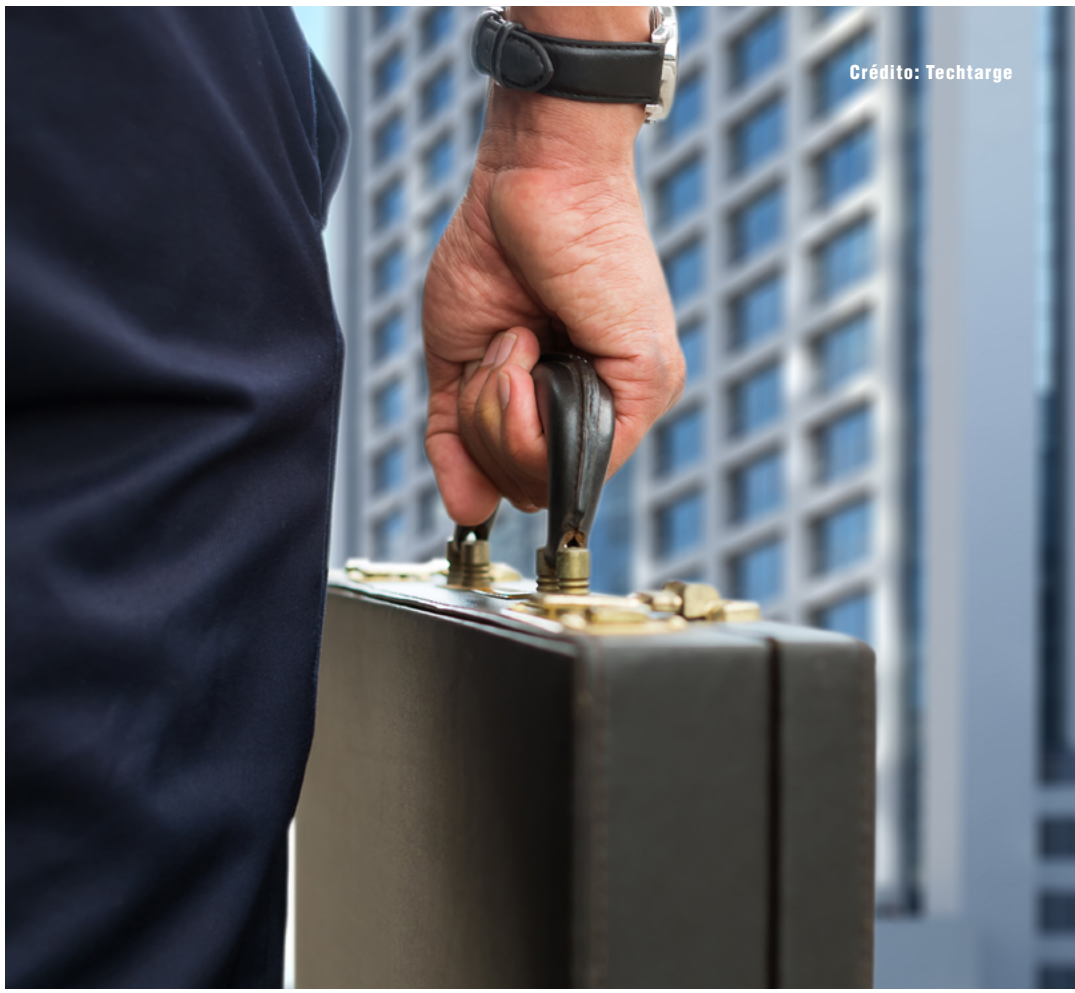
Cualquier organización que esté considerando el seguro de riesgo de ciberseguridad debe consultar con sus departamentos de tecnología y riesgos, así como con otros asesores, como un corredor de seguros que se especialice en cobertura de pólizas de seguridad de la información. Entre todos deben evaluar el riesgo de ataques cibernéticos y evaluar el valor que puede proporcionar una póliza de seguro. Esta evaluación incluiría el deducible, la prima, el límite de cobertura y los términos de cobertura de la póliza de seguro.

Cada organización tendrá sus propias necesidades únicas, que pueden incluir, entre otras: deducibles, niveles de cobertura y riesgos asegurables. Cada una de estas variables puede afectar el costo final del seguro. Es importante tener en cuenta que el costo final del seguro no es únicamente el costo de las primas de la póliza. Las empresas deben examinar el valor esperado de la póliza considerando la probabilidad de que ocurra un evento y la pérdida esperada de dicho evento y equilibrar esos costos con las primas de seguro y los deducibles.

Las tres pautas a tener en cuenta

- Procurar que la pérdida máxima sea asequible para la organización.
- Considerar la probabilidad de pérdidas
- Validar que la transferencia del riesgo valga la prima que pagará

Es importante revisar la cobertura de la póliza con la compañía de seguros y el corredor de seguros para asegurarse de que la organización tenga la cobertura adecuada según sus necesidades específicas y el apetito por el riesgo. Además, la administración de la organización también debe revisar con un asesor legal el riesgo de un ataque cibernético y su impacto en cualquier requisito regulatorio o contractual.


Crédito: Techtarge

Aplicar seguridad a los modelos operativos requiere colaboración

Por Altaz Valani

Los hackers recurren cada vez más a las conexiones seguras para llevar a cabo violaciones de la red y ataques cifrados. Un nuevo informe del proveedor de seguridad en la nube Zscaler ha revelado que los casos de uso de conexiones HTTPS han aumentado en más de un 300% este año.

El informe anual de la compañía, titulado "The State of Encrypted Attacks" (El estado de los ataques encriptados), dice que, al encriptar las conexiones entre sus clientes de malware y los servidores de mando y control, los ciberdelincuentes pueden evadir la detección de los appliances y el software de seguridad de la red.

"El cifrado ofrece en realidad múltiples beneficios a los atacantes", explicó el equipo de Zscaler. "No sólo es menos probable que el tráfico encriptado sea inspeccionado por los equipos de seguridad, sino que los archivos encriptados son mucho más difíciles de identificar, lo que permite que el malware se deslice sin ser detectado".

Aunque la abrumadora mayoría -el 91%- del tráfico malicioso se debe al malware, las conexiones seguras también se utilizan en ocasiones para otros tipos de ataques. Los programas espía publicitarios representan aproximadamente el 7% y los ataques de phishing el 1,8% del tráfico.

En general, el tráfico de malware seguro aumentó un 212%. Los ataques a navegadores aumentaron un 384% en el año, y el spyware publicitario aumentó un enorme 435%.

Los ataques de criptominería se redujeron en un 20%, mientras que los ataques de secuencias de comandos entre sitios cayeron en un 61%. También disminuyeron los ataques dirigidos a proveedores de servicios sanitarios y organismos públicos.

Entre los tipos de malware que hacen uso de las conexiones seguras, el robo de datos es el más común, en particular el robo de información personal identificable.

"Después de la infección inicial, muchas de las nuevas variantes de malware móvil utilizan la comunicación de red SSL para sus actividades de comando y control, incluyendo la obtención de cargas útiles o la recepción de comandos para realizar actividades maliciosas y la exfiltración de datos", escribió Zscaler en el informe.

> “Las organizaciones que no inspeccionan su tráfico cifrado no tendrán visibilidad del malware hasta después de que haya entrado en sus sistemas”

"Mientras que la mayoría de las organizaciones tienen alguna forma de protección contra el malware, los atacantes están mejorando sus técnicas, creando nuevas variantes de malware que son capaces de eludir las tecnologías de huella digital", dijo Zscaler.

"Por supuesto, las organizaciones que no inspeccionan su tráfico cifrado no tendrán visibilidad del malware -incluso del malware conocido- hasta después de que haya entrado en sus sistemas."

Fuente: Techtarget (https://searchsecurity.techtarget.com/post/Applying-security-to-operating-models-requires-collaboration)

Repensar la seguridad de los datos en un contexto de cambio

Juan Manuel Gómez

www.citrix.com

Por Juan Manuel Gómez, director de ventas soluciones de espacios de trabajo, Citrix Latinoamérica

Ser malabarista no es fácil. Lograr lanzar e ir atajando varias pelotas a la vez requiere de múltiples habilidades: capacidad de aprendizaje y de reacción, flexibilidad, concentración para poder seguir el ritmo y poder de anticipación para evaluar las trayectorias de las pelotas, entre otras. El foco no está en que las pelotas no se caigan sino generar un equilibrio perfecto. Algo similar tuvieron que lograr los departamentos de TI en el último año buscando combinar de forma eficiente la experiencia del usuario, la productividad, el trabajo remoto y la seguridad en un escenario laboral distinto. Pero con un riesgo exponencialmente mayor.

En medio de esos cambios, garantizar la seguridad de los datos se convirtió en un gran desafío y se pudo percibir que el trabajo remoto tuvo un impacto en el crecimiento de vulnerabilidades sufridas por las organizaciones. De hecho, un estudio que realizó Citrix recientemente enfocado en seguridad en Argentina, Brasil, Chile, Colombia y México, lo confirma ya que el 77% de los líderes de TI entrevistados creen que las amenazas a la seguridad están directamente relacionadas a la implementación del trabajo remoto.
En este sentido, el 92% afirmó haber tenido que adaptar la estrategia de seguridad y el 92% ha cambiado, incluso, los requerimientos de seguridad de proveedores y partners. Claramente este nuevo escenario laboral requiere una evolución en materia de seguridad y aunque muchos pueden pensar que pronto estaremos regresando a las oficinas, un esquema de trabajo híbrido tampoco se adapta a las estrategias de seguridad que usábamos antes de la pandemia.

Repensar la estrategia de seguridad tiene que ver con implementar tecnologías que sean seguras desde su concepción, arquitecturas basadas en la validación constante del perímetro de seguridad (que ya no puede estar centrado en el edificio corporativo sino en el acceso a los datos), en reforzar la seguridad de la red y de la forma en que se entregan aplicaciones y datos. La gestión de los dispositivos y la visibilidad total de los que sucede en la red también son factores relevantes. De hecho, un 38% de los líderes de TI entrevistados manifestó que ya implementaron tecnologías como machine learning e inteligencia artificial para mejorar la seguridad de sus empresas. Y un 46% afirmaron que su plan es hacerlo en menos de 12 meses.

Otro punto relevante que los líderes de TI mencionaron en el estudio es la capacitación; pero no solo de cara a los empleados para que aprendan medidas de seguridad básicas sino del entrenamiento constante que los equipos de TI necesitan ante una realidad tan cambiante: amenazas de hackers que evolucionan de forma acelerada y estilos de trabajo que ya no son tan predecibles como en el pasado.

Queda claro que el futuro del trabajo que estamos construyendo presenta múltiples desafíos para el departamento de TI. La seguridad, al mismo tiempo, necesita evolucionar al ritmo de la actualidad pero también anticipándose al futuro sin impactar negativamente en la productividad y la experiencia de trabajo. De esa forma, se podrá avanzar en la búsqueda de ese equilibrio perfecto entre los principales factores que impulsan el éxito de las organizaciones hoy.

Cómo aumentar la seguridad en las bases de datos

Las bases de datos son una parte cotidiana de la ciencia y el análisis de datos y, como tales, contienen información que no solo es relevante, sino que a veces también es muy sensible. Como resultado, la seguridad de la base de datos es una parte increíblemente importante de la seguridad de BI. A medida que los ataques se vuelven más sofisticados y la información en los servidores se vuelve más valiosa, es importante validar que los datos estén seguros implementando estas mejores prácticas de seguridad de bases de datos.

> “Asegurarse de que los datos de la empresa y de los clientes estén seguros, no sólo se recomienda en un mundo cada vez más peligroso, es imperativo.”

Cuando se está desarrollando un algoritmo o programa, las funciones tienden a ser opcionales... hasta que se decide que son necesarias. A veces, este pensamiento se extiende a la creación de bases de datos y la implementación de protocolos de seguridad. Sin embargo, este modelo tiene grandes fallas y puede crear vulnerabilidades innecesarias en la seguridad. Las bases de datos deberían tener todos los protocolos de seguridad configurados al máximo, a menos que sea absolutamente necesario cambiarlos o eliminarlos. Cuando se desee eliminar una función de seguridad, hay que asegurarse de que no haya otra forma de resolver el problema actual.

Rigor al establecer privilegios de acceso, especialmente para ser root

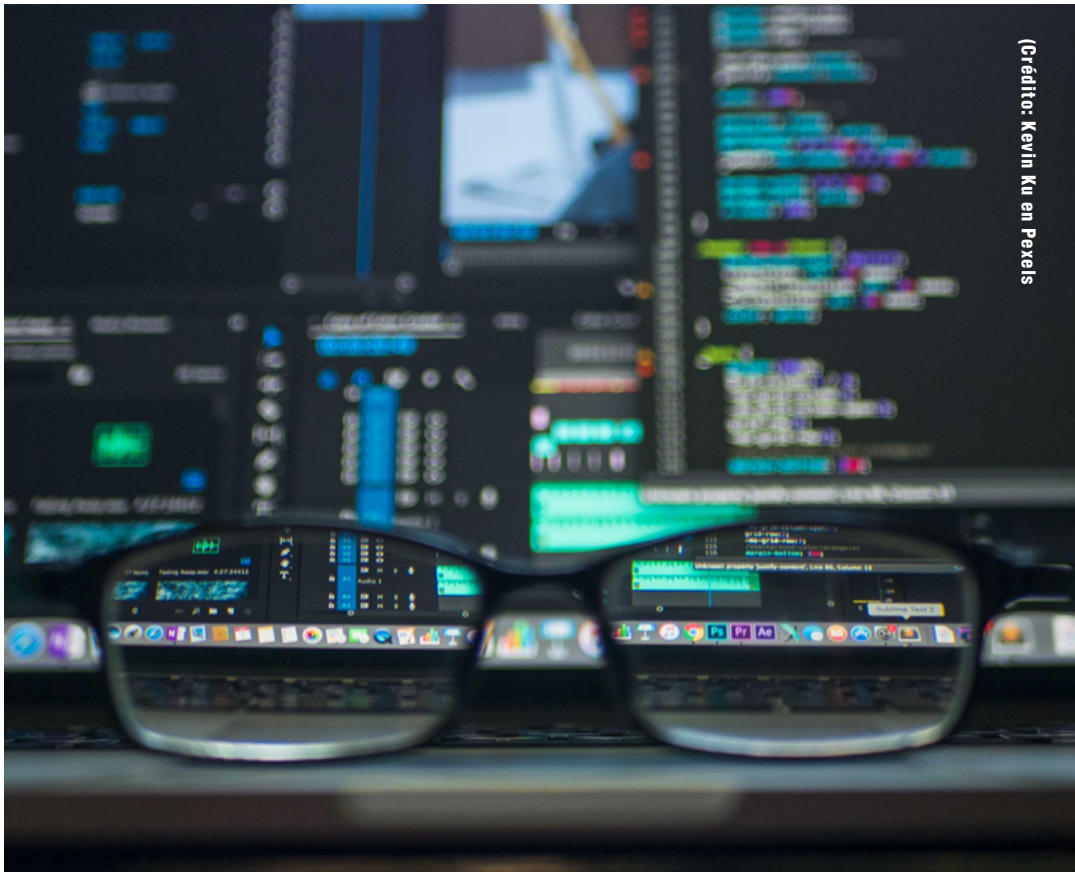
Cuando se trata de análisis y seguridad, hay un tira y afloja constante. Por un lado, la inteligencia empresarial se basa en tener un acceso rápido y libre a los conjuntos de datos. Por el otro, las bases de datos deben tener la capacidad de proteger los datos de modo de evitar que queden expuestos a amenazas accidentales o deliberadas. La solución estándar consiste en crear capas de privilegios de acceso en función de los requisitos de los usuarios. Sin embargo, a veces es demasiado fácil ser negligente en el acceso a funciones de nivel superior en función de lo que la gente cree que necesita.

Para garantizar que los datos estén a salvo, es mejor restringir los permisos según sea necesario. O sea, definir exactamente lo que necesita un usuario antes de elegir su nivel de privilegio. Es probable que algunos no necesiten la capacidad de modificar o manipular datos, mientras que otros pueden requerir un acceso más profundo. De cualquier manera, es vital establecer y establecer límites claros en el acceso de los usuarios.

Implementar múltiples capas de seguridad

Los servidores de bases de datos son esenciales para la inteligencia empresarial, por eso deben estar separados por tantos grados de seguridad como sea viable. Por lo general, los administradores de bases de datos se contentan con guardar tanto los servidores web

como los de bases de datos en la misma plataforma. Esto puede ser conveniente, pero expone de manera significativa los datos a peligros, que pueden ser evitables. Empezar por separar los servidores y crear puentes seguros para que se comuniquen. Una vez que se haya aislado el servidor, también se deben agregar aplicaciones web y firewalls de bases de datos, que puedan manejar mejor el tráfico y filtrar los probables intentos de acceso indeseables. Además, la información siempre deberá estar encriptada cuando se almacena. Finalmente, incluso se pueden eliminar datos no vitales y almacenarlos fuera de línea. Especialmente con los registros obligados a mantener por ley, pero que no son necesarios para las operaciones diarias.


(Crédito: Kevin Ku en Pexels

Supervisar y auditar la base de datos de forma constante

Uno de los mayores dolores de cabeza que enfrentan los admin es la cantidad de intentos de acceso e interacciones que reciben sus bases. No es fácil realizar un seguimiento, y un inicio de sesión o una consulta perdida podría ser causa de daños considerables. Mantener registros precisos y consistentes es un paso clave para mejorar la seguridad pasiva. Si la base de datos se compromete, se puede identificar el momento exacto y la ubicación donde ocurrió. La auditoría está vinculada al registro, pero recopila datos de nivel mucho más profundo, que pueden ser vitales para comprender las infracciones presentes y bloquear las futuras. Se puede realizar el análisis de causa raíz y cumplir con una variedad de protocolos y estándares. Más importante aún, las auditorías constantes ayudan a prevenir ataques al notar irregularidades y probables agujeros en las defensas.

Cuando las necesidades de inteligencia empresarial requieren datos confidenciales y conectividad en línea, es importante saber que las defensas resistirán. La implementación de las mejores prácticas y el cumplimiento de los estándares más actuales son prácticas inteligentes para reforzar la seguridad. Asegurarse de que los datos de la empresa y de los clientes estén seguros, no sólo se recomienda en un mundo cada vez más peligroso, es imperativo.

Qué es el fleeceware y por qué debería importarnos

Malware. Adware. Ransomware. Tantas "wares" lanzados en estos días en el mundo de la ciberseguridad. La última incorporación a esta lista se conoce como "fleeceware". El término fue acuñado por la empresa británica de ciberseguridad Sophos en septiembre de 2019, tras el descubrimiento por parte de la empresa de un nuevo tipo de fraude financiero en Google Play Store

> "El problema con las aplicaciones de tipo fleeceware es que éstas pueden pasar el proceso de aprobación de Google, ya que no se trata de malware y la aplicación en sí no es maliciosa"

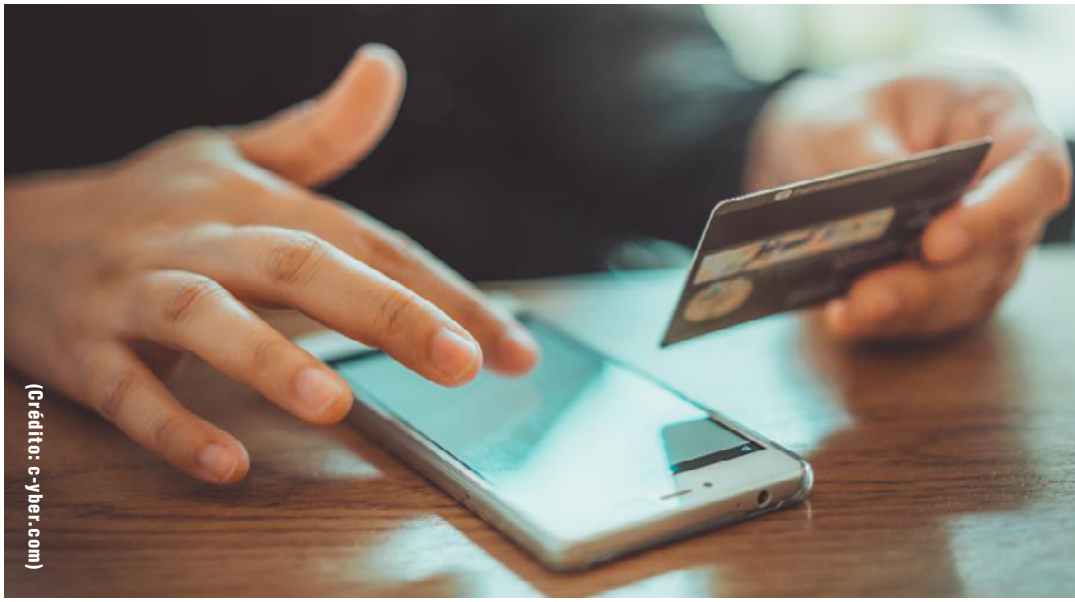
El término Fleeceware hace referencia a situaciones en las que los desarrolladores de aplicaciones manipulan las lagunas de las políticas del periodo de prueba de Play Store para cobrar tarifas excesivas a los usuarios. El proceso consiste en el procedimiento habitual de registro en el periodo de prueba. El usuario rellena sus datos junto con la información de pago al registrarse. La letra pequeña del contrato de software suele indicar que los usuarios deben informar a los desarrolladores de modo de poder cancelar la prueba. Si no lo hacen, los usuarios pueden tener que pagar tasas de cancelación. A veces, estas tarifas pueden ser anormalmente altas, y esto también puede incluirse en la letra pequeña para que los usuarios no presten mucha atención.
A lo largo de los años, los usuarios de aplicaciones se limitan a desinstalar una aplicación cuando termina el periodo de prueba y esto suele ser suficiente para que el usuario se desentienda completamente de la aplicación. Idealmente, esto detendría el periodo de prueba y evitaría que el usuario tuviera que pagar por la aplicación. Sin embargo, una laguna en las políticas de Google permitía que las aplicaciones cobraran a los usuarios incluso después de haberlas eliminado. Esto se debe a que una desinstalación no informa necesariamente al desarrollador de que el usuario no quiere la aplicación.

En términos de Google, estos desarrolladores generalmente siguen las reglas de Google y las aplicaciones funcionan como están previstas. Por lo tanto, Google no reconoce técnicamente a este tipo de desarrolladores como estafadores.

Hace unas semanas, Sophos anunció que nada menos que 600 millones de usuarios de Android han instalado aplicaciones de tipo fleeceware desde Google Play Store. Inicialmente, la compañía se encontró con 24 aplicaciones de este tipo. Estas aplicaciones cobraban a los usuarios hasta 240 dólares al año por funciones básicas como calculadoras y lectores de códigos QR. Sin embargo, un informe de enero afirmaba que esta cifra es mucho mayor.

Sophos afirma que más de 600 millones de usuarios de Android podrían ser vulnerables a diferentes tipos de aplicaciones fleeceware. Pero el analista de malware móvil de Sophos, Jagadeesh Chandraiah, sospecha que las instalaciones reales podrían

ser menores. Chandraiah afirma que es posible que estas aplicaciones utilizaran servicios de pago por instalación de terceros para aumentar el número de instalaciones, seguidas de falsas reseñas de cinco estrellas para aumentar la clasificación en la Play Store y atraer a muchos usuarios. Además, es poco probable que todos los usuarios que instalaron estas aplicaciones se inscribieran en un periodo de prueba. Pero en caso de que seas uno de los que lo hicieron, lo mejor es que compruebes tu historial de pagos en Play Store.


(Crédito: c-yber.com)

El problema va más allá del fleeceware

Por supuesto, no se trata solo de un fleeceware. Las estafas, que van desde el phishing hasta la lotería, existen desde hace décadas. Incluso en 2020, los atacantes siguen engañando a diario.

Tomemos como ejemplo el phishing. Según f-secure, más de un tercio de los incidentes de seguridad comienzan con correos electrónicos de phishing o archivos adjuntos maliciosos enviados a los empleados de la compañía. En un nivel básico, las estafas de phishing suelen producirse a través de correos electrónicos o redes sociales. Normalmente, los atacantes envían correos electrónicos de forma que engañan al usuario para que proporcione información personal y sensible.

A primera vista, estos correos electrónicos parecerán proceder de una fuente oficial. Esto hace que sea más fácil convencer a los usuarios de que hagan clic en un enlace concreto. Si no se tiene cuidado, es posible que, sin saberlo, se proporcione información personal directamente a los propios atacantes.

Otra estafa clásica en Internet es la de la lotería. Normalmente, un atacante envía un correo electrónico llamativo en el que afirma que has ganado la lotería. Aunque este tipo de estafas se hacen bastante obvias cuando se ve el correo electrónico bastante dudoso del remitente. Puede que la gente no sea tan crédula hoy en día, pero sigue ocurriendo.

La cuestión es que las estafas en el espacio digital han estado ocurriendo durante muchos años. Estas adoptan diferentes formas de acuerdo al progreso tecnológico a lo largo de las décadas. Correos electrónicos, SMS, redes sociales, tiendas de aplicaciones para teléfonos inteligentes, los atacantes seguirán manipulando los sistemas existentes si se presenta una oportunidad para extorsionar a la gente. Pero, en cualquier caso, ¿cómo puede uno protegerse de estas estafas?

Cómo protegerse del fleeceware y otras estafas similares

El problema con las aplicaciones de tipo fleeceware es que éstas pueden pasar el proceso de aprobación de Google, ya que no se trata de malware y la aplicación en sí no es maliciosa. Entonces, ¿qué podemos hacer para mantenernos alejados del fleeceware? Para empezar, leer la letra pequeña cuando nos registramos en una prueba ayudará. Es aconsejable evitar las aplicaciones con periodos de prueba muy cortos, por ejemplo, de menos de 7 días. Además, deberíamos prestar atención a cualquier mención de las tasas de cancelación cuando nos insribamos en las pruebas de las aplicaciones de Play Store.

Las estafas que extienden el fleeceware, aunque adoptan muchas formas, suelen operar a través de correos electrónicos y redes sociales. Los servicios como Gmail suelen estar bien equipados para identificar correos electrónicos sospechosos. Pero siempre hay algunos que pueden llegar como correos legítimos. Al igual que en el caso del fleeceware, lo mejor es estar más atentos en general a la hora de comunicarse en línea. Si cualquier proceso requiere que compartamos nuestros datos personales, debemos tener cuidado y estar más atentos.

En cuanto a la colocación de protecciones de software, un método posible es utilizar un antivirus pago. A menudo, estos antimalwares vienen con capas de protección que van más allá de la mera protección antivirus. En los teléfonos móviles, quizá sea mejor desactivar la configuración que permite instalar aplicaciones de tiendas de terceros. Además, si utilizamos cuentas de correo electrónico de la compañía, intentemos utilizarlas a través de Gmail o un cliente de correo electrónico similar en lugar del cliente predeterminado. Esto ayudaría a bloquear mejor los correos electrónicos sospechosos. Por supuesto, estas medidas no protegen por completo de la estafa del fleeceware y de otras estafas relacionadas. Estas son sólo algunas de las cosas que podríamos hacer para protegernos mejor.

El fleeceware es un buen ejemplo de cómo los estafadores siguen desplegando nuevos métodos retorcidos para comprometer a los usuarios desprevenidos. De ahí que sea vital para la población en general una mayor concienciación sobre este tipo de ataques.

SitioSimple

Crear tu página web es tan rápido como leer esta publicidad

Hoy podés tener tu página web o tienda online ¡sin programar y en menos de una hora!

- Más de 200 plantillas pre-diseñadas
- 0% comisiones por venta
- Lista para celulares
- Optimizada para Google
- Múltiples opciones de pago y envíos
- En pesos argentinos

ESCANEÁ
Y EMPEZÁ GRATIS

DonWeb.com

NOTICIAS DEL SECTOR IT EN LATINOAMÉRICA

ITWARE
LATAM.COM

- INFORMACION ACTUALIZADA PARA CIOs
- ENTREVISTAS EXCLUSIVAS.
- COBERTURA INTERNACIONAL DE EVENTOS

Manténgase informado suscribiendo a nuestros newsletter

@ITwareLatam
@ITwareLatam
ITware Latam
ITware Latam
ITware Latam

10 AÑOS