CYBERSECURITY
by itwarelatam.com

Edición - N°15

La revista de Cloud Security

NOTA DE TAPA

Blockchain es segura, pero...

INFORME ESPECIAL

Ciberseguridad en la era Cloud

MÁS TEMAS

¿El fin del Backup?

Prevenir los ataques de estenografía

Top Ten de OWASP en Blockchain

EDICIÓN N°15

NOTA DE TAPA

BLOCKCHAIN ES SEGURA PERO...

04

SUMARIO

CONTENIDO PATROCINADO

16 Por qué las estrategias de seguridad deben ser importantes para los CIOs

INFORME ESPECIAL - DESTACADO

18 Ciberseguridad en la era Cloud

INDENTITY MANAGEMENT

38 Los problemas de gestión del acceso pueden crear agujeros de seguridad

THREAT MANAGEMENT

40 XDR: ¿Bendición para los equipos SOC o moda?

43 Las universidades contratacan

48 Mapeo de los Top Ten de OWASP a Blockchain

RISK ASSESSMENT

54 Hacha y bisturí: el fin del backup

GOVERNANCE

57 Principales regulaciones de la privacidad

61 Riesgo de una “pérdida financiera catastrófica” por los ataques cibernéticos

SECURITY OPERATION

63 Desafíos en Blockchain

64 BaaS: Blockchain como servicio

65 Cómo prevenir los ataques de esteganografía

Blockchain no es tan seguro como aseguran

Nuevo número de Cybersecurity y último de quien esto escribe. A partir del próximo, tendremos nuevo responsable de contenidos.

Pero, mientras tanto, tenemos mucho para leer en éste. Blockchain es un asunto caliente y nuestro tema de tapa lo trata a fondo, especialmente en su relación con la ciberseguridad, que es importante pero a veces... Criptomonedas, contratos inteligentes, ledgers, toda clase de ataques, tanto de malware como de ingeniería se están usando para vulnerar la cadena de bloques y, especialmente, sus datos.

En el informe especial vamos a encontrar un tema que, no por recurrente, está de ninguna manera acabado.

La ciberseguridad en la nube comenzó siendo el principal asunto de esta revista, pero lo ha excedido largamente. Y de eso vamos a hablar con todo detalle.

Y, como no podía ser de otra manera, más contenidos de primera calidad: más amenazas a Blockchain, ataques de esteganografía, y el famoso Top Ten de OWASP. Además, las aseguradoras de ponen nerviosas ante los ciberataques y la vigencia del backup se pone en cuestión, entre otros.

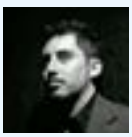
Hasta la próxima.

itseller enfasys ITWARE LATAM.COM

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

Matías Perazzo
Director Editorial
mperazzo@mediaware.org

Ricardo Goldberger
Contenidos
rgoldberger@mediaware.org



Leonardo Devia
Cybersecurity
Consultant - **CSA**

Suscripciones:
info@itwarelatam.com

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

Consultar por suscripción anual

La empresa editora no se responsabiliza por las opiniones o conceptos vertidos en los artículos, entrevistas y avisos.

Prohibida su reproducción parcial o total sin la expresa autorización del editor

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

Edita, diseña, comercializa y distribuye Mediaware Marketing

mediaware MARKETING

BLOCKCHAIN ES SEGURA PERO...

Por Ricardo Goldberger

Como todos ya sabemos, a esta altura del partido, la tecnología Blockchain es un sistema de contabilidad distribuido y descentralizado que puede registrar transacciones entre múltiples computadoras. Blockchain comenzó como la tecnología detrás del bitcoin, pero popularmente se ha convertido en una tecnología de mitigación prometedora para la ciberseguridad.

Blockchain se puede utilizar en cualquier sector o industria. Esto se debe a que cualquier tipo de activo o transacción digital se puede insertar en una blockchain. Se la considera un protocolo de ciberseguridad confiable debido a su capacidad de señalar cualquier juego sucio y brindar certeza en la integridad de las transacciones.

Aunque no es irrompible, blockchain ha evolucionado hasta convertirse en una de las formas más infalibles de realizar transacciones en el ámbito de la red digital. Tal como fue diseñada y prevista, la tecnología ha sido acreditada por su garantía de integridad de la información. Si se utiliza bien, muchos sectores pueden beneficiarse de él.
Es importante dejar aclarado de entrada que la tecnología

Andrés Mercado

> “La tecnología Blockchain fue diseñada para ser transparente por lo que no ofrece privacidad ni confidencialidad de ninguna transacción realizada a través de ella.”

Blockchain fue diseñada para ser transparente por lo que no ofrece privacidad ni confidencialidad de ninguna transacción realizada a través de ella. Cuando se denomina seguro, se pretende describir la integridad de las transacciones, no su privacidad. Uno de sus mejores usos sería utilizar su garantía de integridad para crear soluciones de ciberseguridad para muchas otras tecnologías.
El error humano en particular sigue siendo la principal causa de filtraciones. Blockchain automatiza completamente el almacenamiento de datos y, por lo tanto, reduce el elemento humano en estos sistemas.

Mecanismo seguro

Para Matías Cortés, director de desarrollo de Vortex, “Blockchain es un mecanismo que permite almacenar datos de forma descentralizada, con una trazabilidad y transparencia nunca antes vistas. Previo a esta tecnología el resguardo de los datos estaba siempre en manos de alguna entidad, por lo que en definitiva se debía confiar no sólo en la buena fe de dicha entidad sino también en su capacidad técnica y de procesos para prevenir cualquier intento de acción malintencionada ya sea proveniente desde afuera o desde dentro de la misma organización. De hecho, son numerosos los ejemplos de grandes y reconocidas compañías que sufrieron este tipo de ataques. “

Eduardo Sarmiento

Matías Cortés

"Esta herramienta —afirma Américo de Paula, Líder de Arquitectura de Soluciones para Latinoamérica en AWS— utiliza una red de pares, donde cada parte interesada tiene acceso a un libro de contabilidad compartido en el que se registran las transacciones y que se puede verificar de forma independiente. Como la cadena de bloques no puede modificarse, todas las partes pueden estar seguras de que las transacciones son válidas sin necesidad de ponerse en contacto directamente entre sí."

Andrés Mendoza, jefe técnico para LATAM de ManageEngine, agrega: "La ventaja de blockchain es que no existe una autoridad central y cada nodo se trata por igual. Una transacción se lleva a cabo sólo cuando se alcanza un consenso mayoritario. Esto significa que no hay una copia "oficial" central, y ningún usuario es más confiable que cualquier otro. La naturaleza inalterable y auditada públicamente de blockchain es lo que lo convierte en un candidato ideal para resolver los desafíos de ciberseguridad."

Por su parte, Eduardo Sarmiento, Head Architect de Baufest, añade que "mientras en la mayoría de las bases de datos tradicionales, la seguridad, inmutabilidad y auditoría son características opcionales logradas con diferentes niveles de éxito dependiendo de la implementación; en la blockchain son intrínsecas e inseparables independientemente de su implementación. Notar que esto no significa que los datos estén ocultos, más bien en la mayoría de las blockchain públicas es lo contrario, hay un nivel de acceso a los datos mucho mayor que en sistemas tradicionales, lo que se incrementa exponencialmente es la dificultad de alterar dichos datos o cometer fraude sin dejar un rastro visible para todos los participantes."
Algunos ejemplos de su utilidad los ofrece Martina López, Investigadora de Seguridad Informática de ESET Latinoamérica: "En la industria financiera, por ejemplo, hace algunos años se comenzó a utilizar esta tecnología para mejorar productos y servicios existentes, como los servicios de transferencia internacional de dinero o para realizar pagos. Algunos bancos comenzaron a utilizar blockchain y lograron que las transferencias internacionales se hagan de forma más rápida, a un menor costo y de forma más segura.

Pablo Pirosanto

"En la cadena de suministro también se está usando las bondades de la tecnología blockchain para el seguimiento en tiempo real de bienes a medida que se mueven de mano en mano a través de los que conforman la cadena. Así se garantiza la autenticidad del producto a través de un proce-

so más transparente. Un ejemplo reciente: la distribución de vacunas.

"Algunos hospitales ya están usando blockchain para almacenar y asegurar registros médicos. De esta forma, el historial médico de cada paciente no sólo es asegurado y almacenado, sino que está también disponible para cada médico autorizado, independientemente del centro de salud donde se haya atendido el paciente. Incluso la industria farmacéutica puede utilizar esta tecnología para verificar medicamentos y evitar falsificaciones."

"También está revolucionando el mercado de Internet de las Cosas (IoT) —afirma López—, donde el reto recae en los millones de dispositivos conectados a Internet que deben ser gestionados por las empresas proveedoras. En unos años, el modelo centralizado no va a soportar tantos dispositivos, sin contar que muchos de ellos no son lo suficientemente seguros. Con blockchain los dispositivos pueden comunicarse a través de la red de manera directa, segura y confiable, sin intermediarios."
Finalmente, Pablo Pirosanto, Security Architect en Logicalis, agrega un dato: "Blockchain consta de una arquitectura descentralizada que almacena bloques de datos que a la vez son validados, esta característica de descentralización la vuelve menos vulnerable que un sistema centralizado, sujeto a un único punto de falla. Adicionalmente la validación de bloques la realiza en forma cifrada, lo cual aporta una forma segura de operar."

Sin embargo, Nathan Wenzler, Chief de Estrategia de Seguridad para Tenable, es un tanto escéptico: "Desde una perspectiva de ciberseguridad pura, las tecnologías blockchain son una especie de solución en busca de un problema. Aunque algunas empresas afirman aprovechar Blockchain de alguna manera para aumentar la eficacia de sus productos de seguridad, no ha habido muchos resultados tangibles en ese ámbito.

Sin embargo, desde el punto de vista de la protección y la privacidad de los datos, hay una serie de empresas que trabajan para aprovechar los conceptos de libro mayor distribuido o DTL, por sus siglas en inglés, que las tecnologías Blockchain han construido para crear esquemas de almacenamiento de registros de transacciones y de privacidad de datos más resistentes que tengan menos puntos únicos de fallo o áreas en las que esa privacidad pueda verse comprometida."

Pirosanto remarca: "Si bien las blockchain en general, están constituidas en arquitecturas sólidas y robustas, con mecanismos de protección criptográficos, no dejan de estar expuestas a ataques ya conocidos o a nuevas vulnerabilidades directamente relacionadas a esta tecnología."

Vulnerabilidad y protección

Como dijimos más arriba, Blockchain se considera un protocolo de ciberseguridad confiable debido a su capaci-

Americo de Paula

dad de señalar cualquier juego sucio y brindar certeza en la integridad de las transacciones. Sin embargo, no está exenta de vulnerabilidades.
Pirosanto remarca: "Si bien las blockchain en general, están constituidas en arquitecturas sólidas y robustas, con mecanismos de protección criptográficos, no dejan de estar expuestas a ataques ya conocidos o a nuevas vulnerabilidades directamente relacionadas a esta tecnología."

> "Con blockchain los dispositivos IoT pueden comunicarse a través de la red de manera directa, segura y confiable, sin intermediarios"

"Las redes públicas de blockchain —desarrolla Mendoza— están abiertas y permiten que cualquier usuario se una, asegurando su anonimato. La cadena de bloques pública aprovecha las computadoras conectadas a Internet para validar transacciones y lograr el consenso. Ethereum es un ejemplo de un blockchain público. Por otro lado, las redes privadas de blockchain dependen de las identidades para confirmar los privilegios de membresía y acceso. Por ejemplo, la empresa de banca de inversión, J.P. Morgan, utiliza una red privada de blockchain para simplificar, agilizar y verificar transacciones y contratos."

Sarmiento advierte: "Si bien las blockchain públicas (en la práctica las más utilizadas, pero no las únicas) incorporan las características de seguridad mencionadas también incorporan normalmente otra característica que introduce gran riesgo al sistema: el anonimato. En un robo en un sistema tradicional, los fondos son desviados a una cuenta que por regulación muy pocas veces es anónima. En el mundo de las criptomonedas y productos DeFI, en cambio, muy rara vez ocurre eso, al contrario, los participantes prefieren su anonimato, pero cuando sucede lo peor no hay ningún medio técnico viable para rastrear a un actor malicioso incluso involucrando a las autoridades."

Martina López

Una aplicación que utiliza blockchain como base es en esencia como cualquier otra aplicación hasta el momento donde guarda cierta información o realiza una transacción sobre la blockchain, es en ese momento donde se deben utilizar las claves privadas para poder interactuar con la red. Pero Cortés señala que "el mayor problema es que dichas claves suelen ser complejas para recordar por parte de un usuario final, por lo que la mayoría de las aplicaciones se encargan de guardar dichas claves privadas y el usuario solo posee un usuario/contraseña estándar. O sea, que está 'confiando' en la empresa que desarrolló la aplicación para que resguarde sus claves privadas. Por lo tanto, éste es el punto más crítico

para la compañía que desarrolla una aplicación que funciona sobre alguna Blockchain: ¿cómo resguarda dichas claves privadas? Mi consejo en este punto, es utilizar un producto especializado en soluciones de autenticación y resguardo de metadata sensitiva de alguna de las compañías líderes en el sector."

Otra de las vulnerabilidades —al decir de Sarmiento—, sobre el todo en el mundo de las criptomonedas y aplicaciones DeFI, es la desregulación y confiabilidad de los actores, es frecuente que actores relativamente confiables y con un historial positivo en el pasado, ante un imprevisto actúen negativamente respecto al resto del ecosistema, o incluso hayan tenido intenciones maliciosas desde el inicio. Por ejemplo, hay casos donde los exchange de criptomonedas bloquean los retiros indefinidamente ya sea por falta de liquidez, caídas en el valor de las criptomonedas o simplemente robo."

Las empresas en la actualidad funcionan con datos y dependen de las bases de información para almacenarlos y organizarlos. Aplicaciones de todo tipo, desde banca hasta comercio minorista, confían en Blockchain para mantener la seguridad de sus datos.

> "Los participantes prefieren su anonimato, pero cuando sucede lo peor no hay ningún medio técnico viable para rastrear a un actor malicioso incluso involucrando a las autoridades."

"Con esta tecnología —continúa de Paula—, los ataques cibernéticos son casi imposibles por la forma en que fue armada y pensada: cada transacción tiene un código propio y un libro de contabilidad inmutable y verificable por medio de técnicas criptográficas que confirman que los datos no han sido manipulados, por lo que las aplicaciones quedan bien protegidas."

Ataques y defensas

A pesar del énfasis que los cultores de la cadena de bloques ponen en la seguridad de los datos de una blockchain, lo cierto es que esta tecnología no está exenta de ataques.

Sarmiento es cauteloso: "En general las blockchains en sí han probado ser muy seguras, sobre todo cuando hablamos de redes ampliamente utilizadas (Bitcoin, Ethereum, Cardano, Tron, Polkadot, Solana). Nunca han sufrido el temido ataque del 51%, cuando sucede que más de la mitad de los nodos de la red que debe proteger la integridad de los datos es corrupto. De hecho, han sufrido más problemas de performance que de seguridad. Las redes menos populares, y por ende con menos nodos validadores, tienen mayor riesgo de sufrir un ataque del 51%. En este apartado también se han dado muchos avances, mejorando los mecanismos de consenso de las diferentes blockchains, para no depender del minado (energéticamente ineficiente y poco ecológico). Este punto es muy extenso ya que son numerosos los diferentes mecanismos de consenso que se han desarrollado en los últimos años, algunos con un alto grado de complejidad técnica."

De Paula esboza: "Actualmente, crear una red de blockchain escalable con tecnologías existentes es algo complejo de configurar y difícil de administrar ya que cada miembro de la cadena necesita aprovisio-

nar manualmente el hardware, instalar el software, crear y gestionar certificados para el control del acceso y configurar los componentes de redes. Una vez que la red está en funcionamiento, una autoridad central fiable necesita monitorear continuamente la infraestructura y adaptarse a los cambios, como el aumento en las solicitudes de transacción o que nuevos miembros ingresen a la cadena o se retiren de ella."

> "Las redes menos populares, y por ende con menos nodos validadores, tienen mayor riesgo de sufrir un ataque del 51%"

Además del ataque del 51%, "otra de las amenazas que pueden afectar a las redes blockchain —sigue relatando López— son los ataques de DDoS a los nodos de una red. El objetivo de un ataque de DDoS contra un servicio que utiliza una red blockchain puede ser dejar fuera de servicio un servidor para interrumpir los pools de minería, las billeteras de criptomonedas, plataformas de Exchange, etc.

"Otra forma de ataque se conoce como maleabilidad de transacciones. Ocurre cuando el atacante explota una vulnerabilidad que le permite modificar el hash de una transacción dentro de la red sin invalidarla para engañar al usuario y hacer que pague dos veces. Por último, también está lo que se conoce como ataques de Sybil y el ataque de Erebus. El primero es una modalidad que consiste en crear varias identidades falsas con el objetivo de manipular la red mediante el control de varios nodos y de esta manera tener una mayor presencia en la red; mientras que el ataque de Erebus es una forma de ataque de DDoS, ya que busca interrumpir el funcionamiento de una red haciendo que sea imposible acceder para los usuarios, entre otros."

El eslabón débil

Una especie de axioma de la ciberseguridad en que el eslabón más débil de la cadena suele ser el elemento humano. Y tanto a blockchain como a su tecnología no le faltan argumentos para confirmar el aserto.

"Donde hay dinero, hay piratas informáticos —asevera Mendoza—, y las redes de blockchain están proliferando. Los ataques basados en blockchain provienen tanto de actores externos como de personas internas. Muchos de estos hackers utilizaron tácticas comunes, como phishing, ingeniería social, ataques a datos en tránsito o detectar errores de codificación. Los ataques de blockchain recientes no se han centrado tanto en la tecnología, sino en las vulnerabilidades humanas básicas. Las vulnerabilidades de los endpoints también son puntos de entrada para los actores maliciosos, como los que se encuentran en el nivel del dispositivo, la aplicación, la billetera o el proveedor de terceros."

De acuerdo con Wenzler, "la mayoría de las aplicaciones que utilizan Blockchain hoy en día son carteras de criptomonedas y otros servicios relacionados con las transacciones de criptomonedas. Para estas aplicaciones, el mayor riesgo a menudo se

reduce a problemas de ingeniería social en los que comprometer la contraseña o las credenciales de un usuario conduce a obtener un acceso fraudulento a la cartera y, en última instancia, el robo de la criptodivisa almacenada allí. Esto es especialmente problemático ya que no hay ningún recurso real para que el usuario legítimo recupere su pérdida o recupere su criptodivisa debido a la propia naturaleza de cómo se aprovecha Blockchain para estas transacciones.”.

Y agrega el ejecutivo de Baufest: “Aparte del mal comportamiento de algunos actores que podrían parecer confiables (exchanges / bridges / wallets / DeFi startups), los bugs en los Smart Contracts y problemas de seguridad tradicional en los intermediarios, existe un riesgo intrínseco a las plataformas blockchain basadas en el algoritmo de consenso Proof-of-Work (PoW) (por ejemplo, Blockchain o Ethereum Classic), o comúnmente llamado minería de criptomonedas: si un actor malicioso logra control de más de 51% del poder de procesamiento es posible reescribir la cadena de bloques, con el potencial de introducir transacciones fraudulentas. Por ejemplo, esto sucedió varias veces en el año 2020 a una de las criptomonedas más conocidas y utilizadas: Ethereum Classic”

Mendoza aporta casos “como el intercambio de criptomonedas Bithumb en 2017, un ejemplo de hace algunos años; y algunos casos recientes incluyen Luna Yield a fines de 2021 y el reciente WhaleFarm, un proyecto DeFi que colapsó el 99 % de sus operaciones en cuestión de minutos, estafando a los inversores por U$D 2,3 millones en criptomonedas.”
Y Sarmiento añade: “Efectivamente, hay múltiples casos, solo en el año 2021 se estima fraude por alrededor de 4 mil millones de dólares. Los casos más conocidos están asociados a problemas en el código de los Smart Contracts y en problemas en la seguridad tradicional de los exchanges / bridges de criptomonedas (computa-

dores del personal atacados mediante phishing, troyanos, etc. o de los servidores de la empresa a través de vulnerabilidades no parchadas o similares).

> “Los ataques de blockchain recientes no se han centrado tanto en la tecnología, sino en las vulnerabilidades humanas básicas.”

Y Wenzler da otro ejemplo: “El año pasado, Satnam Narang, uno de nuestros expertos de investigación en Tenable, descubrió cómo se robaron más de 10 millones de dólares en criptomonedas a través de la impersonificación de Elon Musk. En este sentido, los usuarios deben ser muy cuidadosos para proteger las credenciales que aseguran sus carteras de criptodivisas. Como mínimo, nunca se deben compartir contraseñas o utilizar el mismo conjunto de credenciales para las billeteras que las que se utilizan para cualquier otro sitio web o aplicación.”

López ofrece más datos: “Según un informe de Cloud Security Alliance de 2021, en los últimos cinco años 43 exchanges han sido víctimas de incidentes de seguridad y más de 49 protocolos DeFi han sido explotados, lo que ha provocado pérdidas valuadas en más de 2.800 millones de dólares. En los primeros meses de 2022 ya se registraron varios casos, como el ataque a Ronin, la red blockchain que utiliza Axie Infinity, que derivó en el robo de más de 600 millones en ETH. A este incidente se suma el ataque a Wormhole, una plataforma que permite el intercambio de criptoactivos entre distintos blockchain y que derivó en el robo de más de 300 millones o el que sufrió el Exchange Crypto.com, también en 2022.”

Cortés aclara: “Es importante mencionar que muchas veces en la prensa se confunde el término ‘hackearon’ a una blockchain, cuando en realidad lo que sufrió un hack no fue la blockchain sino una aplicación que interactúa con ella. Los casos más conocidos son cuando

Nathan Wenzler

se produce el ‘robo’ de claves privadas de un exchange (casa de cambio de criptomonedas), por lo que básicamente son aplicaciones que no resguardaron debidamente información sensible, como se explicó en la pregunta anterior. “

Y Pirosanto completa: “Existen diferentes amenazas que afectan a la tecnología de blockchain, adicionalmente a las mencionadas anteriormente se podría sumar el MITM (Man in the Middle) attack, que le permite al atacante redireccionar los fondos de las víctimas a sus propias billeteras cambiando la dirección de destino de las transacciones de criptomonedas.”

Mejor que decir…

Ya establecimos las amenazas principales que pueden poner en peligro un sistema Blockchain, su cadena o sus apli-

caciones. Ahora veamos qué podemos hacer para evitarlas, prevenirlas o mitigarlas. Además de las buenas prácticas que se aconsejan en el mundo digital en general, existen diversas empresas que se encargan exclusivamente de brindar seguridad a Dapps (aplicaciones de blockchain). Ofrecen librerías para utilizar ya analizadas, que sirven para la creación de nuevos smart contracts sin tener que reinventar la rueda. Además, hay herramientas para verificar que estos no tengan debilidades o bugs, y evitar luego que puedan corromperse.

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

De Paula ofrece algunos consejos: "Los usuarios y las empresas tienen que respetar normas de ciberseguridad para evitar que otros puedan entrar a su cuenta de Blockchain y hacer transacciones bajo su nombre. Algunas de las medidas que pueden aplicar son crear claves fuertes, no compartirlas con nadie y usar autenticación de factor múltiple, entre otras.

"En general cuando hablamos de aplicaciones que utilizan blockchain de base, la primera sugerencia es utilizar alguna de las redes más populares: Ethereum, Cardano, Tron, Polkadot, Solana, etc. —asevera Cortés—. Al ser más populares tienen mayor distribución de nodos, lo que hace más difícil un ataque del 51%. Algunas también utilizan mecanismos de consenso más avanzados que no se basan únicamente en Pow (Proof of work, el famoso minado). Básicamente el consejo sería: no guarden en infraestructura propia dichas claves, no te pueden robar lo que no tienes. Y para resguardar dicha información confiar en una solución especializada. Tip Adicional: lo mejor es que la interacción con la blockchain se haga directamente desde la aplicación cliente (sin pasar por ningún servidor propio en el medio) y utilizar siempre 2FA para las acciones sensibles."

Sarmiento es más explícito: "En los negocios de criptomonedas y DeFI mayormente desregulados, la mejor estrategia de mitigación está en el conocimiento de la tecnología, sus ventajas/limitaciones y la toma de riesgos calculados. Por otro lado, en las aplicaciones de blockchain para negocios B2B, entidades financieras, bancos centrales, etc., sí existe un conjunto de buenas prácticas ineludibles para evitar las brechas de seguridad; en primer lugar aplicar las mismas políticas de seguridad que se aplicarían bajo cualquier otra tecnología, segundo aplicar las buenas prácticas propias de esta tecnología en particular (por ejemplo, utilizar tecnologías blockchain con permisos, certificar el código de los Smart Contracts, definir sin los datos dentro de cada bloque están encriptados, definir una política de conciliación que haga sentido para el negocio, etc.) y tercero establecer un modelo de gobierno que mitigue los riesgos para todos los participantes y sea fácilmente adaptable a los cambios regulatorios."

> "No guarden en infraestructura propia dichas claves, no te pueden robar lo que no tienes. Y para resguardar dicha información confiar en una solución especializada" - Cortés

Pirosanto expone distintas alternativas según el tipo de ataque:

- Phishing: Mejorar la seguridad del dispositivo mediante la instalación de software de detección de enlaces maliciosos, así como software antivirus confiable. No hacer click en el enlace hasta que se haya revisado que el dominio legítimo.

- Malware (ransomware, mineros y criptojacking): Implementar soluciones de protección contra malware avanzados.

- Vulnerabilidades en los Endpoints de Blockchain: No guardar las claves de blockchain en formato de archivos de texto. Descargar e instalar software antimalware para tus dispositivos electrónicos y revisar el sistema con regularidad, verificando la hora, la ubicación y el acceso al dispositivo.

- 51% ATTACK: Asegurarse de que la tasa de hash sea más alta y evitar el uso de procedimientos de consenso de prueba de trabajo (PoW).

A diferencia de un sistema centralizado, donde si éste es afectado, sus servicios dejan de andar (como sucedió hace un tiempo con Facebook y sus aplicativos, en una red blockchain, al tener varios nodos que replican toda la información, se puede caer una gran parte y la red seguirá funcionando. También posee la ventaja de que, al ser una base de datos compartida, se necesita el consenso para incorporar nuevos datos, pero es imposible modificar el historial. En los sistemas tradicionales centralizados, el administrador puede borrar o modificar información histórica sin restricciones.

Básicamente, cualquier tipo de información que necesite ser preservada de forma intacta, y que deba permanecer disponible, puede ser almacenada en blockchain de manera segura, descentralizada y más económica que a través de intermediarios. Además, si esa información se guarda cifrada se puede garantizar su confidencialidad, ya que sólo quien cuente con la llave de cifrado pueda acceder a ella.

Esto no significa que una cadena de bloques sea lo suficientemente invulnerable como para no preocuparse. Al contrario, tal como menta el “dicho” popular, “si es popular y produce dinero, alguien encontrará la manera de atacarlo.”

SMARTFENSE

Nueva imagen, Misma esencia.

Gestiona el riesgo más relevante con un proceso de Hardening de usuarios

Por qué las estrategias de seguridad deben ser importantes para los CIOs

Por Ilona Simpson, CIO para EMEA de Netskope

Ilona Simpson

Ante las constantes disrupciones, los CIOs están apoyando la adición, modificación o el fortalecimiento de los flujos de trabajo logísticos, las cadenas de suministro, los modelos comerciales y de prestación de servicios, las asociaciones y los detalles geográficos. En todos estos programas, los CIOs a menudo ven la ciberseguridad como un obstáculo; un reto más que hay que sortear en el camino hacia un resultado empresarial exitoso. No obstante, si la ciberseguridad y las estrategias de seguridad, en general, se diseñan y establecen de la manera correcta, deberían verse como un elemento facilitador y no como una restricción para controlar.

Al igual que los seguros de viaje dan a los turistas la confianza para ver el mundo, la seguridad da a los responsables de negocio la confianza y la flexibilidad para innovar.

Tradicionalmente, la seguridad ha consistido en decisiones de acceso binarias: permitir o bloquear. Esto significa que la seguridad actúa como un guarda, con el poder de aprobar o restringir planes y programas. Estos enfoques binarios se siguen imponiendo hoy en día, y los "avances" en seguridad sólo mejoran la capacidad de tomar decisiones binarias de permitir o bloquear (por ejemplo, véase la forma en que las soluciones de seguridad se presentan como de Confianza Cero, mientras se malinterpretan deliberadamente los matices y la flexibilidad continua que el concepto de Confianza Cero fue diseñado para permitir). Y así, la seguridad no consigue desprenderse de su reputación de obstáculo a la innovación, al no facilitar tanto como prohibir.

Pero las cosas están empezando a cambiar. La seguridad está evolucionando por fin para ser más "inteligente", capaz de ver los matices y el contexto, sobre los que puede construir agilidad y flexibilidad. El enfoque en la eficiencia operativa no se ha marchado—de hecho, también se han logrado avances significativos en esa área— pero las inevitables e intensas disrupcio-

> **"La seguridad está evolucionando por fin para ser más "inteligente", capaz de ver los matices y el contexto, sobre los que puede construir agilidad y flexibilidad."**

nes que las empresas han experimentado desde 2019 finalmente ha empujado al departamento de seguridad a hacer de la habilitación un objetivo primordial.
He percibido algunos signos alentadores de interés genuino en la ciberseguridad entre algunos consejos de administración; un interés que va más allá de los ejercicios habituales de marcar casillas. Pero estamos muy lejos de una comprensión amplia y mayoritaria de lo que la seguridad puede hacer por una organización.

En los últimos años, la brecha entre los CIOSs que entienden y adoptan la seguridad y los que no lo hacen probablemente se haya ampliado. Desde 2020, los departamentos de seguridad más astutos de todo el mundo han permitido movimientos en la plantilla a una escala sin precedentes y sin apenas aviso. Han apoyado una agitación rápida y decisiva en las operaciones de la cadena de suministro para garantizar la continuidad del negocio. Han facilitado la reinvención completa de las estrategias de salida al mercado de organizaciones cuya base de clientes desapareció de la noche a la mañana. Los departamentos de seguridad han dado un paso adelante, junto a sus compañeros, para ser héroes de la acción positiva.

Al mismo tiempo, otras organizaciones siguen luchando con estrategias de TI que no logran adoptar las ventajas en agilidad de la nube, o aprovechar el poder de la Inteligencia artificial (IA) y el aprendizaje automático (ML), todo porque no han entendido cómo la seguridad puede desbloquear estas oportunidades.

Y es por ello que un CIO que concibe la seguridad solo como una estrategia de defensa está perdiendo una oportunidad. La seguridad es el primer paso para permitir el crecimiento y la innovación, y la colaboración entre los CIOs y los CISOs es un beneficio para todos.
Las empresas de hoy en día se enfrentan a retos que no se han experimentado en cien años, desde antes de la revolución tecnológica. Los CIOs están dando un paso adelante, utilizando la transformación digital para cumplir con las demandas del negocio para innovar en toda la organización, desde la prestación de servicios a los recursos humanos y todo lo demás. Pero la oportunidad basada en lo digital siempre trae consigo amenazas y riesgos basados en lo digital, y el CISO es un socio crucial para el negocio.

CIBERSEGURIDAD EN LA ERA CLOUD

Por Rocio Bravo

La nube ya es una realidad. Y ese día en que el 100% de los servicios estén en la nube no pareciera estar tan lejos. Sin embargo, en paralelo a que las organizaciones avanzan hacia ese momento, también los ciberatacantes galopan para desarrollar los recursos y las capacidades para lanzar los ataques del futuro. ¿Cómo prepararse?

Un reciente informe de McAfee sobre la adopción de la nube y los riesgos indica un aumento del 630% en 2020.

Alan Mai, especialista en Ciberseguridad y CEO de Bloka, plantea que, en términos estadísticos, el escenario no ha cambiado demasiado en los últimos 2 años, salvo por la cantidad: la cantidad de ataques que estamos viendo se ha incrementado fruto de la adopción de la nube por parte de las empresas, pero en una proporción aún mayor a la adopción; esto es, de manera exponencia

Los riesgos hoy tienen que ver con la customización de los ataques, que permiten vulnerar los controles tradicionales que las organizaciones han implementado, ignorando de forma consciente o inconsciente, el hecho de que la nube - independientemente de qué tipo de implementación de nube estemos hablando - tiene características particulares que deben ser abordadas en la estrategia de ciberseguridad para minimizar la superficie de riesgo y, en su defecto, las chances del atacante de tener éxito.

"Si bien la evolución tecnológica trajo grandes beneficios y aspectos positivos, también nos muestra su costado negativo: la ciberdelincuencia", complementa Martín Malievac, Director de Investigación y Desarrollo de Napse. "Las técnicas para vulnerar servidores, bases de datos, engañar a usuarios y clientes para obtener información valiosa son cada vez más ingeniosas y sofisticadas y se requieren cuidados especiales para evitar caer en este tipo de estafas".

.

Cada vez son más frecuentes los casos de ataques en la nube, en los que las empresas y los usuarios son víctimas del intento o robo de información para después exigirles una recompensa a cambio de la misma.

"Esta es una práctica que no es nueva y que, desafortunadamente, ha aumentado a medida que crece la digitalización. Sin embargo, uno de los puntos fuertes de esta tecnología está dado por su seguridad, la cual aporta numerosas ventajas frente a los sistemas tradicionales", analiza Malievac.

"Hay una gran variedad de ataques que se producen en los entornos de la nube, especialmente debido a la gran variedad de activos que las organizaciones alojan allí", dice Nathan Wenzler, Chief de Estrategia de Seguridad para Tenable.

Los principales riesgos se reducen a dos categorías: la configuración incorrecta de los recursos en la nube y la explotación de las vulnerabilidades tradicionales. Por ello, enfatiza el especilista, "es imperativo que las empresas adopten un enfoque multifacé- Código (IaC), las definiciones y configuraciones de microservicios, así como la configuración y gestión de la nube y los contenedores".

Adriana Jiménez, Gerente Regional de Producto en IFX Networks, comparte la idea de que , como cada vez son más las empresas que trasladan su información a la nube y son más los datos y aplicaciones que desde allí operan y se acceden, "continúa siendo un atractivo para los ciberdelincuentes y un reto muy grande para las organizaciones, los fabricantes y los proveedores de servicio que debemos garantizar la confiabilidad, integridad y disponibilidad de la información".

"El control de identidad y de acceso es hoy en día uno de los principales riesgos a los que se enfrentan las empresas, ya que es fundamental verificar la identidad de los usuarios que acceden a la información, independientemente del lugar y el momento en el que quieran hacerlo, manteniendo niveles altos de protección a través de servicios de seguridad avanzados", detalla la vocera.

Para Octavio Duré, Solution Engineering Director, South of Latin America de VMware, "el cibercrimen ha resultado ser un buen negocio, por lo tanto, es lógico que siga creciendo".

Octavio Duré

La distribución de aplicaciones, hoy ejecutando en múltiples nubes, con microservicios que se comunican e invocan remotamente, crean un expuesto aún mayor que los atacantes se han lanzado a aprovechar, con tecnologías cada vez más sofisticadas. "El principal desafío tiene que ver con la heterogeneidad de plataformas y la dificultad de aplicar políticas de seguridad homogéneas y consistentes en plataformas tan complejas", sostiene.

Rafael Venancio, director de Negocios de la Nube en Fortinet para América Latina y el Caribe, comparte los resultados del Informe de Seguridad en la Nube 2022 que desarrolló en conjunto con Cibersecurity Insiders: el principal riesgo se encuentra en una mala configuración de la plataforma en la nube, a esto le siguen las interfaces y API no seguras, la exfiltración de información confidencial y el acceso no autorizado.

El uso de la nube implica una expansión de la superficie de ataque.

"Ya no solo tenemos que proteger nuestra infraestructura, sino también la que se tiene en la nube", remarca Venancio. "Hoy vemos empresas que tienen sus infraestructuras propias sumadas a diferentes nubes públicas y privadas, con datos y aplicaciones moviéndose entre ellas, que es lo que se llama entornos híbridos. Esto crea entonces no sólo una mayor superficie de ataque, sino también una superficie de ataque heterogénea y dinámica".

Además de eso, sigue, "hay que tener en cuenta algunos aspectos":

- **Seguridad de red:** cómo nos conectaremos a la nube y cómo utilizaremos los servicios que se desplieguen sobre ella. Debemos entender también cómo se interconectará nuestra red y los usuarios a dicha nube. ¿Será por VPN o acceso público, qué protocolos deben permitirse? También debemos entender los esquemas dentro de cada cloud. ¿Habrá múltiples redes o dominios que se deben ver entre sí, y cómo limitamos los ataques dentro de la nube?

- Seguridad de las aplicaciones: es importante considerar si tendremos servicios web publicados, cuáles aplicaciones debemos proteger y si debemos asegurar también servidores mediante mecanismos de IPS. Cabe destacar la integración vía API, que seguirá creciendo, y por lo tanto lo harán sus requerimientos de seguridad.

Santiago Rosenblatt

- Visibilidad y control de la plataforma: esto debe incluir sus configuraciones, actividades de usuarios, análisis de tráficos, seguridad de la información y sus movimientos, y poder determinar su estado de cumplimiento en cuanto a recomendaciones y regulaciones de seguridad de la información.

Los principales riesgos de la nube

Miguel Angel Mendoza, Investigador de Seguridad Informática de ESET Latinoamérica, enumera distintos escenarios los cuales implican que los riesgos varíen en probabilidad e impacto,

en función de los recursos de nube contratados, la arquitectura o las operaciones, incluso si se trata de una nube pública, privada o híbrida. Entre los principales figuran:

- **Pérdida o filtración de información.** Una falla en la aplicación de un cliente podría permitir a los atacantes acceder a los datos de otro cliente. Los datos pueden ser borrados o modificados; las claves de cifrado se pueden perder o robar; existe el riesgo de acceso ilegal a los datos debido a autenticación, autorización y controles de acceso inadecuados, sí como uso indebido de datos por parte de proveedores y terceros.
  Códigos maliciosos y otras ciber amenazas: El uso de la nube no exime del malware, en ocasiones afectando los recursos de los terceros, o bien, utilizando la nube como un repositorio para el almacenamiento y propagación de todo tipo de códigos maliciosos, o campañas de phishing.

Rafael Venancio

- Abuso de servicios en la nube. Los recursos en la nube pueden ser utilizados de forma maliciosa, en caso de que no se aseguren correctamente. Por ejemplo, los atacantes podrían utilizar los sistemas para alojar malware, sitios de phishing, controlar botnets, ejecutar ataques DoS, luego de acceder a la infraestructura mediante ataques de fuerza bruta, explotación de vulnerabilidades u otras técnicas ofensivas.

- Perfil de riesgo desconocido. Los elementos que definen la postura de seguridad de una organización como procedimientos de actualizaciones de software, análisis de amenazas, detección de intrusos y, prácticas de seguridad en general, no se conocen claramente ya que los usuarios están menos involucrados con la propiedad, mantenimiento de hardware y software en la nube. Las organizaciones deben conocer procedimientos de seguridad interna, cumplimiento de medidas de seguridad, endurecimiento de configuraciones, aplicación de parches, auditorías y registros.

German Porras

- **Interfaces inseguras y API. Las interfaces o API** (Interfaz de programación de aplicaciones, del inglés Application Programming Interface) permiten a los clientes administrar e interactuar con los servicios en la nube. Los modelos de servicios en la nube deben estar integrados en la seguridad,

y los usuarios deben ser conscientes de los riesgos de seguridad en el uso, implementación y monitoreo de dichos servicios.

- **Tecnología compartida.** Los proveedores de la Infraestructura como Servicio (IaaS) comparten la infraestructura para brindar los servicios de manera escalable. La mayoría de los componentes subyacentes que conforman esta infraestructura (por ejemplo, GPU, cachés de CPU) no ofrecen propiedades de aislamiento sustanciales en un entorno de múltiples usuarios, lo que permite a los atacantes identificar otras máquinas en las que podrían explotar vulnerabilidades en las aplicaciones de un cliente.

- **Amenazas internas.** Los actores maliciosos podrían ser los denominados insiders, es decir, colaboradores, contratistas u otros socios comerciales actuales/anteriores descontentos que tienen o tuvieron acceso a los recursos de la nube y podrían exceder o maltratar intencionalmente sus privilegios para comprometer la confidencialidad, integridad o disponibilidad de la información de la organización. Los actores maliciosos que tienen acceso autorizado a los recursos de la nube pueden abusar de sus permisos para comprometer la información disponible en la nube. Las amenazas incluyen pérdida de reputación, productividad y robo financiero.

- Diligencias deficientes. Los trámites o prácticas de gestión, generalmente administrativas, que se tiene que realizar para resolver un asunto pueden conllevar desconocimiento del entorno de nube del proveedor, lo que plantea riesgos en las responsabilidades operativas, como la seguridad, el cifrado, la respuesta a incidentes y más problemas de tipo contractual, de diseño, arquitectura, etc.

- Fallo en la cadena de suministro. Este riesgo surge debido a términos del uso incompletos y turbios, dependencia oculta creada por aplicaciones entre nubes, selección inapropiada de proveedores, falta de redundancia, entre otros. Los proveedores de la nube externalizan ciertas tareas a terceros. Por lo tanto, la seguridad de la nube es directamente proporcional a la seguridad de cada enlace y al grado de dependencia de terceros. Una interrupción en la cadena puede conducir a la pérdida de la privacidad e integridad de los datos, la falta de disponibilidad de los servicios, la violación del Acuerdo de Nivel de Servicio (SLA), las pérdidas económicas y de reputación que no satisfacen la demanda del cliente y la falla en cascada.

Alan Mai

Desastres naturales. Según la ubicación geográfica y el clima, los centros de datos pueden estar expuestos a desastres naturales como inundaciones, tormentas, terremo-

tos, etc. que pueden afectar los servicios en la nube.

¿Por qué es importante la seguridad en la nube?

Según Santiago Rosenblatt, CEO de Strike, en la nube es donde se encuentra toda o gran parte de la infraestructura de una empresa, donde hay datos de clientes, de pagos e incluso código fuente y aplicaciones. "Si algo de la nube es atacado exitosamente eso puede causar grandes problemas a las empresas ya que la información descrita anteriormente puede ser comprometida como así también los usuarios/clientes que interactúan en los sistemas/aplicaciones que se encuentran en la nube", sostiene.

En la actualidad los ciberataques son cada vez más sofisticados y requieren de habilidades y herramientas actualizadas para detenerlos.

Al respecto, Carolina Golia, principal architect de Google Cloud Argentina, plantea: "Cuando una organización se sube a la nube, su camino de migración inicia en el on-premise donde la gobernanza de los datos es 100% suya. Luego, conforme se van im-

Andrés Alexander

plementando diferentes servicios como el IaaS, PaaS y SaaS, el gobierno de la información se va repartiendo cada vez más entre el cliente y el proveedor de servicios en la nube, dándose así lo que se conoce como responsabilidad compartida. Es fundamental entonces la inversión del proveedor en seguridad, la forma en que diseña la infraestructura y cómo trabaja en la mitigación de riesgos".

Por su parte, Andrés Alexander, SVP Cluster Regional de Servicios y Cloud de BGH Tech Partner, agrega que cada medida de seguridad en la nube funciona para lograr uno o más de los siguientes objetivos: permitir la recuperación de datos en caso de pérdida de los mismos; proteger el almacenamiento y las redes contra el robo de datos malicioso; evitar los errores humanos o negligencias que causan la fuga de dato; y reducir el impacto de cualquier compromiso de datos o sistemas.

German Porras, Regional Sales Director MCLAC de Arcserve, destaca dos puntos:

El usuario final siempre será responsable de los datos, no existe ningún proveedor de servicios de nube que se responsabilice al 100% por la información, lo que lo convierte en el punto más crítico a considerar. Por ejemplo, si un usuario de un almacenamiento en la nube borra información intencional o accidentalmente, el servicio de nube no lo impedirá, puesto que este usuario tiene todos los permisos necesarios

Miguel Angel Mendoza

para manipular dicha información y por consecuencia, es su responsabilidad y no la del datacenter. De hecho, cada proveedor de servicios de nube, emite un documento conocido como "Modelo de responsabilidad compartida" donde especifica los alcances y responsabilidades del usuario y del data center según el servicio contratado.

Un servicio de nube no es invulnerable, requiere ciertas medidas de seguridad, protección y respaldo de información que permitan una recuperación rápida en caso de desastre. Una falsa expectativa que se ha venido generando en los últimos años es que al contratar un servicio de nube, el usuario se libera de toda la responsabilidad, por lo que se cometen muchos descuidos por desconocimiento.

"La velocidad y la escala de lo que una organización puede desplegar o poner a disposición en la nube significa que puede exponer más de sus activos y datos críticos más rápido y más fácilmente que nunca", agrega el ejecutivo de Tenable. "Las amenazas se mueven más rápido, las desconfiguraciones y los errores pueden afectar casi al instante, y como gran parte de esto suele estar orientado a Internet, el grupo potencial de atacantes que se aprovecharía de estos problemas es enorme. Las organizaciones simplemente no pueden ignorar las prácticas de seguridad sólidas en cada aspecto de su entorno de nube, desde el nivel de código y configuración hasta los diversos puntos finales que se despliegan para que los usuarios finales y los clientes interactúen".

¿Por dónde empezar la migración sin descuidar cuestiones de ciberseguridad?

"Al momento de planificar un proyecto de transformación digital, el proveedor de servicios en la nube tiene la misión de guiar la estrategia de seguridad de la empresa, cualquiera sea su tamaño o industria de la mano de expertos asesores que puedan informar, capacitar y recomendar herramientas específicas como la verificación en dos pasos, la encriptación de datos y gestión de vulnerabilidades, entre otras", informa Golia, de Google Cloud.

Rubén Belluomo

Carolina Golia

Según la expecialista, esto es especialmente importante porque en términos de ciberseguridad, ninguna red, dispositivo o usuario disfruta de confianza por sí mismo. La seguridad debe ser prioridad en cualquier iniciativa de negocio y el trabajo continuo garantizará minimizar los riesgos. "En este punto, desde Google Cloud recomendamos contemplar una estrategia de Zero Trust, que es un modelo de seguridad con el lema 'nunca confíes, siempre verifica'; lo

que significa que no se debe confiar en los dispositivos de forma predeterminada, sino validar previamente su verificación".

"Es importante definir de forma apropiada los usuarios, credenciales y permisos asociados, una mala asignación

Martín Malievac

Lo más importante al empezar la migración es seleccionar una empresa con experiencia en la nube y por ende en ciberseguridad.

de estos puede causar graves problemas que pueden ser aprovechados por ciber criminales", agrega Rosenblatt, de Strike. "Los sistemas operativos son una de las primeras etapas en instalación, por lo que debemos asegurarnos que el sistema utilizado tenga las actualizaciones de seguridad correspondientes.

Posteriormente, cada servicio que es agregado debe de tener la configuración correcta en cuanto a seguridad y permisos establecidos. Esto se complementa con un monitoreo y testeo constantes después de la migración de la infraestructura de la nube para detectar posibles problemas".

Según Jiménez, de IFX, la clave para obtener una migración limpia es contar con un aliado que tenga experiencia en las mismas y en analizar el negocio. A su vez, es necesario aprovisionar la infraestructura de cero, implementar aplicaciones y migrar información para no subir errores locales a la nube. Por último, se busca que el aliado posea servicios profesionales y conectividad propia, lo cual ayuda considerablemente a nivel de gastos y tiempos a la hora de realizar las mismas.

Adriana Jiménez

Rubén Belluomo, Gerente Comercial de Infor Cono Sur, coincide. "La capacidad de los proveedores líderes en la nube de cuidar los valiosos datos de los clientes requiere inversiones y recursos disponibles que la mayoría de las empresas poseen", sotiene.

Alexander, de BGH Tech Partner, comparte medidas que se pueden tomar para trabajar en ciberseguridad durante las migraciones:

Por su parte, destaca los siguientes riesgos:

- **Segmentación de datos de los usuarios:** las empresas deben asegurarse de que ningún otro cliente de su proveedor de servicios en la nube pueda acceder a sus datos. Ya sea que estén alojados en servidores segmentados o cuidadosamente codificados, asegúrese de que se aplique correctamente las medidas de segmentación adecuadas.

- **Cumplimiento legal de los datos**: mantener los datos de conformidad con los reglamentos internacionales como el GDPR es crítico para evitar importantes sanciones y daños a la reputación. Asegúrese de que las medidas como el enmascaramiento de datos y la clasificación de datos confidenciales sean una prioridad para su empresa
.

- **Controles de acceso de los usuarios:** los permisos de control pueden significar que el acceso de los usuarios se reduzca a un nivel que resulte incómodo. Sin embargo, ser restrictivo y trabajar de forma segura para encontrar un equilibrio puede ser mucho más seguro que permitir que los permisos sin asignar se filtren en su red.

- **Escalada cuidadosa de los sistemas de la nube**: con la rápida implementación de los sistemas de la nube, asegúrese de tomarse el tiempo necesario para revisar los sistemas de su empresa para obtener seguridad por encima de la comodidad. Los servicios en la nube pueden extenderse rápidamente hasta el punto de carecer de reglamento.

Por último, desde ManageEngine comparten 8 pasos para reforzar la seguridad de la infraestructura en la nube:

- **Detecta las desconfiguraciones de la nube**: las desconfiguraciones de la nube se producen cuando un usuario configura los servicios de la nube de forma incorrecta o los ajustes no proporcionan la seguridad adecuada para los datos almacenados en la nube. Por ejemplo, un cubo S3 de Amazon Web Services mal configurado podría dar lugar a la exposición de datos críticos al público. Las desconfiguraciones en la nube son la principal causa de las violaciones de datos

Nathan Wenzler

que se producen en ella. Y en la mayoría de los casos, la infracción se debe a una sola configuración errónea. Este reto se hace más difícil debido al modelo de responsabilidad compartida inherente a la computación en nube. Deben realizarse auditorías de seguridad periódicas y exhaustivas de la infraestructura en la nube para poder rectificar estos errores de configuración y detectar las vulnerabilidades. Una educación eficaz de los usuarios puede evitar las desconfiguraciones en la nube.

- **Realiza pruebas de penetración**: Siempre es mejor que te hackees a ti mismo antes de que un atacante lo haga por ti. Debes evaluar la seguridad de su infraestructura en la nube simulando un cibe-

rataque. Esto puede revelar vulnerabilidades y permitirle comprender la madurez de la seguridad de tu organización.

- **Adopta un marco de seguridad, como MITRE ATT&CK o NIST:** Un marco de seguridad, como el MITRE ATT&CK o el NIST, puede aportar la estructura necesaria para crear una estrategia de seguridad. Mientras que el marco ATT&CK le permite conocer los diferentes tipos de comportamiento de los adversarios de los que debe desconfiar, el marco NIST proporciona directrices eficaces para supervisar, identificar y recuperarse de los incidentes. La matriz ATT&CK, de hecho, enumera varias tácticas y técnicas que los adversarios pueden utilizar contra los servicios en la nube, como Azure AD, Office 365 y otros. Comprender lo que se ha observado en el mundo real permitirá a los analistas de seguridad defender mejor su infraestructura en la nube.

- **Obtén visibilidad de toda la actividad en la nube:** La mayoría de las organizaciones de todo el mundo han adoptado una estrategia multicloud en la que utilizan servicios en la nube de varios proveedores. Esto les permite distribuir sus activos, datos, aplicaciones y almacenamiento en múltiples entornos de alojamiento. Aunque una estrategia de múltiples nubes tiene sus ventajas, también dificulta la supervisión de lo que ocurre en la nube en cualquier momento. Es fundamental contar con una solución eficaz de gestión de eventos e información de seguridad (SIEM) que centralice la información obtenida de todas las plataformas en la nube y alerte a los analistas de seguridad en caso de que se produzca un percance. También deben utilizarse técnicas de detección de anomalías para observar cualquier actividad anormal realizada por los usuarios en cualquier host.

- **Minimiza el riesgo con una autenticación y autorización sólidas:** Implanta controles estrictos de gestión de identidades y accesos para garantizar que sólo las personas autorizadas tengan acceso a los recursos de la red. Debe seguirse el principio del mínimo privilegio, y también debe ponerse en práctica el modelo de seguridad Zero Trust, que reconoce la confianza como una vulnerabilidad. El acceso necesario, el acceso justo a tiempo y la autenticación multifactorial también deberían aplicarse para mejorar la seguridad

- **Bloquea las direcciones IP asociadas a comportamientos sospechosos**: El uso de las herramientas de inteligencia de amenazas adecuadas puede alertarte sobre ataques inminentes. Puedes conocer las URLs, IPs y dominios maliciosos que podrían dirigirse a la red de tu organización y tomar las medidas necesarias para bloquearlos.

- **Introduce un agente de seguridad de acceso a la nube**: Un agente de seguridad de acceso a la nube (CASB) es un mecanismo de control de políticas y visibilidad de la nube que se sitúa entre los usuarios de los servicios en la nube y las aplicaciones en la nube. Este software supervisa todas las actividades que los usuarios realizan en la nube y también aplica las políticas de seguridad. El CASB pue-

de ser un despliegue local o una aplicación de software como servicio. Un CASB puede ayudar a una empresa a supervisar toda la actividad de los usuarios en la nube. Cuando un CASB se integra con una solución SIEM, un analista de seguridad puede obtener un contexto más profundo en torno a la actividad de un usuario en la nube para una investigación.

- **Forma a tus empleados para que la seguridad sea una prioridad**: Los empleados deben ser formados regularmente para asegurarse de que no son víctimas de un compromiso de la cuenta. Puede ser necesario formar a tus empleados al menos una vez cada seis meses.
En ocasiones, dice el ejecutivo de ESET, debido a la celeridad para adoptar tecnologías que se consumen a través de la nube, se descuidan aspectos básicos de seguridad.

Gartner estima que para el año 2025, el 99% de los incidentes de seguridad relacionadas con la nube, serán responsabilidad de los clientes.

No hay dudas de que el uso de la nube cumple un papel muy importante en la innovación, porque plantea un entorno dinámico y ágil que permite reducir tiempos de prueba y de lanzamiento al mercado, y escalar rápidamente en caso de ser necesario. “Todo esto sin grandes inversiones iniciales”, aclara el responsable de Fortinet. “Pero, para lograr los objetivos de la migración a la nube, la seguridad es esencial. A medida que las infraestructuras se diversifican y se agregan nuevas tecnologías y herramientas se expande la superficie de ataque, y es justo ahí donde radica la importancia de contar con soluciones de ciberseguridad que permitan a las empresas tener en un solo lugar con visibilidad del estado de sus servicios así como definir políticas para administrar el riesgo de manera efectiva”.

mediaware MARKETING

Servicio 360
MARKETING Y VENTAS

Especializado en Tecnología y Consumo

- MEDIOS DE COMUNICACIÓN
- DISEÑO INTEGRAL
- MARKETING DIRECTO Y SOLUCIONES DIGITALES

Desarrolle su **PLAN** con **NOSOTROS**

mediaware.org

Cloud: ¿Por dónde empezar la migración sin descuidar cuestiones de ciberseguridad?

Por Alain Karioty, Vicepresidente de Netskope para LATAM

Alain Karioty

La nube se ha convertido en un importante campo de batalla, máxime, según las empresas transforman su infraestructura de TI tradicional y trasladan un mayor número de aplicaciones y datos a dicha infraestructura. El 79% de los usuarios suben, crean, comparten o almacenan regularmente datos en aplicaciones en la nube, lo que supone un aumento del 22% en los primeros cinco meses de 2022, según el último Cloud Threat Report de Netskope. Por ello, las organizaciones deben seguir una postura de seguridad que ofrezca una imagen completa de lo que ocurre con los datos y permita mantenerlos protegidos en la nube.

Pero las organizaciones no pueden proteger del mismo modo los datos cuando estos están dentro de la infraestructura corporativa, en un perímetro acotado y resguardado, que cuando están en movimiento, alejados de la protección de las herramientas corporativas clásicas. Necesitan desplegar una seguridad basada en la nube, centrada en los datos y capaz de seguir los datos en cualquier sitio web, servicio cloud, correo electrónico o aplicación privada.

La transformación digital obliga a las organizaciones a actualizar sus plataformas: es momento de renovar los gateways de acceso a Internet con una verdadera plataforma unificada SASE y ofrecer capacidades de Security Service Edge (SSE) de primera clase.

Cualquier tipo de empresa quiere aprovechar las ventajas de ahorro de costos, eficiencia operacional y mejora en las capacidades que supone irse a la nube. Sin embargo, a la hora de desplegar una estrategia en este sentido, las organizaciones deben tener claro qué datos y aplicaciones quieren trasladar a cloud y cuáles prefieren seguir manteniendo en las instalaciones y, en función de ello, definir el tipo de sistema (público, privado, híbrido) y el modelo de servicio más adecuado (IaaS, SaaS o PaaS). También y además de tener en cuenta los beneficios que ofrece la nube, es importante valorar los peligros que encierra, y actuar en consecuencia, no solo a nivel tecnológico, sino también, cuidando y propiciando aspectos como la formación y la colaboración a nivel interno y entre departamentos y adoptando un adecuado enfoque de seguridad, que sitúe la seguridad en la nube por diseño.

Tanto si la nube entra en la empresa a través de grandes proyectos de transformación empresarial, como si lo hace a través de una aplicación descargada en un dispositivo no gestionado, la ciberseguridad no puede ser ignorada por los equipos de seguridad.

Las organizaciones tienen que asumir que el stack de seguridad tradicional no es suficiente cuando los usuarios pueden estar en cualquier lugar y con cualquier dispositivo accediendo a recursos de la compañía, ya estén alojados en un datacenter propio

o en cloud pública, y por ello, la mejor aproximación de seguridad es la confianza cero, para así tener la certeza de quién y cómo acceden a los recursos de la empresa, incluyendo su información sensible. Una estrategia SASE -con sólidos principios de confianza cero- puede detectar lagunas de seguridad y automatizar una corrección, o instruir a los empleados cuando se identifican comportamientos inadecuados de alto riesgo, haciendo que el papel de los responsables de seguridad sea menos reactivo y más proactivo. Además, y frente a los SWG tradicionales, que ofrecen un punto de inspección solo web enfocado en el acceso y las defensas de protección de amenazas web, (pero que no incluye aplicaciones, servicios en la nube, protección de datos y DLP avanzados), SASE asegura defensas en tiempo real en la nube y es la mejor manera de garantizar que la nube siga siendo una fuerza positiva dentro de una organización.

Como complemento, las empresas deben sumar el sentido común a la tecnología de protección. La tecnología es solo una parte de la solución, pero los procesos y la educación son dos pilares adicionales necesarios. Si uno de los tres pilares fracasa, todo el sistema corre peligro. El despliegue de tecnología de vanguardia no es suficiente si falta una política de seguridad eficaz que incluya, entre otros aspectos, la gestión de activos, la aplicación de parches y el cambio de contraseñas.

Al final se trata de una simple cuestión práctica: si los datos están en la nube, allí debes llevar tu seguridad, y si lo haces confiando en una solución de seguridad nativa en cloud, mejor aún.

En Netskope mantenemos una postura de constante innovación, acorde con las demandas que nos llegan de nuestros clientes. También, a nivel tecnológico, intentamos ir un paso por delante, a fin de ofrecer una respuesta satisfactoria a los principales problemas a los que se enfrentan las empresas cuando quieren asegurar sus aplicaciones y servicios en la nube, con una política de reducción de riesgos, de costos y de uso de infraestructuras.

La Nube de Seguridad de Netskope ofrece SSE a través de una plataforma integral, nativa de la nube, de tecnologías que permiten la transformación digital sólida de la empresa y la conectividad segura del trabajo desde cualquier lugar utilizando las capacidades integradas de Agente de Seguridad de Acceso a la Nube (CASB), Gateway de Seguridad Web (SWG) y Acceso a la Red basado en Confianza Cero (ZTNA), con Aislamiento Remoto del Navegador (RBI) y Firewall en la Nube incluidos también.

De este modo, y con la actualización permanente de la plataforma Netskope Intelligent SSE, los clientes de Netskope pueden proteger los datos en SaaS, IaaS, aplicaciones privadas, web, correo electrónico y dispositivos de punto final desde una única solución de seguridad de datos convergente, aprovechando el aprendizaje automático, el análisis del comportamiento de usuarios y entidades (UEBA) y las capacidades de mitigación de amenazas internas para mejorar la eficacia, eficiencia y agilidad de la seguridad. Con estas funcionalidades los clientes obtienen grandes beneficios, siendo los más importantes la sencillez, la transparencia para el usuario, el ahorro de costes para la empresa y la capa de seguridad que posibilita tener información fehaciente al respecto de quién accede y a dónde accede.

La arquitectura de Netskope también incluye NewEdge, la nube privada de más rápido crecimiento y mejor conectada del mundo, que permite un acceso rápido y seguro desde cualquier lugar a los datos, aplicaciones y sitios web sin importar dónde residan. NewEdge tiene actualmente 8 puntos de presencia con capacidad de procesamiento local en América Latina, incluyendo Brasil.

Hacemos de la seguridad algo sencillo, eficiente y rentable. Y con esa idea seguimos avanzando.

Las empresas no se deben conformar con menos visibilidad y control en la nube

Por Miguel Llerena, Vicepresidente de Tanium Latinoamérica

Miguel LLerena

Aprovechar la nube es una prioridad estratégica para los departamentos de TI de la empresa. La computación en la nube representa una oportunidad de transformación para empresas para ganar agilidad y flexibilidad y su adopción continúa a un ritmo acelerado con el 84% de las empresas mencionando que su uso de la nube está aumentando y, al mismo tiempo, el 53 % de las empresas utilizan de 2 a 4 proveedores de la nube.

No obstante, la realidad es que los entornos de nube han obligado a reevaluar la ciberseguridad con un nuevo enfoque, los datos en la nube están siempre accesibles por internet y esto representa el mayor riesgo en esta forma de almacenar información, por lo que ahora el principal reto al que nos enfrentamos para proteger los datos de la nube es saber en donde están.
Cuando se accede a la nube desde un smartphone o computadora portátil la información puede almacenarse en diferentes dispositivos, esto es lo que hace difícil la seguridad, pues no solo se tiene que proteger la red de la organización, ya que esos dispositivos acceden a otras redes, por lo que están poniendo en peligro la información al volverse un nuevo blanco para un atacante.
En ese sentido, los proveedores de la nube permiten la agilidad a través de funciones como el escalado automático, que hace que sea muy fácil para las empresas escalar su capacidad. Si bien esta es una gran noticia para la agilidad, es importante que el departamento de TI se dé cuenta de que todas y cada una de las vulnerabilidades existentes también escalan con la infraestructura.

Es imperativo que las empresas sean estratégicas acerca de la migración a la nube, por lo que deben contemplar:

1. Identificar las aplicaciones correctas para migrar.

2. Cerrar las vulnerabilidades antes de pasar a la nube.

3. Tener una estrategia para las operaciones en curso a través de proveedores de nube que sea eficiente y promueva la seguridad.

Cuando la tecnología, que cambia tan rápidamente, converge con la redefinición del puesto de trabajo, resulta todavía más importante que las organizaciones tengan la capacidad de reaccionar y responder rápidamente. Tanium es una plataforma basada en la nube que está específicamente diseñada para abordar las causas fundamentales de los desafíos de TI y Seguridad rápidamente, al mismo tiempo que unifica esos equipos a través de su único panel.
Tanium puede proporcionar información crítica e identificar oportunidades para racionalizar y proteger la infraestructura antes de migrar a la nube. Lo que hace es evaluar y contener las amenazas (se realizan escaneos de activos no administrados para monitorearlos proactivamente y se implementa activamente la administración de endpoints; se escanean los

endpoints para asegurarse de que no existan vulnerabilidades en ninguno de ellos, y se investigua y reparan las exposiciones; y se asegura la higiene de los endpoints); identificar sinergias y sistemas de actualización (inventario de activos de hardware y software y su uso para identificar las aplicaciones correctas para migrar).

Después de la migración, Tanium proporciona la mejor plataforma para asegurar y administrar infraestructura basada en la nube. Tanium Core Platform, permite a los usuarios hacer preguntas simples o complejas sobre el estado actual de sus redes. Con respuestas de 15 segundos directamente desde todos sus endpoints, pueden tomar medidas inmediatas para proteger y administrar todos sus activos en la nube. Asimismo, con los módulos de productos de Tanium, pueden ampliar el valor de la plataforma Tanium al reemplazar las herramientas puntuales aisladas que no escalarán en la nube o no funcionarán en el entorno de la nube. Así, pueden simplificar su administración y reducir costos mientras aumentan la seguridad, la velocidad y la agilidad con un solo agente.

Finalmente, se debe entender que una nube no es otra cosa que un lugar centralizado de almacenamiento de información al que acceden múltiples usuarios ininterrumpidamente, toda esa información recopilada por unos cuantos proveedores de servicios importantes es el objetivo perfecto para un ciberataque, los delincuentes pueden atacar varias empresas a la vez que se encuentren en el mismo centro de datos y causar importantes filtraciones de información aprovechándose de la velocidad de innovación que permite la tecnología.

TANIUM

¡Vea y controle todos los puntos finales dondequiera que esté!

Administre, asegure y proteja su red con la única plataforma que ofrece datos de terminales de calidad, precisos y completos en los que confían las empresas más complejas y exigentes del mundo.

Tanium: el poder de la certeza

Prueba Tanium gratis

¿Cómo mejorar la productividad de los trabajadores remotos?

Menos productividad y la pérdida de tiempo representan una preocupación desde hace muchos años. Entre otras distracciones, se incluyen navegar en la Web, comprar en línea y comprobar el correo electrónico personal. Todo esto se suma a una posible pérdida significativa de la productividad. En un estudio citado en la revista Inc, se plantea que un empleado promedio dedica solo 2 horas y 53 minutos a actividades productivas. Estas preocupaciones se intensificaron cuando la pandemia forzó a las empresas a aumentar la adopción del trabajo remoto.

Termine con la incertidumbre

Antes de dañar el delicado vínculo de confianza entre el empleador y el empleado, debe asegurarse de los hechos. Debe saber en qué se desperdicia tiempo y quién lo desperdicia. Solo así podrá tomar las medidas adecuadas. Kaspersky Endpoint Security Cloud puede brindarle ayuda para lograrlo.

Además de detectar incursiones de malware, esta solución ofrece una gama de herramientas de supervisión que le permiten verificar qué sistemas se utilizan. Desde el panel de control central, puede acceder a un informe de supervisión en el que se muestra qué aplicaciones se utilizan en los dispositivos Windows conectados a su red.

El informe se divide en cuatro secciones (correo electrónico, uso compartido de archivos, redes sociales y otros) y allí puede ver exactamente a qué sitios web, aplicaciones y servicios acceden los empleados a través de los dispositivos de trabajo. Luego, puede seguir explorando para obtener más detalles, como quién visita cuentas de correo electrónico personales o navega por Facebook en mayor medida.

A partir de estas estadísticas, puede estimar con precisión cuánto tiempo de la empresa se pierde y quién lo desperdicia. Kaspersky Endpoint Security Cloud también asigna un índice de riesgo a cada uno de los servicios. Esto le permite verificar no solo cuánto tiempo de trabajo se pierde, sino también el grado de amenaza que estas actividades representan para la seguridad.

Tome medidas al respecto, de ser necesario

Gracias a la posibilidad de ver los cinco servicios principales que se utilizan (incluidos los no relacionados al trabajo), puede desarrollar una estrategia para abordar el problema. El equipo de TI por fin logrará comprender de forma precisa cómo se utilizan los recursos corporativos y los nuevos riesgos que crean los trabajadores remotos.

Luego, esta comprensión se podrá aplicar al desarrollo de soluciones prácticas. Respecto de donde se identificaron malos hábitos, el equipo puede planificar una capacitación para usuarios finales y ofrecerla con el fin de concientizar e impulsar seguridad en línea y prácticas de TI mejores. Por ejemplo, considere el almacenamiento en la nube.
Al descubrir que los usuarios dependen de servicios “gratuitos”, puede utilizar la oportunidad para recordarles que deben emplear la alternativa oficial que aprobó la empresa por su seguridad y su protección mejoradas. Lo mismo

aplica para los servicios de conferencias en video, redes sociales y correos electrónicos públicos. Todos ellos cuentan con versiones aprobadas oficiales.
El equipo de TI también puede establecer lazos con el departamento de Recursos Humanos para consultar el uso de los recursos y desarrollar una estrategia que alinee las políticas de TI con los objetivos de empleo. En conjunto, pueden desarrollar planes que mejoren la satisfacción de los empleados y protejan la empresa mediante el bloqueo de servicios y aplicaciones que se identifiquen como problemáticos o peligrosos.

Con un solo clic, puede bloquear servicios específicos para un único usuario. O bien, con la misma facilidad, puede crear y aplicar una regla que bloquee el acceso a sitios web y aplicaciones problemáticas para todos los usuarios. Si descubre que existe un sitio en particular del que se abusa de forma generalizada, como Facebook o Gmail, puede prohibirlo de inmediato.

¿Esto es controversial? En realidad, no. Bloquear el acceso a contenido en línea dentro de la oficina es bastante común. Mediante una encuesta breve, se descubrió que el 39 % de los empleadores bloquea los sitios de redes sociales en la red corporativa, el 30 % restringe el acceso a sitios de entretenimiento, el 27 % no permite las visitas a sitios de compras en línea y el 23 % de los empleados de bares no puede revisar sitios web deportivos. No es ilógico aplicar restricciones similares cuando se utilizan equipos de TI que son propiedad de la empresa durante las horas de trabajo, incluso para los usuarios que trabajan de forma remota.

Información más detallada y un mayor control

Gracias al análisis y los informes de uso automatizados, Kaspersky Endpoint Security Cloud le permite comprender mejor la TI de su empresa. Está diseñado para ser simple e intuitivo. Puede comprobar de forma rápida qué funciona y qué no, y planificar en función de ello.
Además, estos beneficios no se limitan a los endpoints remotos. Kaspersky Endpoint Security Cloud se puede utilizar para administrar el estado de la totalidad de la TI, incluidos los sistemas internos de la oficina. Esto significa que se pueden aplicar los mismos controles de acceso y presentación de informes sin necesidad de herramientas o inversiones adicionales. Puede utilizar los informes internos para tomar decisiones estratégicas importantes acerca de cómo impulsar la productividad dentro de la oficina y fuera de ella.

Los problemas de gestión del acceso pueden crear agujeros de seguridad

Los empleados que no tienen credenciales para acceder a los sistemas de la empresa, para realizar su trabajo, encuentran formas de sortear la burocracia que podrían dar lugar a brechas de seguridad.

Las restricciones de acceso destinadas a mantener la seguridad de los sistemas corporativos podrían tener el efecto adverso de hacer que los empleados encuentren soluciones y compartan sus credenciales con sus compañeros de trabajo. Así crean posibles vulnerabilidades de seguridad.

Así lo indica un estudio del proveedor de seguridad StrongDM, que recientemente encuestó a 600 trabajadores de TI, seguridad y DevOps. Descubrió que, en muchos casos, los usuarios encuentran métodos alternativos para acceder a sus contenedores, servicios en la nube y otras herramientas esenciales cuando no tienen acceso a través de los canales gestionados por la empresa.

El problema, según StrongDM, cuyo software proporciona al personal técnico acceso directo a la infraestructura, surge de un conflicto natural relacionado con la presión a la que se enfrentan los empleados para cumplir los plazos frente a la demanda de sistemas y servicios más nuevos y mejor mantenidos.

Mientras que los ejecutivos y gerentes presionan a los administradores de TI para que se actualicen a las últimas y mejores versiones de los servicios de red, así como para que implementen protocolos de acceso seguros y bien mantenidos, los usuarios finales —en particular los desarrolladores y los equipos de DevOps que dependen del código almacenado y los contenedores— necesitan acceder a esos recursos.

La encuesta descubrió que el 73% de los empleados necesita al menos 15 minutos al día para acceder a los datos que necesitan para el trabajo, y el 30% de los encuestados por StrongDM dijo que les lleva más de 30 minutos. Por otra parte, alrededor del 40% de los administradores encuestados afirmó que la simple vinculación de las nuevas herramientas con sus sistemas de gestión de acceso existentes lleva varios días -o semanas o meses para un porcentaje menor de organizaciones-.

> **“Si [los equipos] se encuentran con demasiados bloqueos en un proyecto, cuando se inicie el siguiente pueden crear las puertas traseras para evitar ralentizaciones, saltándose los protocolos adecuados para gestionar el**

Según Justin McCarthy, Cofundador y CTO, StrongDM, “si [los equipos] se encuentran con demasiados bloqueos en un proyecto, cuando se inicie el siguiente pueden crear las puertas traseras para evitar ralentizaciones, saltándose los protocolos adecuados para gestionar el acceso.”

Seguridad vs. plazos

Mientras los nuevos sistemas se integran con los controles de gestión de acceso, los usuarios fina-

les siguen teniendo plazos que cumplir y proyectos que realizar. Esto significa que se salen de los controles de gestión.

"Los empleados técnicos tienden a ser solucionadores de problemas por definición", señala el informe. "Así que, si no pueden acceder a las herramientas o soluciones que necesitan para cumplir un plazo o completar un proyecto, no es de extrañar que se les ocurran soluciones para resolver el problema".
Esas soluciones pueden incluir cosas como acceder directamente al servicio o sistema en la nube utilizando sus credenciales personales o incluso un inicio de sesión compartido; el 55% de los encuestados dijo haber visto a sus equipos mantener un método de acceso de puerta trasera, mientras que el 53% dijo haber compartido credenciales para servicios importantes.

Aquí es donde surge la mayor amenaza para la seguridad. Esas credenciales se vuelven entonces vulnerables a los hackers a través del robo de cuentas, el malware u otros trucos comunes.

El uso de credenciales robadas representó casi el 50% de los ataques en 2021 y estuvo presente en las brechas de terceros,

los ataques de phishing, los ataques a aplicaciones web básicas y las intrusiones en el sistema, según el Informe de Investigaciones de Brechas de Datos de Verizon 2022.

Los piratas informáticos podrían utilizar fácilmente las cuentas comprometidas para moverse lateralmente por la red y lograr tomas de posesión completas y robo de datos. Esto es especialmente peligroso para los desarrolladores y los equipos de DevOps, ya que crea además la posibilidad de ataques en la cadena de suministro contra otras empresas y redes.

"Las puertas traseras se crean cuando los equipos se frustran con retrasos y bloqueos. Si se encuentran con demasiados bloqueos en un proyecto, cuando se pone en marcha el siguiente pueden crear las puertas traseras para evitar ralentizaciones, saltándose los protocolos adecuados para gestionar el acceso", señaló McCarthy.

"Por otro lado, a veces las puertas traseras y las credenciales compartidas se producen al principio de los ciclos de desarrollo porque el equipo se mueve con rapidez, y el acceso abierto es más fácil que la aplicación de los controles adecuados", añadió.

En el mercado existen varios productos de gestión de identidades y accesos que pretenden abordar el equilibrio entre la seguridad y el acceso de los empleados, entre los que se incluyen productos de CyberArk, Microsoft e IBM, así como de proveedores más pequeños.

XDR: ¿Bendición para los equipos SOC o moda?

La industria de la seguridad ha evolucionado a lo largo de los años para combatir las amenazas cibernéticas nuevas y emergentes y, a medida que evolucionamos, se lanzaron nuevos productos para ayudar a los equipos de seguridad.

Algunos de estos productos han sido grandes avances, impulsados por el capital de riesgo y la innovación que fluye hacia la industria de la seguridad, pero muchos de ellos han sido una moda pasajera, ya que desaparecen tan pronto como el marketing en torno a ellos desaparece.

Un problema de demasiados

Se ha vuelto notablemente claro en los últimos años que los equipos de seguridad han estado luchando con un problema de abundancia: demasiados productos puntuales; demasiados datos repartidos entre terminales, redes y nubes; y demasiadas alertas en las que es humanamente imposible sumergirse. La mayoría de las veces, los equipos de seguridad han funcionado como el pegamento humano para unir herramientas dispares, pero eso requiere mucho tiempo y esfuerzo y puede cambiar con cualquier nueva versión. Este ha sido un gran desafío para la mayoría de los equipos de seguridad con escaso personal.

Ha sido difícil recopilar telemetría de seguridad en toda la empresa. Los equipos de seguridad han estado lidiando con este problema desde hace algún tiempo. XDR tiene como objetivo simplificar este problema al reunir la telemetría de puntos finales, redes, nubes, registros y usuarios en una consola unificada. Esto permite una detección más rápida de amenazas y mejores tiempos de investigación y respuesta a través del análisis de seguridad. Tiene el potencial de resolver el mayor desafío al que se enfrentan los equipos SOC en la actualidad. Pero la gran pregunta sigue siendo: ¿Puede XDR resolver este desafío?

> “Los equipos de seguridad han estado luchando con un problema de abundancia: demasiados productos puntuales; demasiados datos repartidos entre terminales, redes y nubes; y demasiadas alertas en las que es humanamente imposible sumergirse”

XDR: innovación o moda

Creo que la respuesta diferiría según la solución a la que nos refiramos. Permítanme elaborar un poco más: la tecnología está evolucionando, no todas las soluciones XDR son iguales: algunas han evolucionado a partir de soluciones EDR, algunas han evolucionado a partir de soluciones SIEM y similares. Los principales proveedores de seguridad esperan subirse al carro de XDR y promocionar su solución como la mejor.

Los analistas de la industria están realizando una amplia investigación sobre este tema. Jon Oltsik, de ESG, recientemente escribió un blog sobre este tema y mencionó sus observaciones sobre XDR. Algunos de los puntos clave destacados por Jon:

- Las soluciones XDR ganarán o perderán según el análisis avanzado, lo que enfatiza el papel importante que desempeñarán la IA y el ML.
- XDR tiene que ver con la respuesta automatizada llave en mano, enfatizando la importancia de construir y personalizar playbooks de respuesta.
- El marco MITRE ATT&CK es la lengua franca de XDR, destacando cómo una solución XDR puede ayudar a poner en funcionamiento el marco MITRE.
- La "apertura" es fundamental, y se centra en el hecho de que la herramienta XDR debe interoperar con otras herramientas.

Abrir XDR

Dado que el tema está evolucionando, los principales analistas de la industria tienen diferentes perspectivas sobre este tema. Si bien Jon cree que XDR se trata de generar mejores resultados para los equipos de seguridad, Allie Mellen, de Forrester Research, enfatiza que una solución XDR debe ser una extensión de la solución Endpoint Detection and Response (EDR). Si bien los puntos de vista de los analistas sobre el tema varían ampliamente, los analistas están de acuerdo en que las soluciones deben ser componibles e integrables.

Según la investigación de Forrester, los equipos de seguridad dan prioridad a las herramientas con capacidades de integración. Por lo tanto, tanto el XDR nativo como el XDR híbrido deben admitir la integración con herramientas de seguridad de terceros de alguna manera; simplemente no hay otra opción.

Claramente, la comunidad de analistas está de acuerdo en que el éxito (o el fracaso) de XDR depende de si se basa en código abierto y estándares abiertos, y de cómo la herramienta/producto XDR interactúa con otros productos. Y tiene sentido: dado que XDR tiene como objetivo reunir las operaciones de seguridad en una sola consola, es posible que no sea posible hacerlo si XDR no interopera con otros productos de seguridad para un flujo de trabajo unificado.

Proyectos OCA y habilitación de XDR

Puede ser extremadamente difícil crear un marco para que las herramientas de seguridad interoperen si solo un proveedor estuviera liderando este esfuerzo. Existe una alta probabilidad de que los propios intereses financieros y competitivos del proveedor tengan prioridad sobre los desafíos de 'interoperabilidad' pura. Por lo tanto, es imperativo que el desarrollo sea liderado por una organización neutral, que lo haya hecho para otros proyectos de TI o Seguridad y tenga la experiencia técnica y arquitectónica necesaria para asumir un proyecto de esta magnitud.

Una de esas organizaciones es Open Cybersecurity Alliance (OCA). Formada bajo los auspicios de OASIS Open, esta organización tiene como objetivo fomentar la colaboración entre proveedores, organizaciones y profesionales de la seguridad e impulsar la interoperabilidad de la seguridad. Open Cybersecurity Alliance está construyendo un ecosistema abierto donde los productos de ciberseguridad interoperan sin necesidad de integraciones personalizadas. Usando estándares y prácticas desarrollados por la comunidad, OCA está simplificando la integración a lo largo del ciclo de vida de la amenaza. En un blog reciente sobre las principales tendencias tecnológicas, Gartner se refiere a una arquitectura de malla de ciberseguridad, que se alinea estrechamente con el trabajo en curso en OCA.

.

Los proyectos actuales de OCA incluyen:

Seguridad proactiva

- Stix Shifter: para permitir que los datos se normalicen en todos los dominios de seguridad para un análisis de seguridad integral
- Ontología OCA: para habilitar el intercambio de datos en tiempo real y la orquestación entre proveedores
- Kestrel: para proporcionar una abstracción para los cazadores de amenazas y centrarse en qué cazar en lugar de cómo cazar

Además, para combatir el creciente panorama de amenazas, OCA ha lanzado recientemente nuevos grupos de trabajo que incluyen:

- Arquitectura unificada de OCA y confianza cero
- Indicadores de Comportamiento

El éxito o fracaso de XDR depende de si está abierto

No hay duda de que hay mucho entusiasmo por XDR en la industria de la seguridad. Es posible que estemos cerca del 'pico de expectativas infladas', según Gartner Hype Cycle. Si bien puede tomar un tiempo alcanzar la 'meseta de productividad', habrá algunas soluciones XDR que cumplan de manera efectiva los requisitos de reunir la telemetría en la red, la aplicación, las nubes, etc., mientras que puede haber otros para quienes esto simplemente sigue siendo una lista de deseos.

> "Es imperativo que el desarrollo sea liderado por una organización neutral, que lo haya hecho para otros proyectos de TI o Seguridad y tenga la experiencia técnica y arquitectónica necesaria"

Lo que separará a los ganadores de los perdedores es cómo abrir XDR, para que pueda integrarse fácilmente con la infraestructura existente y pelear la buena batalla de vencer a los malos y proteger a nuestros clientes y los datos de los clientes de los clientes.

¡Saludos a un Open XDR que podría modernizar el SOC!

1. *Crédito: Open Cybersecurity Alliance*

Las Universidades contraatacan

El campus de Boulder de la Universidad de Colorado fue objeto de un ataque de ransomware en mayo pasado. El mensaje, enviado por correo electrónico a miles de estudiantes y empleados en el campus de Boulder de la Universidad de Colorado la semana pasada, fue alarmante.

Su información personal, incluidas direcciones, números de teléfono, números de seguro social, informes de progreso académico y documentos financieros, había sido robada, y su universidad se negaba a cooperar con las demandas de extorsión. Como resultado, los datos comenzaron a publicarse en la Dark Web, el oscuro canal trasero de Internet donde acechan los ciberdelincuentes

En otras partes del país, los estudiantes y empleados de al menos otras nueve universidades estaban recibiendo advertencias similares. Los campus son parte de un número creciente de extorsiones y ataques de ransomware que el FBI ha estado rastreando desde marzo de 2020, cuando la pandemia de Covid-19 se apoderó de los EE. UU. Los ciberdelincuentes se han aprovechado de las circunstancias únicas de la pandemia para redoblar sus demandas.

"El cambio rápido al aprendizaje a distancia y el trabajo remoto aumentó drásticamente la superficie de ataque", dijo Paul B. Davis, quien asesora a instituciones de educación superior sobre amenazas de seguridad cibernética para Gallagher, un corredor de seguros global. Dijo que sus clientes han informado un aumento significativo en la cantidad y la gravedad de los ataques cibernéticos desde que comenzó la pandemia. "Muchos más dispositivos iniciaban sesión de forma remota, y no todas las instituciones tenían los controles adecuados para administrar el acceso".

En marzo pasado, el FBI emitió una advertencia que detalla cómo los piratas informáticos se infiltran en las redes vulnerables utilizando un software malicioso, o malware, que cifra los datos en una computadora, dejándola inutilizable. Los ciberdelincuentes pueden amenazar con destruir los datos o divulgarlos públicamente a menos que un campus o una persona pague.

> "Los campus son parte de un número creciente de extorsiones y ataques de ransomware que el FBI ha estado rastreando desde marzo de 2020"

A veces lo hacen. En agosto, la Universidad de Utah pagó más de U$S 450.000 para evitar que se publicara información confidencial en Internet. Aunque el FBI desaconseja encarecidamente el pago de un rescate, la advertencia de marzo decía que entiende "que cuando las víctimas se enfrentan a la incapacidad de funcionar, se evalúan todas las opciones para proteger a los accionistas, empleados y clientes".

Sólo una parte del campo minado

Al igual que muchas instituciones, el sistema de la Universidad de Colorado toma precauciones adicionales al transferir archivos grandes y conjuntos de datos que contienen información de identificación personal protegida por leyes de privacidad. Pero a fines de enero, se enteró de que incluso esos pasos se quedaron cortos cuando el software de terceros que estaba usando, del proveedor global de nube Accellion Inc., fue pirateado. Se expusieron más de 300.000 registros de la universidad, la mayoría en el campus de Boulder, pero algunos en el campus de Denver. Estos incluyeron calificaciones y expedientes académicos de los estudiantes, tratamientos y diagnósticos médicos, y una pequeña cantidad de números de Seguro Social. Otras universidades afectadas por el ataque masivo incluyeron la Universidad de Miami, la Universidad de Maryland en Baltimore, la Universidad Yeshiva, Harvard Business School, la Universidad de California en Davis y la facultad de medicina de la Universidad de Stanford.

Colorado cerró inmediatamente su servicio de transferencia de archivos y cambió a una herramienta diferente. La universidad ofreció monitoreo gratuito de crédito e identidad y consulta sobre fraude mientras se sumergía profundamente en la violación de datos. (Accellion emitió un comunicado en marzo que decía que había cerrado "todas las vulnerabilidades conocidas" y que no se habían encontrado nuevas).

Siguiendo el consejo del FBI, la universidad se negó a ceder a la demanda de 17 millones de dólares. "No hay garantía de que los ciberdelincuentes cumplan sus promesas de no publicar información", dijo la universidad en un comunicado. "Tampoco hay seguridad de que no intentarán más extorsiones"

.

Desafortunadamente, las amenazas cibernéticas son solo una parte del campo minado que atraviesan las universidades hoy en día, dijo Ken McConnellogue, un portavoz de Colorado.

"Este es un ataque tan grave como el que hemos tenido, que afectó a una gran parte de nuestra comunidad universitaria", dijo. A los investigadores les preocupa que los datos intelectuales se vean comprometidos, a los estudiantes les preocupan las calificaciones y los números de la Seguridad Social. Aunque el software que fue pirateado pertenecía a un tercero, "la gente espera que seamos tan responsables como podamos con sus datos". La universidad ha acelerado los esfuerzos para reforzar las salvaguardas, así como para "llevar a primer plano la conciencia cibernética".

> "Desafortunadamente, las amenazas cibernéticas son solo una parte del campo minado que atraviesan las universidades hoy en día"

El hecho de que se incluyeran menos de 20 números de Seguro Social en el tesoro de datos a los que accedieron los piratas informáticos se debe a la decisión del sistema universitario hace años de solicitar

identificaciones de estudiantes y empleados en lugar de números de Seguro Social en formularios que requieren identificación personal, según McConnellogue.

'Desencadenantes emocionales'

Desde 2005, los distritos escolares y las universidades han sufrido más de 1300 filtraciones de datos, lo que ha afectado a más de 24,5 millones de registros, según un informe de 2020 del sitio web Comparitec. Las universidades representaron las tres cuartas partes de las infracciones educativas, siendo California y Nueva York los puntos críticos más importantes.

En las universidades, el 43 por ciento de las intrusiones fueron atribuidas a delincuentes cibernéticos que se abrieron paso, mientras que otro 27 por ciento de las infracciones ocurrió cuando las instituciones filtraron información accidentalmente. Eso podría suceder si alguien adjunta por error datos de identificación personal del estudiante a un correo electrónico. Las computadoras portátiles perdidas o robadas y otros dispositivos portátiles representaron otro 15 por ciento.

> "Los ciberdelincuentes se han aprovechado de las preocupaciones financieras y de salud de las personas enviando mensajes de correo electrónico que parecen auténticos"

Los problemas se han intensificado durante el último año. "Una de las cosas que ha hecho la pandemia es que a los piratas informáticos les resulta mucho más fácil lanzar ataques de phishing", dijo Frank Quinn, quien dirige el equipo de respuesta a violaciones en los Estados Unidos para Beazley, una aseguradora cibernética. Estos correos electrónicos pretenden ser de empresas de renombre para solicitar a las personas que revelen información personal como contraseñas y números de tarjetas de crédito.

Los ciberdelincuentes se han aprovechado de las preocupaciones financieras y de salud de las personas enviando mensajes de correo electrónico que parecen auténticos promocionando la disponibilidad de vacunas o los pasos para acceder a la asistencia relacionada con Covid. "Encuentran desencadenantes emocionales que pueden ser ganchos convincentes", dijo Quinn. Las personas que han sido entrenadas para evitar escrupulosamente hacer clic en enlaces de fuentes desconocidas no siempre son tan cuidadosas cuando revisan correos electrónicos en sus teléfonos celulares, agregó.

Las tarifas de los seguros para la protección de la seguridad cibernética se han disparado entre un 30 y un 65 por ciento para sus clientes desde que comenzó la pandemia, dijo Davis. Y para obtener un seguro ahora, es posible que las universidades deban demostrar que han tomado más precauciones, como exigir la autenticación de dos factores y educar a todos los usuarios sobre cómo evitar los ataques de phishing.

En algunos casos, la aseguradora conectará el cam-

pus con un negociador de rescate, dijo Quinn. Algunos piratas informáticos "son muy hábiles y se centran extrañamente en el servicio al cliente, por lo que puede obtener un buen resultado si se ve obligado a pagar", dijo. Otros, los torpes aficionados, "pueden estar usando un software que en realidad no entienden bien". Si hay un problema con el proceso de descifrado, es posible que no puedan cumplir con su parte del trato, incluso si una universidad paga.

Los expertos ofrecen una variedad de consejos para ayudar a los campus a mantenerse un paso por delante de los piratas informáticos:

Asegúrese de que el acceso remoto a la red esté bien protegido. Los estafadores están constantemente escaneando la web, listos para saltar cuando las puertas están abiertas, incluso por un momento. Las redes privadas virtuales son una forma de mantener alejados a los intrusos.

- Siga una estrategia de respaldo 3-2-1 de tener tres copias de datos en dos medios diferentes, con una copia fuera del sitio para recuperación ante desastres. Practique la recuperación de datos para que pueda hacerlo rápidamente.

- Utilice la autenticación multifactor, que requiere al menos dos formas de identificación para iniciar sesión, cuando sea posible. No confíe solo en un nombre de usuario y contraseña

- Reduzca la cantidad de personas que tienen autorización de seguridad elevada para acceder a sitios confidenciales

- Capacite a los estudiantes y empleados para evitar hacer clic en correos electrónicos de phishing.

Un tesoro de datos

El mes pasado, cuando los estudiantes se dirigían a los exámenes finales, la red de la Universidad de Texas en El Paso se cayó repentinamente. Una publicación en Facebook informó a los estudiantes y empleados de "una intrusión no autorizada y potencialmente maliciosa" en la red del campus. "Siguiendo nuestros procedimientos estándar, apagamos de inmediato todos los sistemas de nuestro campus y hemos estado trabajando durante todo el fin de semana para probar y volver a poner en línea cada sistema después de revisarlo a fondo", dijo.

Cuando los estudiantes quedaron desconectados, decenas de mensajes de pánico comenzaron a aparecer en las redes sociales. Mañana era la fecha límite para un examen final. Vencía un trabajo de investigación y un estudiante no podía acceder a la biblioteca ni comunicarse con un profesor. ¿Los profesores retrasarían sus exámenes o les darían prórrogas? Las facturas estaban vencidas y el centro de pago en línea no funcionaba. ¿Se eximirían los cargos por pago atrasado?

Los miembros del personal de la universidad se apresuraron a responder preguntas mientras los sistemas se probaban y restauraban metódicamente. En una actualización reciente, la presidenta de la universidad, Heather Wilson, aseguró a todos que no había indicios de que los datos de identificación personal se hubieran visto comprometidos. Aunque se esperan más actualizaciones, "es posible que nunca sepamos exactamente dónde ocurrió la

1. (Crédito: University of Boulder, colorado)

intrusión o cómo sucedió", escribió. "Cada mes, al igual que otras instituciones de nuestro tamaño y alcance, nuestro equipo de Recursos de Información mitiga con éxito una gran cantidad de vulnerabilidades de software y evita unas 20.000 amenazas de seguridad externas a nuestra red. Continuamos tomando medidas para mejorar la seguridad de nuestros sistemas frente a las amenazas de ciberseguridad en evolución". El siguiente paso será prepararse para los nuevos requisitos de ciberseguridad que el gobierno federal está imponiendo a las universidades de investigación que fortalezcan y documenten los procedimientos de protección de datos, agregó Wilson.

También en Texas, la Universidad Prairie View A&M sufrió un gran ataque cibernético en febrero que inmovilizó todas las redes principales, lo que obligó a la universidad a cancelar las clases y cerrar las clases en línea.

La cantidad de datos confidenciales que recopilan las universidades y las empresas con las que trabajan solo ha aumentado durante el último año. Los datos de salud se rastrean cuidadosamente y la densidad de la multitud se descifra a través de videovigilancia y sensores montados en la pared. Los supervisores remotos escanean las caras y los gestos de los estudiantes en busca de signos de trampa. Todo se suma a un tesoro de datos que algunos ciberdelincuentes podrían considerar maduros para recoger.

Mapeo de los Top Ten de OWASP a Blockchain

Howard Poston

Por Howard Poston

La lista de las diez principales vulnerabilidades de las aplicaciones web del OWASP es uno de los recursos de ciberseguridad más conocidos y utilizados que existen. Esta lista está diseñada para destacar las vulnerabilidades de las que los desarrolladores de aplicaciones web deben ser más conscientes.

El Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP por sus siglas en inglés) es una fundación sin ánimo de lucro que se dedica a mejorar el estado de la seguridad del software. Su objetivo es proporcionar información, incluyendo listas detalladas de vulnerabilidades comunes y recursos, tales como herramientas de prueba y aplicaciones deliberadamente vulnerables, para ayudar a educar a los desarrolladores sobre los posibles problemas de seguridad que podrían existir en su código.

Blockchain es una tecnología que está ganando adopción generalizada rápidamente; sin embargo, las normas de seguridad y los recursos similares a la lista de OWASP no están ampliamente disponibles. Aunque existen Top Ten Lists similares a la de OWASP, incluyendo una creada por el Proyecto de Seguridad de Aplicaciones Descentralizadas (DASP) [1], son específicas para las vulnerabilidades de los contratos inteligentes y no tienen en cuenta todo el ecosistema de la cadena de bloques.

Este estudio mapea las vulnerabilidades listadas en la última versión de la Lista de los Diez Principales de OWASP a la tecnología blockchain. Los sistemas de cadena de bloques y las integraciones externas comunes, como los exploradores de bloques basados en la web y el software de billetera, se examinan en busca de las mismas vulnerabilidades que aparecen en la Lista de los Diez Principales de OWASP.

> “Este estudio mapea las vulnerabilidades listadas en la última versión de la Lista de los Diez Principales de OWASP a la tecnología blockchain.”

La lista de OWASP y Blockchain

En el momento de la publicación, la lista de las diez principales vulnerabilidades de aplicaciones web más reciente de OWASP era la versión publicada en 2017 [2]. Esta versión de la lista llamaba la atención sobre los siguientes diez problemas comunes de seguridad de las aplicaciones web:

Inyección
Autenticación rota
Exposición de datos sensibles
Entidades externas XML (XXE)
Control de acceso roto
Desconfiguración de la seguridad
Cross-Site Scripting (XSS)
Deserialización insegura
Uso de componentes con vulnerabilidades conocidas
Insuficiente registro y monitoreo
das se ejecuten en las computadoras, evitando así que el ransomware funcione.

Aunque esta lista estaba destinada a los desarrolladores de aplicaciones web, muchas de estas vulnerabilidades son igualmente aplicables a la tecnología blockchain.

Inyección

En un ataque de inyección, un atacante se aprovecha de una mala "higiene" de la entrada del usuario para atacar un sistema. Si el desarrollador del software no maneja apropiadamente esta entrada, puede ser manipulada de manera que permita ejecutar comandos no autorizados. Por ejemplo, si no se limpian las entradas SQL, un usuario puede saltarse la autenticación y ejecutar consultas no autorizadas contra la base de datos.

Una mala desinfección de las entradas es sin duda un problema potencial en la tecnología blockchain.

> "Una mala desinfección de las entradas es sin duda un problema potencial en la tecnología blockchain."

Antes del lanzamiento de la red principal de EOS los investigadores de Qihoo 360 informaron de una vulnerabilidad en la función de análisis de contratos inteligentes de EOS que permitía una escritura fuera de los límites del búfer [3]. Los investigadores desarrollaron una prueba de concepto en la que la vulnerabilidad les permitía salir de la sandbox de EOS y lanzar un shell inverso en la máquina infectada. Si esta vulnerabilidad se hubiera explotado en una red en funcionamiento, podría haber permitido al atacante comprometer cada nodo de la red, al ejecutar el contrato inteligente malicioso una vez incluido en un bloque válido.

Autenticación rota

La autenticación rota es una vulnerabilidad general que se refiere a cualquier problema en la implementación de un mecanismo de autenticación en una aplicación. Estos problemas podrían permitir a un atacante hacerse pasar por un usuario legítimo de forma de forma temporal o permanente.

La correcta implementación de la funcionalidad de autenticación es vital para el buen funcionamiento del sistema blockchain, y el amplio uso de la criptografía de clave pública significa que existe una gran superficie de ataque.

La criptomoneda LISK es un buen ejemplo de cómo los descuidos de diseño permitieron un ataque a la autenticación en una cadena de bloques. En LISK, la

dirección de un usuario en la cadena de bloques se obtiene haciendo un hash de su clave pública y truncando el resultado a 64 bits [4]. Este método de hash y truncamiento para generar direcciones es común; sin embargo, la corta longitud de las direcciones LISK y el hecho de que las direcciones no estén inmediatamente vinculadas a las claves públicas hace que LISK sea vulnerable a los ataques.

Las direcciones en LISK sólo se vinculan a las claves públicas cuando un usuario inicia una transacción, ya sea enviando un valor fuera de la cuenta o votando un delegado. Como resultado, muchas cuentas que sólo habían recibido valor eran vulnerables a ataque. Un atacante sólo tiene que realizar 264 operaciones de generación de claves para encontrar un par de claves privadas/públicas que se asigne a una dirección determinada. Apuntar a cualquiera de las M direcciones disminuye la complejidad de encontrar cualquier coincidencia por un factor de M. Este ataque es definitivamente factible, y algunas cuentas vulnerables tenían millones de dólares.

Exposición de datos sensibles

La exposición de datos sensibles es una vulnerabilidad que se explica por sí misma. Si una aplicación contiene datos valiosos que deben mantenerse secretos, estos datos deben estar debidamente protegidos.
La tecnología blockchain es en gran medida propensa a esta vulnerabilidad debido a la falta de comprensión de la tecnología.
La cadena de bloques es inmutable, lo que significa que cualquier dato almacenado en ella no puede ser eliminado (sin el control de cada nodo en la red).

La mayoría de las cadenas de bloques también son públicas, lo que permite a cualquiera descargar y almacenar una copia completa de los datos del ledger. A corto plazo, esta combinación hace que las cadenas de bloques sean vulnerables a los esfuerzos de minería de datos. Muchas organizaciones se especializan en la minería de la cadena de bloques en busca de datos públicos que puedan agregarse para obtener información útil. Estos datos pueden ser utilizados para la aplicación de la ley, el espionaje corporativo y otros fines.

A largo plazo, toda la criptografía es rompible. La computación cuántica está en el horizonte y, aunque no romperá la tecnología blockchain, permitirá descifrar cualquier dato almacenado en la blockchain que esté cifrado con algoritmos clásicos de encriptación asimétrica. Si los datos deben mantenerse privados para siempre —como los datos personales protegidos por leyes de privacidad como el GDPR o HIPAA— nunca deberían almacenarse en una blockchain pública, ni siquiera en un formato cifrado.

Entidades externas XML (XXE)

Las entidades externas XML (XXE) son vulnerabilidades basadas en referencias a entidades externas dentro de documentos XML. El riesgo de éstas es que los archivos internos sensibles almacenados en el servidor web pueden ser accesibles utilizando estas referencias. Dado que blockchain no se basa en XML, esta vulnerabilidad no es aplicable en general a esta tecnología.

Control de acceso roto

El control de acceso roto es similar a la autenticación rota, pero algo distinto. En la autenticación rota, un atacante se hace pasar por un usuario no autorizado, mientras que, en el control de acceso roto, un usuario malicioso obtiene acceso no autorizado a funcionalidad protegida.

> “La mayoría de las cadenas de bloques también son públicas, lo que permite a cualquiera descargar y almacenar una copia completa de los datos del ledger.”

Los mecanismos de control de acceso mal implementados son una de las principales vulnerabilidades observadas en los contratos inteligentes de Ethereum. El monedero multi-firma basado en el contrato inteligente Parity es conocido por haber sido explotado dos veces debido a vulnerabilidades de control de acceso. En ambos casos, estos contratos tenían una función diseñada para permitir al propietario llamarla y reclamar la propiedad, pero no comprobaba que sólo se llamara una vez.
En el primer ataque, un atacante llamaba a esta función para tomar el control de los contratos de Parity wallet y vaciarlos de los fondos almacenados. En el segundo, se atacó una función similar en un contrato de biblioteca utilizado por todos los monederos de Parity. El atacante tomó el control y luego autodestruyó la función, haciendo que todas las billeteras de Parity fueran inutilizables y causando que alrededor del 1% de todo el Ether se perdiera para siempre [5].

Desconfiguración de la seguridad

La desconfiguración de la seguridad es otra vulnerabilidad general de OWASP. Se refiere al uso de configuraciones inseguras por defecto o el uso de configuraciones que hacen que el sistema sea vulnerable a los ataques. Como tal, es uno de los tipos de vulnerabilidades más comunes. Las cadenas de bloques se implementan como software que se ejecuta en las máquinas de los clientes en una red peer-to-peer, por lo que tiene sentido que las

desconfiguraciones de seguridad puedan afectar a la seguridad. En un caso, los usuarios de un monedero de Ethereum configuraron sus monederos para escuchar y aceptar comandos externos a través de RPC (puerto 8545). Los atacantes que se aprovecharon de esta vulnerabilidad fueron capaces de robar 20 millones de dólares en Ether [6].

> “La desconfiguración de la seguridad es otra vulnerabilidad general de OWASP. Como tal, es uno de los tipos de vulnerabilidades más comunes.”

Cross-Site Scripting (XSS)

Un sitio web es vulnerable a un ataque de cross-site scripting si incluye datos no confiables dentro de una página web sin validar y sanear primero. Esta vulnerabilidad permite a un atacante ejecutar scripts dentro del navegador de la víctima.

Las vulnerabilidades de cross-site scripting pueden afectar a los sistemas de blockchain de un par de maneras diferentes. Las vulnerabilidades XSS han sido explotadas en otro software para permitir la ejecución de malware de criptominería en la computadora de la víctima. Las vulnerabilidades de cross-site scripting pueden afectar a la seguridad de la cadena de bloques más directamente si existen en los exploradores de blockchain. Estos muestran datos de transacciones, que son datos no fiables que pueden estar bajo el control de un atacante. Si existe una vulnerabilidad XSS en un explorador de blockchain y un monedero combinados, la explotación del explorador podría permitir el acceso a la clave privada de un usuario y el control de su cuenta [7].

Deserialización insegura

La serialización se utiliza habitualmente para la transmisión de conjuntos de datos a través de una red. Si el código de deserialización está implementado incorrectamente, una transmisión maliciosa podría permitir a un atacante explotar una máquina vulnerable.

Aunque no se ha informado de ningún ataque que se aproveche de las vulnerabilidades de la deserialización, los sistemas de blockchain suelen utilizar serialización para la transmisión de transacciones. Dado que los datos de las transacciones están bajo el control de usuarios (potencialmente maliciosos), un código de deserialización vulnerable podría llevar a comprometer los sistemas de blockchain.

Componentes con vulnerabilidades conocidas

La mayor parte del software se construye sobre o reutiliza otro software. Si estas dependencias contienen vulnerabilidades, el software que las utiliza puede ser explotado por los atacantes que se dirigen a estas vulnerabilidades. El hackeo de Equifax es un gran ejemplo de cómo el código vulnerable de terceros puede tener impactos significativos en la seguridad de una organización.

La reutilización de código en los contratos inteligentes de Ethereum es incluso más común que en las aplicaciones que no son de cadena de bloques. De hecho, menos del 10% de los contratos inteligentes de Ethereum no reutilizan el código [8]. Dado que muchos programadores de contratos inteligentes tienen poca experiencia con la tecnología y los riesgos asociados, esto significa que muchos contratos inteligentes en la blockchain de Ethereum contienen vulnerabilidades conocidas debido a la reutilización de código.

Registro y supervisión insuficientes

Aunque los procesos de desarrollo seguros son importantes, sólo son la mitad de la batalla. Una vez que se ha desplegado un sistema también es importante registrar y supervisar los eventos del sistema para detectar anomalías que puedan indicar un ataque. Si no se hace esto, el sistema puede ser vulnerable a la explotación a través de vectores de ataque que se pasaron por alto durante el proceso de diseño.

La cadena de bloques crea un registro inmutable de las acciones realizadas en el sistema, lo que la hace ideal para el registro. Sin embargo, aunque el registro es estupendo, es inútil si nadie lo mira. Muchos contratos inteligentes en la cadena de bloques son “fire and forget” y no son supervisados por sus propietarios, lo que los hace potencialmente vulnerables a la explotación sin ser detectados.

Conclusión

Actualmente, blockchain carece en gran medida de orientación y recursos de seguridad específicos. Sin embargo, la tecnología blockchain no es diferente de la infraestructura de TI tradicional, y muchas de las vulnerabilidades que existen en otros entornos también se aplican a la cadena de bloques. De las diez vulnerabilidades enumeradas en la versión actual de la lista de los diez principales de OWASP, sólo una no se adapta bien a blockchain porque ésta no utiliza el formato XML.

> “Una vez que se ha desplegado un sistema también es importante registrar y supervisar los eventos del sistema para detectar anomalías que puedan indicar un ataque.”

El desarrollo de normas y orientaciones de seguridad específicas para blockchain debería ser una prioridad a medida que el uso de estas plataformas para almacenar y procesar información sensible. Sin embargo, mientras tanto, la adaptación de los frameworks existentes al ecosistema de la cadena de bloques permite obtener información útil sobre la seguridad.

Hacha y bisturí: el fin del backup

El aterrador éxito del ransomware se debe a una malvada combinación de ingeniería social y de software. Las mentes retorcidas que están detrás del malware entienden a las personas tan profundamente como entienden la tecnología, por lo que estos ataques son casi inevitables. La cuestión no es si su empresa tendrá que enfrentarse al ransomware. La cuestión es qué hará cuando el ransomware ataque y qué herramientas utilizará para recuperarse. El proceso de recuperación tendrá la contundencia de una amputación o la precisión de una cirugía cerebral, dependiendo de la herramienta que tenga a su disposición. ¿Utilizará un hacha o un bisturí?

> “El ransomware no afecta a todos los archivos y carpetas simultáneamente. La línea de tiempo del ataque es irregular y varía de un usuario a otro en toda la organización.”

Volvamos por un momento a los aspectos sociales y de software de estos ataques. La parte social es relativamente sencilla: El objetivo de los atacantes es engañar al usuario final para que descargue software malicioso. Esto puede hacerse mediante amenazas, promesas de recompensas u otros medios, pero sólo tiene que funcionar una vez en una persona. En una gran empresa formada por miles o incluso cientos de miles de usuarios, estos intentos podrían fallar el 99,99% de las veces. Todo lo que los atacantes necesitan es que una sola persona baje la guardia y el juego habrá terminado.

Una vez que el malware se cuela por esa primera puerta social, comienza la oleada de ataques. El código se abre paso a través del sistema del usuario y la red en general. Los ataques de ransomware más avanzados lo hacen de forma silenciosa, cifrando archivos y volúmenes sin que nadie se dé cuenta de lo que ocurre.

El usuario inicial puede incluso seguir trabajando sin interrupción mientras el malware se propaga. Un ataque exitoso de ransomware a escala empresarial pasará desapercibido durante unos diez días. En ese momento, alguien de la organización intentará acceder a un archivo y se encontrará con que está bloqueado. Otros usuarios comenzarán a experimentar el mismo problema. Finalmente, alguien avisa al departamento de TI. Ellos investigan, descubren el problema y dan la alarma. Para entonces ya es demasiado tarde.

La línea de tiempo del ataque irregular

Las copias de seguridad son incapaces de proteger a las grandes organizaciones contra los sofisticados ataques de ransomware a escala empresarial porque fallan en la recuperación. La cuestión no es si sus archivos están a salvo, sino cuánto tiempo le llevará volver a poner su negocio en marcha con normalidad. Colonial Pipeline pagó el rescate y aun así tardó semanas en volver a la normalidad.

Volviendo al hacha de guerra frente al bisturí… supongamos que el ataque pasa desapercibido durante diez días antes de que el departamento de TI dé la alarma. Es entonces cuando el reloj empieza a correr. La gente no puede acceder a sus archivos y el duro trabajo de recuperación acaba de empezar.

El enfoque del hacha, característico de las copias de seguridad, exige retroceder todo el sistema de archivos hasta antes del momento del ataque. Todos pierden al menos diez días de trabajo. Esto equivale a una amputación. Es drástico y desordenado, y todavía llevará mucho tiempo, pero es eficaz para retroceder el reloj al momento anterior al inicio de la infección.

Pero ¿qué pasa con los usuarios finales que fueron atacados el noveno día? ¿Por qué deberían perder los nueve días anteriores de trabajo? El ransomware no afecta a todos los archivos y carpetas simultáneamente. La línea de tiempo del ataque es irregular y varía de un usuario a otro en toda la organización. Sin embargo, con el enfoque de la copia de seguridad y el hacha, los usuarios que sólo se vieron afectados uno, dos o tres días antes de que se detectara el ataque tienen que sufrir tanto como el empleado de la zona cero que hizo clic en el nefasto enlace.
Aumente la escala a miles de usuarios, algunos de los cuales pueden no haber sido afectados en absoluto. Obligar a todo el mundo a retroceder al mismo punto en el tiempo es un desastre para la empresa, ya que mucho trabajo bueno —archivos sanos— se retrocederá innecesariamente a la zona cero. Y puedes culpar de ello directamente a las copias de seguridad.

Un hacha de guerra es una herramienta eficaz. No es una herramienta de precisión.

Recuperación de ransomware a escala empresarial

Una mejor solución a nivel empresarial es tomar un bisturí —un bisturí rápido— y revertir a versiones sanas en diferentes puntos del tiempo. Con un registro de auditoría y versiones inmutables de sus archivos almacenados en la nube, puede seguir

“El ransomware no afecta a todos los archivos y carpetas simultáneamente. La línea de tiempo del ataque es irregular y varía de un usuario a otro en toda la organización.”

1. *(Crédito: Cloud Security Alliance - cloudsecurityalliance.org)*

la línea de tiempo irregular que corresponde al perfil de penetración del ataque de ransomware. Tampoco se trata de un proceso lento o minucioso, sino que permite recuperaciones en cuestión de horas, en lugar de días o incluso semanas. Con este bisturí de versiones, el culpable original perderá diez días de trabajo, pero todos los demás volverán a los momentos anteriores a que el ransomware infectara sus archivos. Las personas afectadas el día 9 sólo perderán un día de trabajo.

El bisturí con versiones es una solución más eficaz para las organizaciones modernas y mucho menos frustrante para los usuarios finales, especialmente cuando se amplía a empresas con miles de empleados. El trabajo productivo que preserva el versionado de archivos —y el dinero que ahorra— es enorme.

Las afirmaciones infundadas que hacen los actuales proveedores de copias de seguridad me recuerdan al Caballero Negro de Monty Python y el Santo Grial. Después de haber perdido todos los miembros, sigue lanzando insultos, gritando: “No es más que un rasguño”. Sabemos que no es así, y el backup pronto correrá la misma suerte que ese caballero herido de muerte, a pesar de las protestas de los expertos atrincherados en la industria. En la era del ransomware, el fin del backup es inminente.

Principales regulaciones de la privacidad

Por Leonardo Devia

Las empresas de todos los tamaños que se dirigen a clientes en la UE deben evaluar y ajustar sus prácticas de recopilación de datos para cumplir con los estrictos requisitos de GDPR. Estos esfuerzos incluyen dar los pasos iniciales para lograr el cumplimiento e integrar los principios fundamentales del GDPR en cada parte de sus operaciones. Y además, vemos las principales regulaciones en Sudamérica.

> “No existe una guía rápida, y el cumplimiento de GDPR es diferente para cada empresa.”

Cumplir con este reglamento europeo sobre protección de datos significa garantizar que los datos se compilan, utilizan y almacenan legalmente. Esto incluye recoger el consentimiento de los interesados, revelar por qué se recopila la información y cómo se usa, y mantener los datos seguros (es decir, protegidos contra infracciones). Ese es sólo el punto de partida: como veremos, el GDPR garantiza que los interesados siempre mantengan el control sobre sus datos, incluso después de que autoricen su uso por parte de una corporación.

Para cumplir con las normas, las autoridades públicas y las empresas que procesan datos a gran escala deben contratar a un Oficial de Protección de Datos (DPO) para supervisar sus actividades de procesamiento.
Por otro lado, cualquier empresa que participe en actividades de datos de alto riesgo, como el procesamiento de categorías especiales de datos personales (como datos biométricos o genéticos), debe completar una Evaluación de impacto de protección de datos (DPIA).

Desafortunadamente, no existe una guía rápida, y el cumplimiento de GDPR es diferente para cada empresa. Nuestra guía de requisitos legales y cumplimiento del GDPR te ayudará a decidir por dónde empezar.

Importancia de la privacidad de los datos

Muy brevemente, estos cuatro son los principios que se deben tener presentes.

- Es la capacidad de una persona para controlar la exposición y disponibilidad de la información sobre uno (Diccionario informal)

- Estado de lo que es privadoMuy brevemente, estos cuatro son los principios que se deben tener presentes.
, personal

- Es el derecho al respeto a la vida privada de una persona, en su entorno familiar y, por supuesto en su correspondencia

- Dependerá de cómo se recopilen los datos, almacenado y compartido con terceros, además del cumplimiento de las leyes de privacidad aplicable

Teniendo en cuenta esto…

- Límite de poder: cuanto más sabe alguien sobre nosotros, más poder puede tener sobre nosotros. Es adecuado limitar el poder que las empresas pueden tener sobre nosotros, valga la redundancia

- Respeto a las personas: La privacidad es respetar a las personas. Si una persona tiene el deseo de mantener algo en secreto, es una falta de respeto ignorar sus deseos sin una razón de peso

- Gestión de la reputación: la privacidad nos permite gestionar nuestra reputación. Cómo somos juzgados por los demás afecta nuestras oportunidades, amistades y bienestar general

- Mantenimiento de las limitaciones sociales: las personas establecen límites para los demás en la sociedad. Esos representan los límites tanto físicos como también informativos. Por ejemplo, nadie necesita saber dónde estamos en todo momento

- Confianza: En las relaciones, ya sean personales, profesionales, gubernamentales o comerciales, dependemos de confiar en la otra parte. Las violaciones de la confidencialidad son violaciones de esa confianza. ¿Confiaría en una empresa que promete usar sus datos para un propósito y los usa para otro?

- Control sobre nuestras vidas: Sin saber qué datos se están utilizando, cómo están siendo utilizados, la capacidad de corregirlos y cambiarlos, estamos virtualmente indefensos en el mundo de hoy

- Libertad de pensamiento y expresión: La privacidad es la clave para la libertad de pensamiento. Una mirada a estar atentos a todo lo que leemos o vemos puede impedirnos explorar otros pensamientos

- Libertad de actividades políticas y sociales: la privacidad ayuda a proteger nuestra capacidad de asociarse con otros y participar en actividades políticas

- No tener que dar explicaciones ni justificarse: Puede ser demasiado traumático el pensar en “cómo”, todo lo que hagamos será notado por los demás y para eso tendremos que estar listos en explicar situaciones embarazosas

- Capacidad de cambio y segundas oportunidades: Las personas están en constante evolución; Nos mudamos y crecemos a lo largo de la vida. Hay un gran valor en la capacidad de tener una segunda oportunidad, de ser capaz de aprender de los errores, capaz de reinventarse. ¿Es justo que una persona sea juzgada eternamente por un comentario publicado en una red social?

Luego de estas premisas, ahora… es evidente porqué es importante nuestra privacidad…

> “La privacidad es la clave para la libertad de pensamiento.”

Directrices Básicas de GDPR

Hay siete principios clave para el GDPR que dictan cómo las empresas procesan los datos para cumplir con los estándares de protección de datos de la UE.

1. Legalidad, equidad y transparencia. El procesamiento de datos debe ser legal y la información recopilada debe usarse de manera justa. Tampoco debe inducir a error a los usuarios sobre cómo se utilizan sus datos.

2. Limitación de la finalidad. El propósito del procesamiento debe ser claro desde el principio, registrado y solo modificado si existe el consentimiento del usuario.

3.Minimización de datos. Solo se deben recopilar los datos necesarios para el propósito de procesamiento declarado.

4.Precisión. Se deben tomar medidas razonables para garantizar que los datos recopilados sean precisos y estén actualizados.

5.Limitación de almacenamiento. Los datos no deben conservarse más tiempo del necesario.

6.Integridad y confidencialidad. Se deben implementar medidas de ciberseguridad adecuadas para proteger los datos personales que se almacenan.

7.Responsabilidad. Las organizaciones son responsables de cómo manejan los datos y cumplen con el GDPR .

Ley General de Protección de Datos de Brasil (LGPD)

La Lei Geral de Proteção de Dados (LGPD) es un marco legal para regular la recolección y uso de datos personales. Entró en vigor en Brasil el 16 de agosto de 2020. La ley fue aprobada y será aplicada por la Autoridade Nacional de Proteção de Dados (ANPD). Las sanciones entraron en vigor el 1° de agosto de 2021, y los interesados y las autoridades públicas pudieron hacer valer sus derechos a partir del 18 de septiembre de 2020.

La LGPD no es la primera ni la única ley de privacidad de datos en América del Sur, pero es quizás la mejor publicitada de esa región. La LGPD estuvo influenciada por el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, y también ha ampliado su cobertura en algunas áreas a partir de los parámetros del GDPR. La ANPD también será fundamental en la evolución de sus parámetros.

Ésta es una ley federal diseñada para unificar 40 leyes y está compuesta por 65 artículos. Los artículos 17 a 22 tratan de los derechos de los interesados, aquellos cuyos datos se recopilan y/o procesan, principalmente individuos o personas físicas. Cuenta con 10 bases

legales para el tratamiento de datos personales, cuatro más que el GDPR.

Los fundamentos de la ley de protección de datos personales son:

- El respeto por la privacidad
- La autodeterminación informativa
- La libertad de expresión, información, comunicación y opinión
- La inviolabilidad de la intimidad, el honor y la imagen
- La inviolabilidad del desarrollo económico y tecnológico e innovación
- La inviolabilidad de la libre empresa, la libre competencia y la defensa del consumidor
- La inviolabilidad de los derechos humanos, el libre desarrollo de la personalidad, la dignidad y el ejercicio de la ciudadanía por las personas naturales

Privacidad de Datos en Argentina: Ley 25326

La Ley de protección de datos personales es un régimen que regula los datos asentados en archivos, registros y bases de datos para garantizar el derecho al honor y a la intimidad de las personas. La ley prohíbe usar los datos para algo diferente al propósito para el que fueron recolectados. El habeas data se incluye en la Constitución Nacional que en su artículo 43 dice: "Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley. En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva."
Los principios que establece la ley son:

- Todos los archivos de datos personales deberán estar inscriptos en el Registro de la Dirección Nacional de Protección de Datos Personales.
- Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.
- La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la Ley Nro 25326.
- Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.
- Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.
- Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la Ley N.º 25.326.
- Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.
- Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

Riesgo de una "pérdida financiera catastrófica" por los ataques cibernéticos

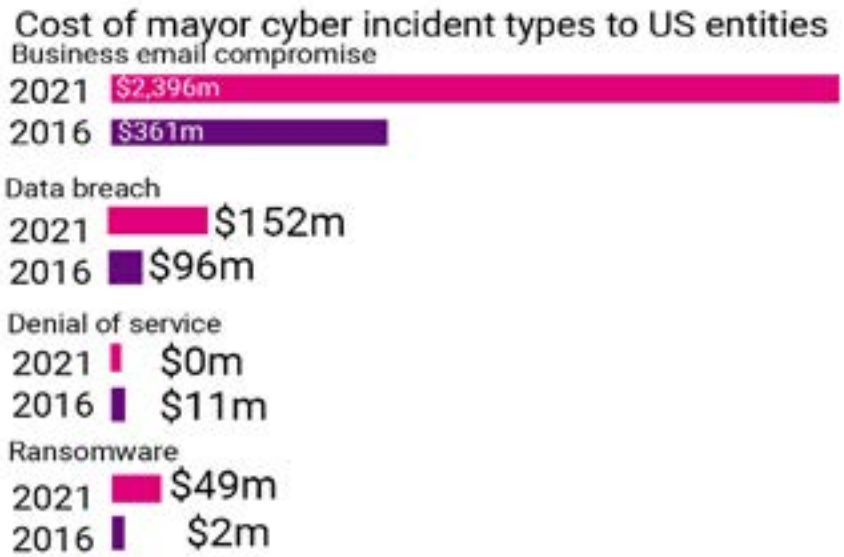
Las empresas corren el riesgo de una "pérdida financiera catastrófica" por los ataques cibernéticos, advierte el organismo de control de EE. UU. Las compañías de seguros privadas limitan cada vez más la cobertura contra las principales amenazas cibernéticas, según un informe de la GAO

> "Dada la amplia y cada vez más hábil gama de actores dispuestos a apuntar a entidades estadounidenses, la cantidad de incidentes cibernéticos está aumentando a un ritmo alarmante."

Un organismo de control del gobierno de Estados Unidos advirtió que las compañías de seguros privadas se están retractando cada vez más de cubrir los daños de los principales ataques cibernéticos, lo que deja a las empresas estadounidenses enfrentando "pérdidas financieras catastróficas" a menos que se pueda encontrar otro modelo de seguro.

El creciente desafío de cubrir el riesgo cibernético se describe en un nuevo informe de la Oficina de Responsabilidad Gubernamental (GAO, por sus siglas en inglés), que exige una evaluación del gobierno para determinar si se necesita una opción federal de seguro cibernético.
El informe se basa en evaluaciones de amenazas de la Agencia de Seguridad Nacional (NSA), la Oficina del Director de Inteligencia Nacional (ODNI), la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) y el Departamento de Justicia para cuantificar el riesgo de ataques cibernéticos en infraestructura crítica, identificando tecnologías vulnerables que podrían ser atacadas y una variedad de actores de amenazas capaces de explotarlas.

Citando una evaluación anual de amenazas publicada por ODNI, el informe encuentra que los grupos de hackers vinculados a Rusia, China, Irán y Corea del Norte representan la mayor amenaza para la infraestructura de los EE. UU., junto con ciertos actores no estatales como las bandas organizadas de ciberdelincuentes.
Dada la amplia y cada vez más hábil gama de actores dispuestos a apuntar a entidades estadounidenses, la cantidad de incidentes cibernéticos está aumentando a un ritmo alarmante.
"Aunque las agencias federales no tienen un inventario completo de incidentes de seguridad cibernética", dice el informe, "varias fuentes federales y de la industria clave muestran (1) un aumento en la mayoría de los tipos de ataques cibernéticos en los Estados Unidos, incluidos los que afectan la infraestructura crítica, y (2) costos significativos y crecientes para los ciberataques".



En 2016, las empresas y los organismos públicos de EE. UU. se vieron afectados por un total de 19 060 incidentes en las cuatro categorías principales (ransomware, violaciones de datos, compromiso de correo electrónico empresarial y ataques de denegación de servicio) con un costo total de U$S 470 millones, según un análisis de GAO de Informes del FBI. En 2021, hubo 26 074 incidentes y el costo total fue cercano a los 2600 millones de dólares.

El informe también cita incidentes específicos que han tenido un efecto indirecto en la economía en general, en particular el ataque cibernético en el Oleoducto Colonial (Colonial Pipeline) que desconectó una operación de transporte de combustible de 5500 millas de largo. En ese ataque, el operador del oleoducto pagó un rescate de 4,4 millones de dólares a los piratas informáticos, a pesar de los consejos de los organismos encargados de hacer cumplir la ley de que siempre se deben rechazar las demandas de rescate.

"Costos significativos y crecientes de los ciberataques"

Asustados por la posibilidad de tener que cubrir pérdidas tan grandes, las aseguradoras privadas se están retirando del mercado al excluir algunos de los ataques cibernéticos de más alto nivel de la cobertura de las pólizas de seguro. Si bien las violaciones de datos y los ataques de ransomware generalmente todavía están cubiertos, el informe encuentra que "las aseguradoras privadas han estado tomando medidas para limitar sus pérdidas potenciales por eventos cibernéticos sistémicos", y se niegan a cubrir las pérdidas sufridas por actos de guerra cibernética o ataques deliberados a la infraestructura. Según el Departamento del Tesoro de EE. UU., algunas aseguradoras también han mitigado su exposición al reducir la cantidad máxima que pagará una póliza en caso de un ataque cibernético y/o aumentar las primas en un intento de protegerse de las pérdidas. Hay más pruebas de que algunas compañías de seguros se están retirando por completo de la cobertura en los sectores de infraestructura, según descubrió la GAO, al considerar que el riesgo de ataque es demasiado alto.

En general, el informe de la GAO sugiere que CISA y la Oficina Federal de Seguros lleven a cabo una evaluación para determinar si los factores anteriores requieren una respuesta del seguro federal similar al seguro de la FDIC para depósitos bancarios y el Programa Nacional de Seguro contra Inundaciones.

Desafíos en Blockchain

No hay duda de que Blockchain es una tecnología emergente prometedora, pero enfrenta algunos desafíos. Estos desafíos a veces limitan su uso. Hay muchos problemas, como procesos de consenso, gestión de datos, almacenamiento, sistemas de cadena, legislación, gobernanza, etc.

Algunos de los principales desafíos son:

Escalabilidad

Hay varias transacciones que aumentan día a día en la cadena de bloques, lo que hace que se almacenen más datos. Todos los nodos tienen que almacenar todas las transacciones para su validación. Debido a la restricción del tamaño del bloque y al tiempo necesario para crear un nuevo bloque, blockchain solo puede procesar siete transacciones por segundo.

La capacidad real de los bloques es deficiente y muchas transacciones pequeñas podrían retrasarse ya que los mineros prefieren transacciones con una tarifa de transacción más alta. El problema de la escalabilidad es, por lo tanto, alto.

Fugas de privacidad

En la cadena de bloques, las transacciones de los usuarios se consideran seguras ya que se realizan con direcciones creadas en lugar de identidades reales.

En caso de fuga de datos, los usuarios pueden generar varias direcciones. Sin embargo, la cadena de bloques no puede garantizar la privacidad transaccional ya que el valor de las transacciones es visible públicamente para cada clave pública. El anonimato del pago debe reforzarse en el Blockchain.

Leyes y reglamentos

La introducción de blockchain ha traído muchos cambios sociales, incluso en sistemas legales y regulatorios. Blockchain desencadenó una serie de problemas legales al retrasar la supervisión legal en las primeras etapas de desarrollo. Las leyes y regulaciones adecuadas sólo se pueden fortalecer después de una comprensión rápida de las características de la cadena de bloques. Mediante el fortalecimiento de las medidas regulatorias, la mayoría de los países comenzaron a implementar Blockchain.

> “En la cadena de bloques, las transacciones de los usuarios se consideran seguras ya que se realizan con direcciones creadas en lugar de identidades reales.”

Gobierno

Blockchain tiene un amplio panorama de implementación en términos de gobierno e infraestructura y se puede esperar que transforme las funciones y roles del gobierno. También ayuda a que las estructuras organizativas gubernamentales sean menos complejas, la seguridad de los datos gubernamentales y la transparencia de los procesos de gobierno y servicio. Dado que blockchain es una red distribuida sin la necesidad de un tercero, ofrece viabilidades más amplias para el avance de las políticas, ya que es un problema crítico que necesita una resolución inmediata.

BaaS: Blockchain como servicio

Muchas compañías, así como también particulares, quieren adoptar la tecnología blockchain. Desafortunadamente, crear, configurar y operar una cadena de bloques representan todo un desafío, por lo que la mayoría se desalienta por esta dificultad. BaaS o Blockchain as a Service son servicios en la Nube que permiten a las organizaciones operar la cadena de bloques sin tener que desarrollar y administrar sus propias infraestructuras.

Debido al rigor técnico de blockchain, muchas empresas emergentes y gigantes tecnológicos ofrecen servicios en la nube de tipo BaaS.

Definición de BaaS

BaaS o Blockchain as a Service es la creación y gestión por parte de un tercero de redes basadas en la nube para empresas que desarrollan aplicaciones Blockchain.

Este tipo de servicio en la Nube permite a los usuarios crear, alojar y utilizar sus propias aplicaciones, contratos inteligentes y funciones de Blockchain. El proveedor de servicios en la nube es responsable de administrar las tareas y actividades necesarias para mantener la infraestructura ágil y operativa.

BaaS se basa en el concepto de SaaS (Software as a Service) y funciona de la misma manera. Se enmarca en un contexto donde los modelos económicos de servicios ligados al Cloud Computing son cada vez más requeridos.

Se trata de una novedad en el floreciente campo de la tecnología Blockchain. Como los casos de uso de Blockchain ahora se extienden mucho más allá de las transacciones de criptomonedas, la demanda de servicios de hosting está en crecimiento.

Funcionamiento de BaaS

Tratándose de Blockchain as a Service, un proveedor de servicios Cloud externo se responsabiliza de montar, configurar y gestionar una infraestructura de tecnología Blockchain. Al pagar por un servicio BaaS, el cliente le indica al proveedor que configure y mantenga los nodos conectados de la cadena de bloques.
El proveedor se encarga del mantenimiento de la infraestructura y de todos los elementos relacionados con la cadena de bloques. Otras actividades relacionadas también forman parte del servicio: gestión de ancho de banda, asignación de recursos, hosting, funciones de seguridad y protección contra ciberataques.

> “BaaS se basa en el concepto de SaaS (Software as a Service) y funciona de la misma manera.”

Por lo tanto, el modelo BaaS permite a los clientes concentrarse únicamente en la funcionalidad de sus cadenas de bloques en lugar de tener que preocuparse por problemas de rendimiento e infraestructura al mismo tiempo
.
El funcionamiento de un servicio BaaS se puede comparar con el de un servicio de alojamiento web, en el que el cliente paga a un proveedor como por ejemplo Amazon Web Services para hostear su site en sus servidores en lugar de tener que alojarlo en su propio ordenador y gestionar el mantenimiento e infraestructura.

En este sentido, el modelo BaaS podría permitir una llegada más amplia y más sencilla de la tecnología blockchain en las empresas y organizaciones de todas las industrias. Independientemente del tamaño y la industria, una compañía ahora puede subcontratar todo el soporte técnico de blockchain y enfocarse en sus objetivos.

Cómo prevenir los ataques de esteganografía

Los ciberdelincuentes utilizan la esteganografía como un nuevo vector de ataque para distribuir malware, evadir los análisis de seguridad y obtener persistencia.

Los ciberdelincuentes están bien versados en cambiar sus técnicas de piratería y adaptar nuevas estrategias de amenazas a situaciones y oportunidades específicas. Los actores de amenazas a menudo aprovechan varias tácticas como el phishing y la ingeniería social para propagar malware disfrazándose. Recientemente, se encontraron adversarios usando un nuevo vector de ataque llamado Steganography para implementar malware, evadir escaneos de seguridad y obtener persistencia.

Según un informe de Kaspersky, los agentes de amenazas se dirigieron a múltiples distribuidores de equipos y software para empresas industriales para robar credenciales utilizando técnicas de phishing y esteganografía.

¿Qué es la esteganografía?

En general, la esteganografía es un arte antiguo de ocultar información en imágenes y pinturas. La mayoría de los artistas usan esta técnica para ocultar sus firmas y otros mensajes ocultos dentro de sus pinturas. Incluso los reyes utilizaron esta técnica de ocultación de datos para enviar mensajes secretos a sus soldados en la zona de guerra.

Uso de la esteganografía en ciberataques

Los ciberdelincuentes ahora están aprovechando la esteganografía como vector de ataque para ocultar JavaScripts maliciosos y malware dentro de las imágenes y distribuirlos a los objetivos. Cuando la víctima hace clic en la imagen maliciosa, el malware incrustado en la imagen descarga automáticamente el código malicioso o el malware e infecta el sistema objetivo.

Según los objetivos, los atacantes utilizan diferentes tipos de ataques de esteganografía, que incluyen:

- Esteganografía de texto. En un ataque de esteganografía de texto, los piratas ocultan información (código de malware) dentro de los archivos de texto. Los malos actores hacen esto alterando el formato de texto en el archivo existente, como cambiar palabras, crear caracteres u oraciones aleatorias.

> “Recientemente, se encontraron adversarios usando un nuevo vector de ataque llamado Steganography para implementar malware, evadir escaneos de seguridad y obtener”

- Esteganografía de imágenes. Los atacantes ocultan datos maliciosos en imágenes. Aprovechan la gran cantidad de bits o píxeles de una imagen y los reemplazan con códigos de malware. Los actores de amenazas aprovechan diferentes tácticas para establecer ataques de esteganografía de imágenes, incluidos los métodos de inserción de bits menos significativos, enmascaramiento y filtrado, codificación de patrones, codificación y transformación de coseno.

- Esteganografía de audio. En un ataque de esteganografía de audio, los actores de amenazas explotan los archivos de audio WAV para ocultar su malware personalizado. Los atacantes incrustan el código malicioso dentro de los archivos de audio WAV que contienen un componente de carga para decodificar y ejecutar el contenido malicioso incrustado en los archivos de audio.

- Video esteganografía. La esteganografía de video es una combinación de ataques de esteganografía basados en texto e imágenes. Los adversarios incorporan una gran cantidad de datos maliciosos dentro del flujo de imágenes y archivos de audio en movimiento.
.

¿Cómo se previenen los ataques de esteganografía?

- Evite que los empleados descarguen software y otras aplicaciones de fuentes desconocidas, ya que pueden contener códigos esteganográficos.

- Nunca haga clic/abra/descargue archivos de texto/audio/imagen sospechosos de fuentes desconocidas.

- Supervise de cerca los procedimientos de distribución de software en sus organizaciones para identificar a los malintencionados.

- Entrene a los empleados en varios señuelos de phishing e ingeniería social.

- Use herramientas antimalware para identificar la presencia de malware en los archivos, documentos de texto e imágenes recibidas de fuentes desconocidas.

emBlue

Hacemos que la **omnicanalidad sea simple**

Marketing automation, email, sms, push notifications y más.

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