CYBERSECURITY
by itwarelatam.com

Edición - Nº 13

La revista de Cloud Security

NOTA DE TAPA

No hay Big Data sin Ciberseguridad... y viceversa

INFORME ESPECIAL

Los desafíos de la ciberseguridad en el trabajo híbrido

MÁS TEMAS

Tendencias 2022 en la industria de la ciberseguridad

¿Qué es el Seguro de Cibernética?

Rusia, Ucrania y la ciberguerra

EDICIÓN N°13

NOTA DE TAPA

NO HAY BIG DATA SIN CIBERSEGURIDAD... Y VICEVERSA

04

SUMARIO

Big Data, ciberseguridad y trabajo híbrido

Si bien son más leves, todavía seguimos con algunas restricciones debido a la pandemia. Eso significa que varias de las condiciones de trabajo que se modificaron por el encierro y la cuarentena seguirán vigentes. El trabajo remoto no sólo incrementó las preocupaciones de seguridad, también aumentó la cantidad de datos transaccionados y almacenados. Por eso este número está dedicado a dos de los tópicos más importantes del momento.

Nuestro tema de tapa hablará de la relación directa e indivisible entre Big Data y Ciberseguridad y haremos hincapié en un par de temas relevantes: la necesidad de almacenamiento, el papel de la Inteligencia Artificial y el talento necesario para operar. Tres de entre muchos enfoques posibles. Por su parte, el Informe Especial tratará, precisamente, del Trabajo Híbrido. Temas como la protección de la identidad, configuraciones correctas y adecuadas y, sobre todo, la capacitación y concientización de los empleados, no pueden faltar en este resumen.

Además, tenemos notas sobre seguridad y experiencia del usuario, Inteligencia Artificial en la ciberseguridad, desarrollo seguro e interoperabilidad, nuevas normas ISO y riesgos de seguridad en la administración de la identidad, entre otras.

Los esperamos en el próximo número.

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

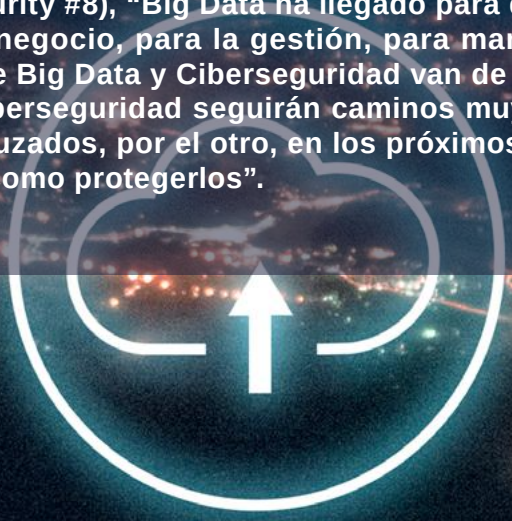
Puede leer y descargar la versión digital de esta revista en www.itwarelatam.com.com

Edita, diseña, comercializa y distribuye Mediaware Marketing

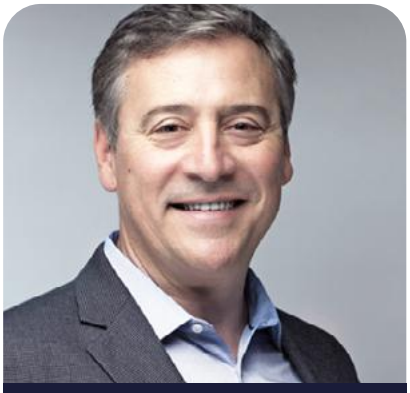
NO HAY BIG DATA SIN CIBERSEGURIDAD... Y VICEVERSA

Por Ricardo Goldberger

Como dijimos en un número anterior en el que también nos dedicamos al tema Big Data y ciberseguridad (Cybersecurity #8), “Big Data ha llegado para quedarse ya que es cada vez más necesario para el negocio, para la gestión, para mantener el status quo... o cambiarlo. Y es evidente que Big Data y Ciberseguridad van de la mano.” Y concluimos: “Tanto Big Data como la Ciberseguridad seguirán caminos muy paralelos, por un lado, pero continuamente entrecruzados, por el otro, en los próximos años, ya que es tan importante analizar los datos como protegerlos”.



Miguel Llerena, VP de alianzas y canales para Latinoamérica de Tanium, ofrece un poco de contexto: "Las técnicas de Big Data suelen hacer uso del almacenamiento en la nube. Esto permite a las organizaciones manejar grandes volúmenes de datos de forma flexible y rentable. Si bien, pese a sus beneficios, en los últimos años ha aumentado el riesgo de fuga de datos y los ciberataques a empresas. A menudo, los datos sensibles no están bien protegidos o no están protegidos en absoluto. De esta forma, su seguridad representa uno de los mayores obstáculos para las empresas que buscan aprovechar los beneficios del Big Data. Cuando las empresas no pueden asegurar de manera confiable y consistente los datos confidenciales, suelen aparecer varias vulnerabilidades concretas."



Miguel Llerena

Diego Macor

Algunos de nuestros referentes acercan datos:

Diego Macor, Gerente de Ciberseguridad de IBM para Argentina, Chile, Paraguay y Uruguay, acerca algunos datos del estudio global X-Force Threat Intelligence Index: 23% de los ataques fueron de Ransomware; "los actores de Ransomware Sodinokibi (también conocidos como REvil) hicieron al menos U$S 123 millones en ganancias en 2020, robando alrededor de 21,6 TB de datos."

Max García, Head of Technology and Transformation Argentina & Perú de Oracle revela que "Con el costo promedio de una violación de datos alcanzando los 4 millones de dólares (de acuerdo con estudios del grupo de analistas Kuppinger Cole), las pérdidas financieras directas pueden ser catastróficas para muchas empresas, sin siquiera considerar daños reputacionales indirectos."

Según Sergio Corizzo, Gerente de Ingeniería y Servicios de Quick Informatica, "El desafío de Big Data es el manejo de grandes volúmenes de información proveniente de múltiples orígenes, muchos de ellos desconocidos y el problema se genera en la dificultad de poder conocer tales orígenes, que sean confiables y que la información que aporten sea verídica. Hoy Big Data tiene como mayor enemigo la generación de información malintencionada, para alterar tendencias o modificar los comportamientos en la toma de decisiones."

Max García

> “Cuando las empresas no pueden asegurar de manera confiable y consistente los datos confidenciales, suelen aparecer varias vulnerabilidades concretas.”

Sergio Corizzo

Almacenar amenazas

Varios son los riesgos asociados a Big Data y Ciberseguridad, entre ellos, el del almacenamiento de datos.
Leonel Marino, socio de 7Puentes, da un panorama general: “[los datos] se almacenan en miles de nodos, y que la autenticación, autorización y cifrado de la información en estos nodos se convierte en un trabajo difícil. Por ello, es necesario encontrar un mecanismo que garantice que los datos se encuentren seguros, pero que puedan procesarse sin tener que cifrar y descifrar constantemente.”

Elías Vucinovich, Arquitecto de Soluciones de Seguridad de Logicalis Argentina, agrega: “El negocio está adoptando Data Storage en la nube para aumentar su flexibilidad en lo referente a almacenamiento, lo cual conlleva a que si no se tiene un correcto y estricto control sobre el acceso a estos datos, algún atacante podría tener acceso a datos sensibles, privados, que luego podrían ser utilizados como medio de extorsión. Es de extrema importancia la aplicación de políticas seguras sobre estos almacenamientos en nube.”

Andrés Piñango Galindo, Asesor de Soluciones, Plataformas & Tecnologías de SAP Región Sur, ofrece algunos datos: “Se estima que sólo en el año 2020 fueron creados 64 Zettabytes (1.000 millones de TB) en el mundo, con tipos de datos tan variados como videos, fotos, datos personales, información de sensores, etc. Esta gran cantidad de información almacenada no sólo da un gran poder a las

Elías Vucinovich

organizaciones para generar valor, sino que además una gran responsabilidad, ya que son responsables primarias del correcto manejo de los datos propios y de los de sus clientes. Dado el contexto, se deben utilizar estrategias y herramientas de ciberseguridad para poder asegurar la seguridad y privacidad de la información de los datos de la organización y sus clientes.”

Andrés Piñango Galindo

> “Se estima que sólo en el año 2020 fueron creados 64 Zettabytes (1.000 millones de TB) en el mundo, con tipos de datos tan variados como videos, fotos, datos personales, información de sensores, etc.”

En línea con lo que dice Piñango, **Victoria Martinez, Business Development Manager en AI Projects de Red Hat** opina que “en la mayoría de las empresas, el almacenamiento local tradicional ya no es suficiente para los terabytes y petabytes de datos que se generan en la operación diaria. La necesidad de contar con información en tiempo real, la respuesta instantánea genera una demanda de procesamiento y almacenamiento por eso las soluciones en la nube y en la nube híbrida se eligen cada vez más por su escalabilidad e infraestructura de almacenamiento simplificada.

“Las tres V de big data (volumen, variedad y velocidad) —refiere **Rakesh Jayaprakash, product manager en ManageEngine**— hacen que la seguridad de Big Data sea un gran desafío. Los volúmenes de datos crecen con cada transacción y la mayor parte de los componentes de datos estructurados y no estructurados en Big Data los hace altamente vulnerables a las amenazas de seguridad. Además, el propósito de administrar data lakes enormes se frustra sin las medidas de seguridad adecuadas para complementar (no obstaculizar) las velocidades de datos. Por ejemplo, se requiere que un banco o una tienda de comercio electrónico procese y analice Big Data a alta velocidad sin comprometer su seguridad para mantenerse al día con las demandas de sus usuarios finales.”

Victoria Martinez

Rakesh Jayaprakash

Corizzo habla de herramientas: “Se requieren herramientas mucho más eficaces de almacenamiento, ya que suele ser un volumen de datos importante que dificulta la encriptación en los servidores, al igual que el respaldo y la tolerancia a fallos. Y, por otro lado, está la alteración de dicha información antes que llegue a almacenarse, que es el punto más difícil de detectar.”

Concuerda **Miguel Llerena, VP de alianzas y canales para Latinoamérica de Tanium:** “Dado que los datos se almacenan en miles de nodos, la autenticación, autorización y cifrado de la información en estos nodos se convierte en un trabajo difícil. Por ello, es necesario encontrar un mecanismo que garantice que los datos de carácter sensible se encuentran seguros, pero que puedan realizarse consultas y analíticas sin tener que cifrar y descifrar constantemente.”

Big Data e Inteligencia

Cuando hay ingentes volúmenes de datos, imposibles de analizar de manera humana o, aunque más no sea, analógica, se impone recurrir a alguna tecnología de Inteligencia Artificial.

“Es fundamental tener un medio seguro y confiable para almacenar, organizar y recuperar los muchos terabytes de datos —afirma Piñango Galindo— pero es clave contar con algoritmos avanzados y analíticas impulsadas por IA para gestionar grandes volúmenes de información”. Y prosigue: “Una de las ventajas que tiene la Inteligencia Artificial es que permite aprender sin uno explícitamente enseñarle, ya que utiliza información histórica, detectando patrones y realizando predicciones acerca de la naturaleza de la información. Esta característica se hace muy relevante en la ciberseguridad, ya que puede ayudar a detectar y bloquear ataques que nunca se hayan realizado en el pasado y por lo tanto no exista ninguna regla de detección.”

> “Es clave contar con algoritmos avanzados y analíticas impulsadas por IA para gestionar grandes volúmenes de información”.

Juan Marino, Cybersecurity Sales Strategy Manager de Cisco, advierte: “El reto más importante reside en la gobernanza de la información. La misma tecnología puede ayudar para detectar el uso que se le da a los datos y las analíticas que se obtienen al utilizar IA. Dado que la IA puede ser aplicada de diversas formas en cada industria, es fundamental definir el alcance de los marcos regulatorios no sólo de manera general, sino de forma específica.”

Martínez, especialista en las tecnologías de la IA, sostiene: “La inteligencia artificial, es el motor impulsor de la innovación en el mundo de los datos. Entenderlos a través de diferentes técnicas, predecir comportamientos, anticiparse a la próxima jugada en el mundo de la

ciberseguridad es clave. Hoy se incorporan estos beneficios desde el sistema operativo, de manera muy natural, en cómo poder anticiparme y recomendar una configuración, alertar sobre un posible issue antes de que suceda, forma parte de un feature que el cliente exige. Entender el comportamiento de mi red, anticiparme a una posible falla, ataque o hueco de seguridad es lo que hablamos de brindar un valor agregado a los clásicos productos que ya existen en nuestros clientes.

"Además de todo esto, está el beneficio de poder generar mejores y experiencias únicas a mi cliente. Desde acceder a la información de maneras cada vez más simples, como lo es el lenguaje natural aplicado a las búsquedas, intervienen técnicas de IA para entender qué se está consultando y poder acceder y resumir esa información al usuario."

Juan Marino

Marino, de 7Puentes, resume: "Los ciberataques son cada vez más complejos y la Inteligencia Artificial es una importante herramienta para mejorar la seguridad de la información de las empresas. Con la ayuda de la IA se pueden analizar situaciones y comportamientos rápidamente, para detectar amenazas, incluso, antes de que ocurran".

Por su parte, Macor detalla: "La IA puede aumentar las habilidades de los analistas de seguridad en ciertos tipos de tareas operativas, lo que les permite enfocarse en áreas más importantes y realizar su labor de forma más precisa y eficiente. También puede ayudar a mejorar el tiempo de detección de las ciberamenazas. Por ejemplo, con analítica predictiva se pueden identificar anomalías de red, detectar malware y analizar patrones de comportamiento de los usuarios con el fin de detectar a los usuarios de riesgo dentro de una empresa, y potencialmente frustrar el fraude o las amenazas de información privilegiada". Pero advierte que "los cibercriminales han aprendido sobre el poder de la IA y lo están

Leonel Marino

explotando. Para hacerle frente, los profesionales de seguridad, aprovechando el mismo poder de la IA, pueden mantenerse al día con amenazas cada vez más sofisticadas, desarrollar herramientas que puedan detectar actividades maliciosas y detener a los ciberdelincuentes de forma más rápida."

García sostiene que "la inteligencia artificial no solo ayuda a 'consumir' grandes volúmenes de datos, permitiendo encontrar y descubrir información valiosa y patrones de valor en ellos, sino que también ayuda a gestionar de forma eficiente todas las plataformas de un entorno Big Data; esto incluye identificar acciones fraudulentas, mantener controles de configuración, identificar actividad anómala de los usuarios y clasificar y priorizar los eventos de seguridad; todo ello sin la lentitud, sesgo o el riesgo del error humano. Los sistemas de Base de Datos pueden embeber capacidades de AI/ML para brindar auto-securización, además de otras capacidades como auto-administración, auto-parchado, y auto-escalabilidad, facilitando la seguridad y operación de los datos en un entorno Big Data porque se protegen a sí mismos en lugar de tener que esperar a que haya un administrador disponible. Esto se aplica a las defensas contra ataques externos e internos.

Finalmente, Jayaprakash concreta: "La IA ayuda a proporcionar ciberseguridad de tres maneras: Monitoreo automatizado a escala (el monitoreo las 24 horas del día de todas las actividades es la piedra angular de todas las operaciones de seguridad, un proceso que sería imposible de lograr sin la IA), planificación de escenarios (los algoritmos de ML pueden analizar grandes volúmenes de datos históricos de amenazas para predecir amenazas futuras. Además, se puede implementar para analizar cómo estas amenazas afectan la seguridad de Big Data, en caso de que se materialicen. Esto permite que la seguridad de TI ejecute varias simulaciones hipotéticas para comprender el impacto de varias amenazas y desarrollar estrategias para prevenirlas) y detección y alerta de intrusiones (es casi imposible detectar intrusiones maliciosas en tiempo real. Sin embargo, es posible detectarlos casi en tiempo real utilizando sistemas de detección de intrusos impulsados por IA. Estos utilizan análisis avanzados para escanear sistemas de manera integral y analizar los datos generados para detectar amenazas. Junto con las alertas de amenazas en tiempo real, permite que los equipos de seguridad reaccionen antes frente a las amenazas)."

Big Data y la gente

La industria IT viene creciendo sin prisa pero sin pausa desde hace, por lo menos, veinte años. Y, sin embargo, hay un problema que no ha logrado solucionar: el talento humano necesario.

De acuerdo con el Banco Interamericano de Desarrollo (BID), en 2020 hubo más de un millón de puestos vacantes en tecnología, mientras que menos de 100.000 profesionales se graduaron en toda la región.

Según la CESSI Cámara de Empresas de Software y Servi-

cios), en la Argentina hay 15.000 puestos de trabajo sin cubrir entre empresas de la industria del software y compañías de otros rubros que buscan talento con perfil tecnológico. Y si nos atenemos a los expertos en estadísticas, menos del 10% de los puestos ocupados corresponden a Ciberseguridad, no hace falta mucho más para tener el panorama claro.

Miguel Llerena, VP de alianzas y canales para Latinoamérica de Tanium, tira la primera piedra: "La escasez de talento calificado en Ciberseguridad agrava la tarea, ya difícil, de protegerse frente un creciente volumen de amenazas cada vez más avanzadas y sofisticadas."

"La demanda de talento de seguridad se ha disparado en los últimos años. Desafortunadamente, la oferta no se mantiene al ritmo de la demanda —propone Macor— Una de las posibles soluciones a esta problemática, es buscar la participación de candidatos con trayectorias profesionales no tradicionales. Distintas personas pueden tener el tipo adecuado de habilidades, aptitudes y la experiencia amplia y necesaria para ocupar diversos roles clave en el ecosistema de seguridad, así no tengan un título de cuatro años. La inclusión de más mujeres es clave también, llevar a más mujeres a áreas como la ciberseguridad es clave para fortalecer la postura de seguridad de la industria."

Avanzando un poco más, según García, "es necesario invertir en capacitación para contar con el talento para usar la tecnología de manera efectiva. Recomendamos que las organizaciones que implementan soluciones y estrategias de Big Data deben evaluar sus requisitos de habilidades de manera temprana y frecuente, y deben identificar de manera proactiva cualquier posible brecha de talentos. Estos pueden abordarse mediante la capacitación de sus profesionales de datos, la contratación de nuevos recursos y/o el aprovechamiento de las empresas de consultoría."

Marino de Cisco va un poco más allá. Según él, el talento humano, las políticas y la tecnología "son los tres pilares que sostienen una estrategia de ciberseguridad. Las carencias en cualquiera de estos tres elementos socavan la efectividad a la hora de mantener una organización segura. Tal vez se ha sobrevalorado la capacidad de las tecnologías desde una lógica de prevención pura, mientras que la madurez y capacidad real de lograr resiliencia se da en una lógica que trasciende la prevención construyendo los procesos y políticas, que de la mano de la tecnología permiten detectar situaciones, adaptarse y minimizar los daños. Hoy en día el elemento humano sigue siendo clave para poder crear la estrategia correcta, llevarla a la práctica y luego desde el punto de vista de la operación de la seguridad detectar y responder a tiempo cuando suceden cosas malas."

A lo que Martínez de Red Hat, agrega: "El talento, sobre todo el equipo humano, es el corazón de todo el proceso. Los equipos hacen al éxito de las implementaciones, la tecnología es el medio para poder articular la necesidad, que la entiende y captura el talento, y las políticas ayudan a que los cambios puedan perdurar a largo plazo. A regular las nuevas tecnologías. Siempre la innovación va más rápido que las políticas y el talento es la llave para articular y llevar adelante cada uno de estos puntos."

"La escasez de talento calificado en Ciberseguridad agrava la tarea, ya difícil, de protegerse frente un creciente volumen de amenazas cada vez más avanzadas y sofisticadas."

Y la pandemia trastocó todo...

La pandemia, y más específicamente, la necesidad de virtualizar la oficina e impulsar el trabajo remoto, trajo consigo riesgos nuevos y sofisticación de los ya conocidos. La "desaparición del perímetro", como se la ha caracterizado últimamente, sumada a la dificultad añadida de controlar los dispositivos y los usuarios —tanto el ámbito tecnológico como en el de la autenticación de la identidad— trajo desafíos nuevos. Que implicó, además, la redefinición de prioridades ante la necesidad de hacer inversiones no previstas.

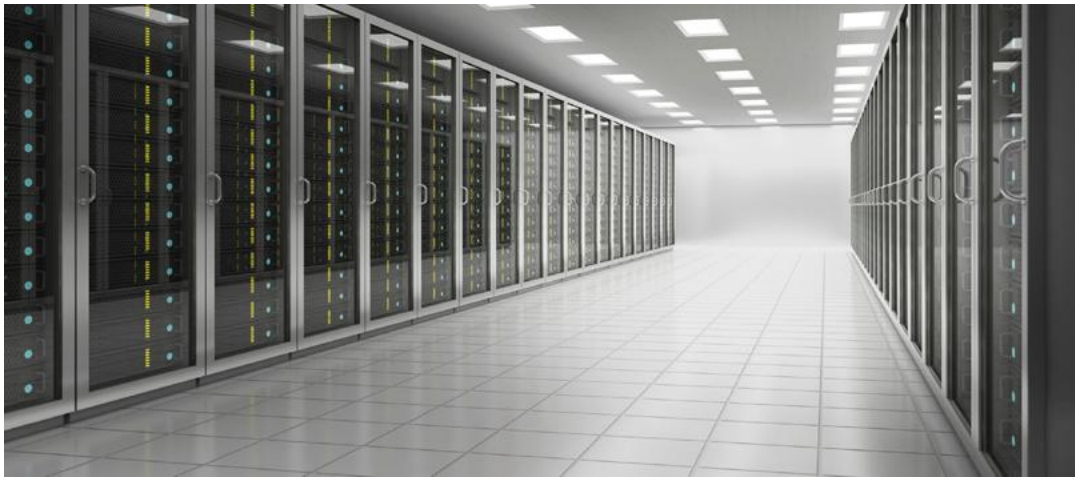
Marino de 7Puentes lo sintetiza de la siguiente manera: "La nueva normalidad de trabajo remoto, en conjunción con un mayor uso en el hogar de Internet, potenciaron los riesgos de virus y malware en la red hogareña a la que se encuentra conectado el teletrabajador." Macor, por su parte, cita datos de un estudio (Cost of a Data Breach): "las filtraciones de datos ahora cuestan a las empresas un promedio de U$D 1,82 millones por incidente en América Latina, un aumento del 30% en comparación con el año anterior". Aquí van más datos:

- Los sectores que enfrentaron grandes cambios operativos durante la pandemia (salud, retail, hotelería y manufactura de consumo/ distribución) también experimentaron un aumento sustancial en los costos de filtraciones de datos año contra año.
- Casi la mitad (45%) de las filtraciones analizadas expusieron datos personales de clientes como nombre, correo electrónico, contraseña o incluso datos médicos, lo que representa el tipo más común de registro filtrado en el informe.
- Las credenciales de usuario comprometidas fueron el método más común utilizado como punto de entrada por los atacantes, representando el 18% de las filtraciones de datos estudiadas.
- El tiempo promedio para detectar y contener una filtración de datos en Latinoamérica fue de 356 días (256 días para detectarla, 100 días para contenerla).
- Las filtraciones de datos en el sector financiero fueron las más costosas de la región, alcanzando los USD 2,94 millones por incidente, seguido por el sector de servicios con un costo de USD 2.36 millones y el industrial con USD 2.22 millones.

Ariel Campanari

Campanari agrega más datos: "En ese sentido, las estadísticas del informe Verizon 2021 Data Breach indican que el 85% de las filtraciones fueron causadas por un elemento humano: el 61 % involucró el uso de credenciales no autorizadas y el phishing aumentó al 36 % (frente al 25 % del año anterior). Los ataques web representaron el 80 % de los ataques, y más del 10 % de los sistemas violados involucraron ransomware, el doble de las cifras de 2019."

Vucinovich es más específico: "Durante la pandemia la utilización de Big Data fue de gran importancia para tener en tiempo real datos de salud, cómo responde la sociedad a las medidas de cuarentena, dónde se encuentran los focos de contagio, etc. No solamente la utilización, sino también la importancia de Big Data se vio incrementada."



Marino de Cisco, por su parte, puntualizó: “La adopción masiva del trabajo remoto como consecuencia de la pandemia, dio lugar a un aumento significativo del riesgo cibernético. Claramente la mayoría de las organizaciones no estaban preparadas ni cultural ni tecnológicamente para mantener un nivel de seguridad, una gestión de riesgo aceptable para un entorno de trabajo completamente descentralizado en el que muchas veces la necesidad de continuidad de negocio se ha llevado por delante algunos controles dando lugar a una “relajación” de la seguridad. Así, son múltiples las estadísticas que apuntan a, por lo menos, una duplicación de los ataques sufridos que fueron reportados por las empresas.”

Martínez mueve el foco a un tema importante, ya que se “comenzó a exigir algo que era un pilar pero que muchas veces se lo pasaba por alto y es lo que hace al uso ético de los datos. Comenzaron a desarrollarse normativas internacionales y locales que resguardaban y cuidaban este activo privado y personal. Es decir, lo que cambió fue el contexto, se sumaron exigencias, muchos nuevos competidores y una necesidad de poder generar valor diferencial a mi cliente. Por eso es que la solución de la nube y nube híbrida se transformó en la manera sencilla de poder afrontar estos nuevos retos y sumarle, como mencionábamos antes técnicas de AI para poder entender comportamientos, contenidos siempre respectando el uso de esas herramientas.”

Y Jayaprakash ilumina otro rincón: “Los ciberataques corporativos han aumentado significativamente solo en el último año, especialmente para las pequeñas y medianas empresas que han sido objeto de varias violaciones de datos debido a la falta de recursos y experiencia en seguridad, con educación e investigación, salud, gobierno y militar, comunicación y la tecnología siendo las cinco industrias más atacadas. La vulnerabilidad Log4j aumentó la cantidad de ataques cibernéticos en el cuarto trimestre del año pasado y esta tendencia solo continuará en 2022.”

Hemos tocado sólo cuatro ítems porque si no deberíamos ocupar muchas más páginas. Asuntos como las estrategias de prevención y de remediación, capacitación y awareness, nuevas tecnologías, son algunos de los temas que prometemos tocar en un futuro número de la revista.

> “Durante la pandemia la utilización de Big Data fue de gran importancia para tener en tiempo real datos de salud, cómo responde la sociedad a las medidas de cuarentena, dónde se encuentran los focos de contagio, etc.”

Big data y ciberseguridad tienen años de coexistencia

Por Luis Lombardi, CEO de MicroStrategy para Latinoamérica Cono Sur

Big data es una herramienta que también se puede utilizar para analizar patrones de ciberataques. Cuánto se hacen, desde dónde se hacen y poder sacar conclusiones.

Luis Lombardi
CEO de MicroStrategy para Latinoamérica Cono Sur

Pero en cuanto a la ciberseguridad con Big Data (y más en general aún), cada vez hay más ataques y esto se puede deber que, al haber grandes conglomeraciones de software, eso ha proliferado, algunos ataques para de alguna forma debilitarlas, si es que las pueden debilitar.

Sobre Inteligencia Artificial, tiene que ver con Big Data, con IA se puede sacar la conclusión, ya que IA va a entender si hay un patrón mezclado con datos que no responde a ningún patrón, y definir qué es o no seguro. Pero en cuanto ataques a big data, no se si hay una relación directa.

En particular sobre MicroStrategy, está más expuesto en su historia por la figura pública que ha tomado por sus inversiones en Criptomoneda, y eso lo ha hecho blanco de mayores ciberataques.

Pero en cuanto al producto MicroStrategy, nosotros recomendamos estar siempre con la última versión, de hecho, nosotros mismo migramos al cliente, y en muchos casos, sin costo. Además, recomendamos estar en la última versión para estar más actualizado sobre las vulnerabilidades ya resueltas. Los ciberataques van evolucionando y, por ende, el producto debe hacerlo para que sea inmune a esos ataques. Y la posibilidad de vencer a esas vulnerabilidades, es mantenerse siempre actualizado en su totalidad.

> “Los ciberataques van evolucionando y, por ende, el producto debe hacerlo para que sea inmune a esos ataques. Y la posibilidad de vencer a esas vulnerabilidades, es mantenerse siempre actualizado en su totalidad.”

DISENIA BOX
IDEAS CREATIVAS

POSICIONA TU MARCA
y elevá las ventas
de tu empresa
EN EL MUNDO DIGITAL

Diseño Gráfico

Social Media

Desarrollo Web

Email Marketing

Videos

¡NO DEJES PASAR ESTA OPORTUNIDAD
que tenemos para vos!

diseniabox

www.diseniabox.com

Tendencias 2022 en la industria de la ciberseguridad

Robert Hannigan
Presidente de BlueVoyant International

Por Robert Hannigan, Presidente de BlueVoyant International

Encontrar un desarrollo integral en optimizar las defensas, sigue siendo un proyecto importante para muchas corporaciones. A pesar del contexto de continua complejidad, el año 2022 nos presenta tres tendencias impulsadas por los atacantes criminales que debemos considerar; los estados nacionales; la industria de la ciberseguridad y sus clientes:

En primer lugar, los cibercriminales seguirán buscando modelos de negocio que funcionen contra los sectores que son productivos. Esto significa que el ransomware seguirá dominando, generando grandes dividendos para los atacantes. Se espera un impacto a largo plazo a partir de los esfuerzos en lograr la destrucción de los modelos de negocio ilícitos, interrumpiendo los pagos en criptomoneda y mejorando las defensas contra la entrega de ransomware.

La realidad es que los servicios de salud serán probablemente el sector más atacado. Se considera que es más lento para mejorar su seguridad y por razones obvias no puede tolerar la interrupción del negocio. Se espera así un aumento continuado de los ataques contra la manufactura, la tecnología operativa (OT) y un mayor ataque a los sistemas de gestión remota.

Los Estados nación hostiles seguirán con acciones desfavorables y contraproducentes, legitimando la ciberdelincuencia dentro de sus respectivas jurisdicciones: hay pocas posibilidades de acuerdo político a través de las fronteras. En respuesta, los gobiernos occidentales, liderados por Estados Unidos, se volverán más intervencionistas en un esfuerzo por aumentar las defensas en el gobierno y la economía en general.

En tercer lugar, el sector de la ciberseguridad está proyectado a consolidarse cada vez más. Las grandes empresas verán los servicios de seguridad gestionados en la nube como una parte importante de la respuesta; impulsado tanto por la adopción de la nube en toda la empresa, acelerada por la pandemia. Las oportunidades de visibilidad de "panel único", control de datos, cumplimiento, consolidación de productos y optimización de costos serán significativas, abarcando todo el ecosistema.

Todas las empresas necesitarán ayuda externa para gestionar de forma proactiva el riesgo de terceros, así como para evaluar sus cadenas de suministro en tiempo real, clasificar el riesgo y tomar medidas para reducirlo. La industria cibernética tendrá éxito en proporción a su capacidad para automatizar a escala masiva, ofreciendo detección y remediación altamente sofisticadas en todo el ecosistema.

BlueVoyant®

93% de las organizaciones sufrieron una brecha de ciberseguridad debido a debilidades en su cadena de suministro/proveedores externos.

CONFÍE EN NUESTRA PLATAFORMA DE CIBERDEFENSA INTERNA Y EXTERNA LÍDER EN LA INDUSTRIA

Descargar el Reporte

www.bluevoyant.com | contact@bluevoyant.com | 646.558.0052

LOS DESAFÍOS DE LA CIBERSEGURIDAD EN EL TRABAJO HÍBRIDO

Si bien el modelo híbrido implica flexibilidad para los trabajadores y un aumento de productividad para las organizaciones, también trae aparejado nuevos retos en términos de ciberseguridad.

Por Rocio Bravo

Millones de personas en todo el mundo han comenzado a trabajar desde casa en lugar de ir a las oficinas y otros lugares de trabajo durante la pandemia. Según una encuesta global de más de 200.000 personas en 190 países, Boston Consulting encontró que el 89% de las personas esperaba poder trabajar desde casa al menos algunas veces a la semana después de que terminara la pandemia. Y si bien el trabajo desde casa tiene sus méritos, como costos más bajos para las empresas, este aumento también genera algunos problemas de seguridad de TI preocupantes.

Desde DigiCert comparten lo siguiente:

- Transición a la nube. Desde la pandemia, se prefieren las soluciones de acceso remoto y las organizaciones están trasladando gradualmente los procesos comerciales críticos a la nube. Sin embargo, depender cada vez más de la nube y crear agilidad en la nube podría crear más vulnerabilidades si no se asegura adecuadamente. Microsoft descubrió que el 39% de las empresas priorizan las inversiones en seguridad en la nube sobre la seguridad de los datos y la información o incluso la seguridad de la red.

- Suplantación de identidad por correo electrónico. El phishing por correo electrónico durante la pandemia se disparó. Hay una mayor prioridad para capacitar a los trabajadores y prepararlos para reconocer y saber cómo lidiar con las amenazas desde la pandemia y desarrollar las mejores prácticas para el acceso seguro al correo electrónico.

- Diversos dispositivos remotos. Los dispositivos móviles necesitan su propia

protección de seguridad única, pero al 52 % de las organizaciones les resulta difícil proteger los dispositivos móviles de los problemas de ciberseguridad. Un primer paso crítico para resolver esto es implementar una política efectiva de administración de dispositivos móviles (MDM).

- Sin ciberseguridad en la oficina. La empresa es más vulnerable cuando su personal no puede utilizar las medidas de seguridad informática de la oficina, como los cortafuegos.

- Protección de contraseñas. Los empleados deben recibir capacitación sobre las mejores prácticas de la política de contraseñas y su organización debe implementar la autenticación de múltiples factores.

Muchas organizaciones, especialmente las grandes o multinacionales, solían tener prácticas de teletrabajo que se llevaban adelante con medidas bastante acotadas o las mínimas necesarias (en general el uso de VPNs). Para poder sobrellevar la crisis originada por la pandemia y seguir operando en el aislamiento, a esta situación se sumaron aquellas empresas que hace dos años no tenían ninguna práctica ni medidas de trabajo remoto instaladas. Todas ellas debieron hacer un cambio en sus dinámicas laborales de la noche a mañana. Este abrupto vuelco al trabajo a distancia y la hiperconexión, sin dudas incrementó los riesgos de ciberataques, dejando en evidencia las carencias que muchas compañías presentan con respecto a seguridad de datos y de protección de su infraestructura.

"El gran reto que atraviesan hoy las organizaciones es el de desarrollar y mantener un programa de seguridad íntegro, que les permita operar bajo un ecosistema de riesgos identificados y controlados, donde primen la seguridad de la información, protección de los datos, identificación de riesgos, prevención y gestión adecuada de los incidentes de seguridad", plantea **Luis Padilla, Gerente de Business Transformation & Technology de ManpowerGroup Argentina.**

Según el vocero, algunos de los aspectos que siempre han estado pendientes y que forman parte del reto de contar con un programa de seguridad íntegro, son invertir en tiempo y recursos en capacitación y conciencia acerca de la ciberseguridad y la difusión de las buenas prácticas en todos los niveles de la organización. "Aunque suene muy trillado, la realidad es que todos somos responsables de la seguridad en una empresa", remarca.

Luis Padilla

Actualmente ya no alcanza solo con proteger la computadora de la oficina o la red corporativa con las mejores herramientas de encriptamiento, de VPNs firewalls o antivirus. También las computadoras de uso personal, los celulares y las redes sociales se usan para trabajar a toda hora, para conectarnos, para transferir datos, información, etc.

"La información que manejan las compañías y nuestros colaboradores es la que desean los ciberdelincuentes, quienes se aprovechan del desconocimiento de los usuarios y colaboradores para acceder a ella desde cualquier dispositivo y con diferentes técnicas de persuasión", expone Padilla. Por todo esto, "cada vez se requieren mejores skills o habilidades de nuestros usuarios para poder identificar y mitigar situaciones en la que estén siendo parte de un ataque de ciberseguridad".

De acuerdo con **Matías Berardi, SMB Lead para AMD Spanish South America**, se vislumbra que los ciberdelincuentes continúan buscando vulnerabilidades en el trabajo remoto para acceder a las redes corporativas a través de los empleados que trabajan desde sus hogares interceptando sus comunicaciones y redirigiéndolos a sitios maliciosos. De esta manera, dice: "El problema está en que aún muchas empresas no han reparado en la importancia de invertir en plataformas de seguridad integradas, las cuales son fundamentales para tener visibilidad y control de todo dentro de las redes corporativas. Con ataques cada vez más robustos, con grandes grados de sofisticación y eficiencia, los ciberdelincuentes están utilizando tecnologías avanzadas e inteligencia artificial (IA) para desarrollar ataques dirigidos con mayores posibilidades de éxito".

Por su parte, desde Avast, **Jakub Kroustek, su Director de Investigación de Malware,** plantea: "Las VPN mal configuradas, especialmente sin autenticación de dos factores, dejan a las empresas especialmente vulnerables ya que son básicamente una puerta cerrada que protege información extremadamente valiosa que estaría mejor protegida con una segunda cerradura o en una caja fuerte. Este escenario facilita a los ciberdelincuentes el acceso a la red de una empresa, si consiguen hacerse con las credenciales de acceso o pueden descifrarlas".

Praveen Sengar

David López

Otro riesgo relacionado con el trabajo desde casa, sigue el experto, "es que los empleados descarguen datos de la empresa en su dispositivo personal, que puede no tener el mismo nivel de protección que el dispositivo emitido por la empresa".

Para **Praveen Sengar, CEO de ETEK International,** la estrategia de ciberseguridad debe centrarse en los riesgos asociados a las personas (como la falta de conciencia en ciberseguridad), tecnológicos (como el uso de múltiples dispositivos de usuario final para la conexión a los servicios) y, sobre todo, entornos basados en la nube.

Mientras que para Según **David López, vicepresidente de ventas para Latinoamérica** de Appgate, el reto está en la implementación de filosofía basada en el modelo Zero Trust, "que tiene como principios de nunca confiar y siempre verificar, motivando a las empresas a crear un acceso condicional para los colaboradores que trabajan por fuera del perímetro confiable y a controlarlos continuamente, sin importar el lugar en el que estén ubicados".

"En **AppGate** creemos que el paradigma de seguridad que proteja la red y los recursos de la empresa debe estar construido alrededor de las personas y no de la red misma, centrado en la identidad de los empleados más que en sus credenciales (nombre de usuario y contraseña), evaluando en tiempo real si estos deben tener acceso a la información y estableciendo comunicaciones uno a uno entre los colaboradores y los recursos a los que desea llegar. Esto elimina la posibilidad de que el usuario al conectarse tenga acceso a la totalidad de la red o a un segmento importante de ella", explica el ejecutivo.

Cuentas pendientes

Aunque las compañías han avanzado, tomando las políticas necesarias para limitar el acceso de los hackers a su información privada y la de sus usuarios, la realidad es que aún falta mucho por hacer. "Las soluciones a implementarse no deben ser pensadas en función de la protección, sino en la detección y respuesta proactiva para anteponerse a cualquier ciberataque", plantea **Ernesto Blanco, Country Manager de HP Inc. Argentina.**

Sergio Corizzo

Según él, el desafío es considerable y, con el paso del tiempo, gracias al aumento desmesurado de los dispositivos en la era del Internet de las cosas y el aumento de la sofisticación de los delitos cibernéticos, será cada vez más grande, necesitando un nuevo enfoque de seguridad.

Sergio Corizzo, Gerente de Ingeniería y Servicios en Quick Informática, explica que muchas empresas optaron por compartir sus sistemas y servicios en forma abierta a internet, sin ningún tipo de VPN o control de acceso a aplicaciones, lo que genera una gran posibilidad de explotar vulnerabilidades o recibir ataques. "Si bien la cultura se fue adaptando a "conectarse por VPN", hoy creo que no se están validando muchas de las cuestiones mínimas de seguridad e integridad de todos los equipos que se conectan a una red o que acceden a un servicio crítico", dice.

También, agrega, "está pendiente el control de qué información se puede descargar y sacar de las compañías, lo que antes se controlaba bloqueando los periféricos de un equipo y la navegación, para que no se envíe información sensible fuera de la compañía, hoy se puede descargar y trabajar desde casa, sino sería imposible hacer home-office".

Renato Marchi, Sales Engineer para SoLA en WatchGuard, agrega a la lista que "aún hay

empresas que no actualizaron completamente la forma de realizar sus negocios o efectivamente educaron a sus empleados a trabajar de forma segura en un entorno remoto".

Renato Marchi

Las empresas han provisto rápidamente de computadoras portátiles a sus empleados, pero estos dispositivos no solo necesitan seguridad ahora que están fuera de la red, sino que además es importante que nos aseguremos de que no permitan el ingreso de malware y otras amenazas cuando se vuelvan a conectar a la red, ya sea a través de VPN o al volver a la oficina.

Los riesgos del trabajo remoto

Debido a que se ha enviado masivamente a los empleados a trabajar desde sus casas el uso de las VPN ha aumentado vertiginosamente. La migración repentina de los usuarios de la oficina al hogar ha hecho que muchas empresas deban ingeniárselas para ofrecer licencias de VPN a sus empleados. "El riesgo es que sin conectividad VPN, los usuarios no tendrán acceso a los recursos que necesitan o utilizarán conexiones inseguras para acceder a ellos. Es importante tener en cuenta que, sin un sistema de protección en la red en las casas de los empleados, la protección del endpoint se torna aún más importante. Una protección de AntiVirus completa no es más suficiente, una solución completa con EDR y doble factor de autenticación es imprescindible para proteger las credenciales de los empleados y los datos accedidos por ellos", aclara Marchi.

Por su parte, **Marcelo Felman, director de Ciberseguridad de Microsoft Latinoamérica,** destaca los siguientes riesgos:

Continuidad operacional: un negocio puede dejar de operar a causa de un ciberataque, incluso en instancias sensibles como salud o defensa. En este sentido, entre

Marcelo Felman

las amenazas más comunes que enfrentan las empresas está el ransomware, un virus que infecta las computadoras y redes empresariales. Este virus representa un peligro porque encripta, de manera silenciosa, los archivos e información sensible de los dispositivos y luego pide un rescate monetario para su recuperación.

Reputacional: la exfiltración o robo de datos es un ataque al activo más sensible de las organizaciones, los datos, lo cual puede impactar negativamente su imagen hacia el exterior.

Legales o de cumplimiento: el incumplimiento en el tratamiento de los datos, dependiendo de la industria o el caso en particular, puede

llevar a incluso sanciones legales.

Fraude: entre este tipo de riesgos, podemos identificar las estafas de soporte técnico, un tipo de fraude cibernético que adopta la forma de "pop-ups" o ventanas emergentes que se muestran en las computadoras de los usuarios con el objetivo de que estos paguen un cierto monto por "arreglar" problemas falsos.

Otro de los principales factores de riesgo tiene que ver con las contraseñas. Según un estudio de Microsoft, actualmente se realizan 579 ataques de contraseña por segundo, es decir, 18.000 millones al año. Por este motivo, cuenta el ejecutivo, "recientemente anunciamos la disponibilidad general de Microsoft Authenticator o Windows Hello, la cuales ofrecen una forma más personal de iniciar sesión en una cuenta de Microsoft a través del reconocimiento facial, huella digital o un PIN".

Lucas Lavié, MCLA Workspace Sales Engineer para Citrix comparte los resultados de un estudio de Citrix para Argentina en 2021 a los encargados de TI de diferentes empresas. Según el mismo, los principales riesgos de seguridad son: el phishing (54%), ataques ransomware (50%) y malware (40%). "En cualquiera de estos ataques, dirigidos al usuario final, el riesgo para las empresas es la fuga de información corporativa. Al conectarse a través de redes públicas, con dispositivos no autorizados y fuera del edificio corporativo, las organizaciones empiezan a perder control sobre el accionar de su staff, y con ello, se dificulta aún más pensar en una estrategia para protegerlos", detalla el vocero.

Carlos Convit

Planteado de esta manera, el escenario pareciera desolador. Sin embargo, expresa el vocero, "es posible entregar movilidad y habilitar el trabajo remoto sin perder el control ni la visibilidad de la información si se cuenta con las tecnologías adecuadas".

Carlos Convit, Assistant Vice President GM Sectec, agrega que los riesgos asociados al trabajo remoto se fundamentan en cómo este puede impactar los principios del triángulo de la CIA (por sus siglas en inglés confidenciality, integrity and availability) en función a la probabilidad de que esto ocurra por estar trabajando remotamente. "Al trabajar remotamente, si bien obtenemos varios beneficios, también estamos introduciendo nuevos riesgos a la organización como la suplantación de identidad, infección de malware y el robo de información confidencial".

Cómo lograr entornos laborales seguros

Para el vocero de Watchguard son 8 puntos los principales que un administrador de red/seguridad debe tener en cuenta para proteger los ambientes laborales y sus empleados:

1 Evalúe las capacidades de trabajo local y remoto que tiene su empresa. Con el aumento del número de ataques de ransomware y amenazas avan-

zadas, ahora es el momento de auditar y evaluar el nuevo acceso a la red que requiere su empresa, y tener en cuenta las consecuencias que eso puede tener en la seguridad. Los proveedores de servicios de seguridad administrada (MSSP) son expertos en evaluación de seguridad y pueden ayudar a las medianas empresas a lograr estar a la altura rápidamente y brindar a sus usuarios lo que necesitan.

2 Establezca y comunique las políticas de seguridad y expectativas para el trabajo dentro y fuera de la oficina. Es probable que muchos de sus empleados estén trabajando desde sus casas por primera vez, es un excelente momento para explicarles las políticas de su empresa respecto al "trabajo desde casa" y refrescar las políticas de trabajo en la oficina. Es importante establecer las expectativas en relación a los empleados. Un simple correo electrónico, o una llamada en conferencia con su equipo, puede ser muy útil.

3 Promueva la cultura de la seguridad cibernética. Debido a que sus empleados están bajo amenaza de ataques dirigidos la cultura corporativa con frecuencia termina siendo un factor determinante que consigue interceptar el ataque o infectar a toda su red. Los actores maliciosos utilizan técnicas como phishing para manipular a sus usuarios usando como arma la autoridad y la urgencia. Los administradores de la empresa deben estimular el uso de canales de comunicación abiertos, de forma tal que cuando un empleado, incluso los de menor jerarquía de la organización, vea algo que considere una amenaza, sienta la tranquilidad de que su preocupación será tenida en cuenta.

4 Implemente soluciones de multifactor de autenticación. Los hackers tienen cada vez más interés en las credenciales de los empleados, y tienen la mira puesta en la información de las cuentas de sus usuarios. Por este motivo, es importante implementar la autenticación multifactor (MFA) para todos los usuarios cada vez que se conecten a su red. La solución les debe permitir proteger el acceso a aplicaciones y entornos en la nube a los que los trabajadores remotos podrían acceder directamente desde la internet.

Ofrezca acceso de VPN a sus usuarios (con una solución de multifactor). Las redes privadas virtuales (VPN) agregan una capa de seguridad a las redes privadas y públicas, lo que permite a sus empleados enviar y recibir datos de manera segura cuando trabajan de forma remota

5 Mantenga a los usuarios protegidos con filtrado de DNS basado en la Nube. Utilizar un filtrado de DNS permite bloquear conexiones y limitar el acceso a áreas de riego en la internet. Es posible evitar hacer clic en enlaces maliciosos o intentar conectarse a dominios relacionados con la suplantación de identidad (phishing) y malware, sin tener que usar una VPN

6 Proteja los Endpoints contra malware avanzado con un EDR. Las amenazas de malware y ransomware han aumentado significativamente en los últimos años tanto para usuarios que trabajan dentro y fuera de las oficinas. Las soluciones de antivirus tradicionales detectan muchas de las amenazas, pero no tienen poder alguno frente al malware evasivo y persistente de día cero, más y más común en los días de hoy. Las soluciones de detección y respuesta de endpoints (EDR) no solo pueden detectar estas amenazas avanzadas, sino que también pueden eliminarlas y hacer que el dispositivo infectado vuelva a funcionar con normalidad, todo de manera remota sin la necesidad de una VPN o de estar por detrás de un firewall.

7 Conserve el control de la red Wi-Fi con una protección WIPS completa. Nos olvidamos de que, muchas veces, un actor malicioso puede estar más cerca de lo que

pensamos. Un ataque en el entorno inalámbrico de la oficina y hogares de los empleados pueden convertirse en una puerta de entrada para vecinos maliciosos que buscan entrar sin permiso. Los hackers o, vecinos maliciosos, podrían aprovechar el hecho de que casi el 50% del tráfico de IP es ocupado por Wi-Fi y tomar provecho de esta situación para adentrar la red o infectar un dispositivo conectado en la misma. Es importante que los administradores de red consideren APs con una solución completa de WIPS (Wireless Intrusion Prevention System) para proteger los dispositivos WiFi conectados en la red corporativa y educar a los empleados a siempre utilizar una VPN cuando conectados en una red no confiable como un WiFi público o en una red con muchos dispositivos desconocidos o IoT.

Para el ejecutivo de Quick Informática, no existe una receta, "es un camino por recorrer", remarca. Tampoco existe un ambiente 100% seguro, "pero a la seguridad tecnológica es muy importante sumarle la capacitación del personal en materia de ciberseguridad, los usuarios tienen que conocer los riesgos, estar al tanto de los métodos de ataques y estafas y el correcto uso de las tecnologías", asegura.

Por último, desde Appgate destacan tres aspectos claves para abordar esta problemática en el trabajo híbrido. "Lo primero es la inversión, ya que no todas las instituciones han decidido innovar en temas de ciberseguridad, quedando rezagadas de aquellas que sí han decidido invertir para proteger recursos e información sensible que pueda tener la organización", dice su responsable. "Además, contar con un modelo de riesgos resulta de gran utilidad, ya que en muchas ocasiones el plan de seguridad informática de la empresa no está diseñado para un evento de crisis y se basa en tecnologías antiguas; por lo que prever situaciones críticas en estos temas les permitirá estar a la vanguardia y responder de mejor manera ante las situaciones que se presenten". Finalmente, "la cultura de los colaboradores con relación a la ciberseguridad, para poder implementar el teletrabajo de buena manera. Una conciencia cibernética de las personas es esencial para poder asegurar los activos de una organización; es muy importante instruir al personal respecto a las buenas prácticas que se deben tener al respecto".

"Las organizaciones deberían hacer de la seguridad una parte clave de sus estrategias"

Por Miguel Llerena, Vicepresidente Regional para LATAM de Tanium

Miguel Llerena
Vicepresidente Regional para LATAM de Tanium

El trabajo remoto y la proliferación de dispositivos que lo acompañan, han aumentado el área de ataque para los ciberdelincuentes. La rápida transición a la virtualidad ha dejado a muchas organizaciones con serios problemas para implementar la infraestructura necesaria.

De acuerdo con una investigación de Tanium, el 61% de las organizaciones observan dificultades para cambiar su fuerza laboral a un esquema de trabajo remoto. Esto ha implicado que las organizaciones que carecen de sistemas de ciberseguridad sólidos se conviertan en objetivos atractivos para los ciberdelincuentes, que se aprovechan de las vulnerabilidades y, en algunos casos de alto perfil, mantengan los datos de la empresa a cambio de un rescate.

En este sentido, la incapacidad para regular el comportamiento de los trabajadores remotos es un desafío común, ya que muchos empleados se enfrentan a más distracciones en el hogar y se involucran en comportamientos cibernéticos más riesgosos de lo habitual, por ejemplo, hacer clic en enlaces de correo electrónico de phishing, filtrar datos confidenciales y utilizando aplicaciones no autorizadas.

De manera similar, un aumento reciente en los ataques de ransomware está demostrando ser una amenaza importante y una preocupación comercial continua. Los ciberdelincuentes generalmente obtienen acceso a los sistemas de la empresa atrayendo a los empleados con correos electrónicos fraudulentos de phishing. En tales casos, todo lo que se necesita es una persona distraída y un clic para dar acceso no autorizado a una banda de ransomware a los sistemas de una empresa.

En 2022 las organizaciones deberían hacer de la seguridad de las herramientas de colaboración una parte clave de sus estrategias de seguridad. Al respecto, deberán tomar decisiones importantes sobre cómo administrar las plataformas, como permitir que personas ajenas a la organización las usen o si solo se les da acceso a los miembros permanentes del personal. Además, los programas de capacitación en seguridad deben actualizarse para cubrir específicamente las amenazas que los usuarios podrían encontrar en las plataformas de colaboración.

¿Cómo se podría abordar esta problemática desde una perspectiva de la ciberseguridad?

Con las amenazas de ransomware en aumento y en evolución, y una línea cada vez más delgada entre las redes internas y externas, las empresas deben buscar prioridades en la ciberseguridad para el bien de todas las partes. Muchas soluciones VPN luchan por adaptarse al volumen de empleados que trabajan de forma remota, lo que dificulta que los equipos se desempeñen a la velocidad y capacidad necesarias. Aquí es donde se necesita un modelo operativo alternativo más eficiente y capaz, como la confianza cero, para satisfacer las necesidades de ciberseguridad de una empresa moderna.

Claves para asegurar un entorno seguro en los ambientes laborales

Para Mauro Graziosi, CEO de SMARTFENSE, la ciberseguridad es un gran desafío dado que muchas medidas de ciberseguridad estaban implementadas dando por hecho de que los empleados trabajaban en un entorno físico y lógico controlado y ahora no están bajo su control ninguno.

Mauro Graziosi, CEO de SMARTFENSE

"Es un reto aún más presente porque ante la digitalización acelerada por la pandemia muchas medidas se han hecho de forma poco metódica y expuso a la organización y sus empleados a mayores riesgos", agrega el experto.

Como pendiente, está la aplicación de medidas que tengan en cuenta este ambiente híbrido, donde requiere re balancear los controles para que el perímetro físico pase a un segundo plano y se ponga al usuario y la información en foco. Hoy en día se sigue pensando en una protección tanto a nivel de confidencialidad, integridad y disponibilidad enfocada en el período previo o de transición, pero a los tecnólogos les cuesta pensar más allá de la solución de problemas específicos y diagramar una estrategia global de protección en un ambiente híbrido.

En este sentido, surgen riesgos que tienen que ver con el desconocimiento del flujo de información en un ambiente híbrido y la falta de gestión del riesgo humano. Con esto último, explica Graziosi, "me refiero desconocer cuál es el grado de exposición de la organización por el personal poco concientizado y, por otro lado, no tener un programa integral de concientización y medición".

Teniendo en cuenta esto, para abordar esta problemática desde una perspectiva de la ciberseguridad, es clave establecer una línea base del riesgo del factor humano a través de la medición del comportamiento, por ejemplo, con ejercicios de simulación de phishing y ransomware. Luego diseñar un plan anual de concientización para disminuir paulatinamente el riesgo hasta los niveles aceptables para la organización.

Por último, el responsable de SMARTSENSE plantea ponerse en los zapatos del trabajador, entender cuál es su situación actual en todo sentido. Y ejemplifica: "Ver si en su ambiente de trabajo está cómodo, si tiene todo lo que necesita, si le gusta teletrabajar o no (o un mix), si necesita complementar el teletrabajo con otras acciones, si se siente cómodo con la supervisión actual, si los sistemas están preparados para este entorno, si necesita tener momentos de interacción con otros colegas para evitar la soledad, si está pensando en irse, etc. Darle un espacio para expresarse. Una vez que se conoce la situación del empleado, ver si los sistemas y las medidas de seguridad deben adaptarse a esta nueva realidad y obviamente aprovechar la oportunidad para revisar todo lo vinculado al control de acceso a la información".

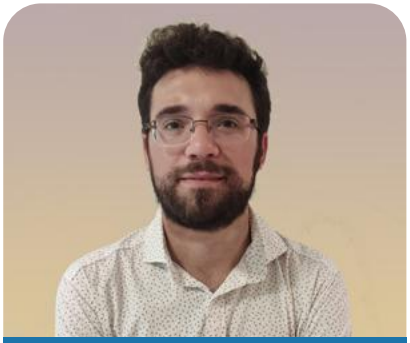
SMARTFENSE

Nueva imagen, Misma esencia.

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

Los riesgos del trabajo híbrido

En 2019, las empresas veían el trabajo remoto como algo lejano. Con la pandemia, la adaptación pasó a estar dentro de la agenda de prioridades y hoy muchas compañías siguen en este proceso.



Ariel Filippazzo
Cybersecurity Solution Sales de Softline

"La nueva modalidad de trabajo nos obliga a prestar especial atención en la seguridad: durante los casi dos años del COVID-19, los ataques cibernéticos aumentaron de forma exponencial y, según diversas fuentes, Argentina es uno de los países con mayor cantidad de ciberataques luego de Brasil", comparte Ariel Filippazzo, Cybersecurity Solution Sales de Softline.

Los riesgos aumentaron porque en la misma proporción también aumentó la concentración de los ciberdelincuentes en las vulnerabilidades: desde las estafas de phishing hasta el malware relacionado con el COVID-19, los hackers se aprovechan del trabajo descentralizado y/o los sistemas de TI encontrando grietas por donde filtrarse.

Por este motivo, dice el vocero, "este año una de las tendencias del sector es la implementación de los diferentes métodos de seguridad para defensa de los activos de IT de los ataques cibernéticos".

Un largo camino por recorrer

Las campañas de phishing siguen siendo el principal modo de ataque dado que depende casi un 100% del factor humano. Por más protegido que esté el sistema, si el usuario cae en la trampa de hacer click donde no debe o dejar sus datos sin tener claro los riesgos, la seguridad se desploma.

Queda al descubierto la otra cara del trabajo híbrido: desempeñar las funciones lejos de un equipo de trabajo también nos hace más proclives a caer en trampas, porque, dentro de los ejemplos más comunes, recibimos un email o tenemos que entregar datos.

Las botnets y los dispositivos IoT: es una de las mayores amenazas de los últimos años, y ha generado un gran interés en los atacantes; En esta modalidad, apuntan a vulnerabilidades más antiguas en productos de IoT para incrementar la fuerza de la red. Los ciberdelincuentes son conscientes de que los dispositivos de IoT están menos protegidos ya que no suelen contar con las últimas actualizaciones de seguridad, esto les permite aprovecharlos para incrementar así su red de ataque.

Frente a este contexto es determinante entender qué medidas de seguridad son importantes tomar a la hora de defender una empresa que utiliza la modalidad Home Office: capacitación del personal de forma frecuente; uso obligatorio de apps seguras para levantar redes privadas virtuales (VPN) y contar con firewall y antimalware. También, el uso del multifactor de autenticación en casi cualquier aplicación corporativa; la habilitación de las actualizaciones de seguridad de forma automáticas en los dispositivos; el uso exclusivamente de dispositivos entregados por la empresa, verificados y controlados por el equipo de TI; y la verificación de las redes WiFi de cada colaborador, no aceptar cualquier red abierta, es importantísimo.

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

El equilibro en SecurityUX

Imaginemos un escenario en el que no se necesita una contraseña para iniciar sesión y consultar el correo electrónico; por otro lado, un aplicativo donde se necesita autenticar las credenciales cada pocos minutos usando códigos CAPTCHA. Sin duda, el primer escenario es muy agradable desde el punto de vista de la experiencia del usuario, pero carece de seguridad. Por el contrario, el segundo es extremadamente seguro, pero es muy irritante desde la perspectiva de la experiencia del usuario, y nadie estaría interesado en usarlo. Es aquí donde las organizaciones deben aprender a equilibrar la experiencia del usuario y la seguridad.

El vínculo entre la experiencia del usuario (UX) y la seguridad se ha estudiado muy de cerca académicamente y se conoce como HCISec (también conocido como HCI-SEC o Human Computer Interaction and Security). Los profesionales de la seguridad deben ser plenamente conscientes del hecho de que, si bien deben dar la máxima prioridad a la seguridad del sistema, no pueden pasar por alto la experiencia del usuario. Deben asegurarse de que solo los usuarios autorizados tengan acceso al sistema y también asegurarse de que los usuarios estén seguros sabiendo que su información está segura en línea y que pueden continuar usándola de manera segura.

Las amenazas cibernéticas a una organización

Uno de los mayores fraudes en línea que la mayoría de los usuarios temen es el robo de identidad. No sólo destruye la reputación, sino que también puede provocar importantes pérdidas financieras para las organizaciones. En un momento dado, más de 2 mil millones de personas navegan por Internet e inician sesión para acceder a la información guardad y almacenada. Los spammers y los piratas informáticos pueden tener un día de campo tratando de piratear la información personal de los usuarios. Por ejemplo, la mayoría de las aplicaciones web tienen una capa de conexión segura adicional que se puede verificar mediante su URL que comienza con https:// en lugar de http://. Pero, también, incluso esta capa no es inmune a los ataques cibernéticos y puede ser explotada por un ataque de intermediario, que puede interceptar información confidencial del usuario y es un ejemplo clásico de robo de identidad.

> “Los profesionales de la seguridad deben ser plenamente conscientes del hecho de que, si bien deben dar la máxima prioridad a la seguridad del sistema, no pueden pasar por alto la experiencia del usuario.”

¿Qué pueden hacer las empresas?

En el mundo cada vez más cibernético, no será fácil determinar que uno es quien realmente dices ser. Se ha vuelto necesario que las organizaciones utilicen la gestión de acceso e identidad para reforzar la seguridad y proteger la información confidencial. Los servicios de autenticación de identidad se aseguran de que los usuarios sean realmente quienes dicen ser. Las industrias necesitan:

- Es importante asegurarse doblemente de que los datos de los usuarios estén seguros, por medio de la incorporación

de capas adicionales de encriptación. Cuando las empresas emplean dichos servicios, deben tener en cuenta que la implementación de servicios de autenticación de identidad no debería causar inconvenientes a los usuarios. La seguridad y la protección son de gran importancia, pero eso no tiene una implicancia de que los usuarios deban estar sometidos a una experiencia en línea negativa.

- Trabajar junto con los profesionales de seguridad para crear servicios de autorización y verificación de identidad que puedan integrarse perfectamente y facilitar las transacciones de los usuarios
- Considerar emplear los servicios de una empresa que brinde tales servicios y ayude a proteger la identidad y la información en línea de sus clientes, mientras les brinda una experiencia sin esfuerzo.
- Crear un sistema que tenga capas de seguridad y que además brinde una experiencia agradable al usuario.

El objetivo principal de los profesionales de la seguridad debe ser maximizar la experiencia grata del usuario, minimizar las infracciones de seguridad, crear un sistema que disuada a los atacantes y que sea extremadamente fácil de usar. Como empresa comprometida con evitar el uso indebido de la información de los usuarios, pensar seriamente en la experiencia y la seguridad del usuario, porque incluso si se descuida algún aspecto, se terminará obteniendo un sistema que tiene fallas de seguridad o usuarios muy insatisfechos.

¿Pueden convivir en armonía la experiencia del usuario y la seguridad?

Sí, se puede. Para la mayoría de los aplicativos, adherirse a los principios como también a las pautas de la experiencia del usuario puede mejorar la seguridad.

Por ejemplo, tomemos este caso. Supongamos que alguien le pide que le recomiende un buen navegador web. Hay dos browsers entre los que puede elegir. El primero oculta su configuración debajo de una barra de herramientas poco clara, utiliza controles obsoletos, contiene mu-

cha jerga técnica y carece de ayuda para las opciones avanzadas. El segundo es exactamente lo contrario. Los botones de su barra de herramientas están claramente etiquetados, tiene controles de selección simples, un lenguaje fácil de entender y ayuda contextual. Suponiendo que ambos navegadores tengan el mismo nivel de seguridad, ¿qué navegador web recomendarías?

¡El segundo navegador, por supuesto!

La razón es simple: si cualquiera de los navegadores detecta un problema de seguridad, imaginemos lo engañoso, como también difícil, que sería entender lo que está sucediendo (bajo un estado de pánico que acompaña a cualquier violación de seguridad) cuando se usa un navegador web que es difícil de usar incluso en circunstancias normales…
La experiencia del usuario y la seguridad son esenciales para cualquier sistema. De hecho, recientemente se ha descubierto que 2 de cada 3 usuarios abandonan una compra utilizando su dispositivo móvil debido a una mala experiencia de usuario y problemas de seguridad.

En el extremo de la opinión entre la experiencia del usuario y el debate sobre la seguridad, algunos incluso llegan a decir que la experiencia del usuario anula la seguridad. De hecho, las principales preocupaciones de los diseñadores de experiencia de usuario (UX) y los profesionales de la seguridad radican en estas preguntas:

- Para los diseñadores de experiencia de usuario (UX), la pregunta es: ¿Cómo se diseña la experiencia de seguridad para que se ajuste a las necesidades de la identidad digital? Detrás de cada identidad hay una persona con las mismas necesidades básicas que todos, la jerarquía de necesidades tiene como origen una excelente experiencia de usuario.

- Para los profesionales de la seguridad, la pregunta es: ¿Cómo habilitar el negocio de sus clientes en un entorno en el que la velocidad y la comodidad eviten anular la comprensión tradicional de la seguridad? Que la aplicación, por supuesto cuente con las mejores prácticas en materia de ciberseguridad.

El arte de lograr el equilibrio adecuado entre la experiencia del usuario y la seguridad aún está evolucionando dinámicamente. Los usuarios también se vuelven más responsables con cada día que pasa, pero lamentablemente a la mayoría aún no le importa una capa adicional de seguridad antes de poder acceder a su información personal, si eso tiene la implicancia de una seguridad adicional.

Por supuesto, esto cambiaría si los usuarios son concientizados, educados, más que nada instruidos sobre los riesgos en materia cibernética.

Rusia, Ucrania y la ciberguerra

Han surgido informes que arrojan luz sobre un elemento opaco de la guerra entre Rusia y Ucrania: la ciberguerra. Muchos expertos predijeron que Rusia lanzaría importantes ataques cibernéticos en Ucrania, apagando la red eléctrica del país, por ejemplo. Pero, aunque las operaciones a gran escala no se han materializado, a la escritura de esta nota, empiezan a surgir informes de incursiones más pequeñas.

El lunes 7 de marzo Google dijo que había descubierto ataques de phishing generalizados dirigidos a funcionarios ucranianos y militares polacos. La empresa de seguridad Resecurity Inc. también compartió pruebas de una campaña coordinada de piratería informática dirigida a empresas estadounidenses que suministran gas natural (un producto que se ha convertido en un elemento crítico a medida que las sanciones occidentales afectan a las exportaciones energéticas rusas). En ambos casos, los ataques podrían estar vinculados a grupos asociados con Rusia y sus aliados.

El Grupo de Análisis de Amenazas (TAG) de Google dijo que la campaña de phishing se dirigió a los usuarios de UkrNet, una compañía de medios de comunicación ucraniana, así como a "organizaciones gubernamentales y militares polacas y ucranianas". Los ataques fueron realizados por grupos como el bielorruso Ghostwriter y el ruso Fancy Bear.

"En las últimas dos semanas, TAG ha observado la actividad de una serie de actores de amenazas que monitoreamos regularmente y que son bien conocidos por las fuerzas de seguridad, incluyendo FancyBear y Ghostwriter", escribió Shane Huntley de Google en una entrada de blog. "Esta actividad va desde el espionaje hasta las campañas de phishing. Estamos compartiendo esta información para ayudar a concienciar a la comunidad de seguridad y a los usuarios de alto riesgo."

La campaña dirigida a las empresas de gas natural de EE.UU. logró infiltrarse en más de 100 computadoras pertenecientes a empleados y exempleados. Se desconocen los motivos de la operación, pero Resecurity describió el trabajo como un "preposicionamiento", es decir, el hackeo de máquinas para preparar una operación mayor de algún tipo.

> "Google dijo que había descubierto ataques de phishing generalizados dirigidos a funcionarios ucranianos y militares polacos."

Los ataques comenzaron dos semanas antes de la invasión de Ucrania, y asegurar un punto de apoyo en los proveedores de gas de EE.UU. ciertamente ofrecería muchas oportunidades de influencia geopolítica. A medida que los países europeos han tratado de desprenderse del gas natural ruso como parte de una serie de sanciones económicas, las empresas energéticas de Estados Unidos han aumentado su suministro, convirtiendo a este país en el principal proveedor mundial de gas natural licuado o GNL.

El director general de Resecurity, Gene Yoo, declaró a Bloomberg que creía que el ataque había sido llevado a cabo por piratas informáticos patrocinados por el Estado, pero no especuló sobre quién podría ser.

Inteligencia Artificial por una Ciberseguridad mejor

La IA está cambiando el rol de la ciberseguridad, analizando cantidades masivas de datos de riesgo para acelerar los tiempos de respuesta y aumentar las operaciones de seguridad con recursos insuficientes.

> “Las tecnologías de inteligencia artificial permiten a los analistas responder a las amenazas con mayor confianza y velocidad.”

En la medida en que los ataques cibernéticos aumentan en volumen y complejidad, la inteligencia artificial (IA) está ayudando a los analistas de operaciones de seguridad con escasos recursos a adelantarse a las amenazas. Sin dudas, la inteligencia artificial proporciona información instantánea para ayudar a luchar contra el ruido de miles de alertas diarias, reduciendo drásticamente los tiempos de respuesta.

Qué se espera de la Inteligencia Artificial

Las tecnologías de inteligencia artificial como el aprendizaje automático y el procesamiento del lenguaje natural permiten a los analistas responder a las amenazas con mayor confianza y velocidad.

El aprendizaje

La inteligencia artificial se retroalimenta, consumiendo miles de millones de artefactos de datos de fuentes estructuradas y no estructuradas, como blogs e historias de noticias. Mediante técnicas de aprendizaje automático y aprendizaje profundo, la IA mejora su conocimiento para “comprender” las amenazas de ciberseguridad y el riesgo cibernético.

La reacción y la respuesta
La IA recopila conocimientos y utiliza el razonamiento para identificar las relaciones entre las amenazas, como archivos maliciosos, direcciones IP sospechosas o personas con información privilegiada. Este análisis toma segundos o minutos, lo que permite a los analistas de seguridad responder a las amenazas hasta 60 veces más rápido.

La reducción de tiempo

La inteligencia artificial elimina las tareas de investigación que consumen mucho tiempo y proporciona un análisis curado de riesgos, lo que reduce la cantidad de tiempo que los analistas de seguridad tardan en tomar las decisiones críticas y lanzar una respuesta orquestada para remediar la amenaza.

Seguridad proactiva

La seguridad cognitiva combina las fortalezas de la inteligencia artificial y la inteligencia humana. La IA cognitiva aprende con cada interacción para detectar y analizar amenazas de forma proactiva, proporcionando información útil a los analistas de seguridad para que tomen decisiones informadas, con velocidad y precisión.

Factor crítico: las personas

Esta carrera tecnológica ha propiciado innumerables avances y desarrollos en la infraestructura tecnológica de compañías e instituciones, pero no podemos olvidar un factor crítico: las personas, sistemas con cientos de vulnerabilidades conocidas desde el principio de los tiempos, la gran mayoría de las cuales siguen sin corregirse.

Según datos recogidos por Proofpoint, el 20% de los usuarios habría interactuado con correos electrónicos que contenían archivos maliciosos, y otro 12% habría accedido a enlaces proporcionados en dichos correos. Diversas fuentes sitúan el porcentaje de fugas de datos inducidas por los empleados entre el 88% y el 95%. Ignorar este factor humano en la ciberseguridad supone un enorme riesgo para las organizaciones.

Hackear al humano

El conjunto de técnicas y procedimientos utilizados para intentar motivar al usuario a realizar alguna acción a favor de los ciberdelincuentes se conoce como Ingeniería Social. Aunque también se le conoce con otros nombres más artísticos, como "manipulación mental" o "hacking humano", no es más que otro ejemplo de persuasión o cambio de actitud.

En este contexto, en psicología se propone el Modelo de Probabilidad de Elaboración (ELM - Elaboration Likelihood Model). El nivel de elaboración de una persona se basa en dos factores: su capacidad para entender el mensaje y su motivación para hacerlo. Para ser sinceros, cuando leemos correos electrónicos un lunes por la mañana antes de nuestro primer café, no tenemos ninguna de las dos cosas.

Los cambios de actitud que se producen en un sujeto altamente procesado son manejados por la llamada "vía central", y son más profundos y duraderos en el tiempo, pero requieren argumentos más fuertes para surtir efecto. Afortunadamente para los ciberdelincuentes, basta con que duren los segundos necesarios para que las víctimas sigan un enlace o introduzcan sus credenciales, por lo que no necesitan estar prestando demasiada atención.

Un empleado bajo el efecto de factores como la fatiga, el estrés o el sueño es la víctima perfecta de la ingeniería social. Esto no significa necesariamente que si estamos en perfectas condiciones no podamos ser víctimas de las mismas técnicas, pero sí nos hacen enormemente vulnerables.

> "Las personas: sistemas con cientos de vulnerabilidades conocidas desde el principio de los tiempos, la gran mayoría de las cuales siguen sin corregirse."

Detección y concientización

Tanto las compañías como los usuarios pueden tomar medidas para intentar reducir el éxito de estas técnicas de ingeniería social. Entre ellas, campañas de concienciación y formación en la detección de mensajes y actividades fraudulentas u ofrecer canales de denuncia para que los usuarios puedan alertar en caso de detectarlas, entre otras.

Como usuarios, también a nivel personal, es importante ser conscientes de nuestra huella digital: la información disponible sobre nosotros en el ciberespacio puede ser utilizada para dirigir con mayor precisión los ataques mediante ingeniería social.

En palabras del criptógrafo y experto en seguridad informática Bruce Schneier: "Si crees que la tecnología puede resolver tus problemas de seguridad, ni entiendes los problemas, ni entiendes la tecnología".

"Endpoint Explosion" y Monitoreo Continuo

La computación en la nube y el coronavirus se encuentran entre las fuerzas más importantes que afectan la ciberseguridad en la actualidad. Juntos, han creado el concepto "endpoint explosion".

Claramente, la pandemia está acelerando la migración a la nube. Casi por definición, la computación en la nube facilita el distanciamiento social. También apoya el movimiento más amplio hacia un entorno de trabajo reinventado y de densidad reducida, una tendencia que probablemente continuará incluso después de que termine la pandemia.

Endpoint Explosion

La migración a la nube y el coronavirus están creando una explosión de endpoints. Más criterios de valoración significan más exposición al riesgo. La nube facilita la creación rápida de activos orientados a Internet, como webs y bases de datos, todos los cuales tienen superficies de ataque vulnerables. La nube crea más puntos de acceso digitales para empleados, clientes y proveedores. Facilita la adopción de aplicaciones nuevas y más amplias, agregando puntos finales de riesgo cibernético adicionales.

El coronavirus contribuye aún más a la explosión actual de endpoints. Para junio de 2020, una amplia gama de la fuerza laboral trabajaba desde casa a tiempo completo. Se estima que una gran porción de ese staff trabajará desde casa varios meses más para fines del 2021 y mediados de 2022.

Estos nuevos endpoints introducen una abrumadora cantidad de nuevas vulnerabilidades cibernéticas y nuevas superficies de ataque en las que los actores de amenazas pueden aprovecharse.

Las medidas periódicas de ciberseguridad son una base necesaria. Son importantes las mejoras de seguridad, como la formación de los empleados, contraseñas más seguras, controles de acceso, cortafuegos, pentesting y puntuación de riesgo del proveedor. Pero no pueden seguir el ritmo del crecimiento de las superficies de ataque iniciadas por la computación en la nube y la pandemia. En la actualidad, la mejor esperanza para una gestión eficaz de la ciberseguridad es la supervisión en tiempo real.

> "Estos nuevos endpoints introducen una abrumadora cantidad de nuevas vulnerabilidades cibernéticas y nuevas superficies de ataque."

Monitoreo continuo

El monitoreo en tiempo real verifica las amenazas agregadas, identifica señales de alerta y monitorea continuamente los riesgos potenciales. Idealmente, los descriptos:

- El adoptar el punto de vista de un pirata informático sobre las brechas en todas las posibles superficies de ataque.
- Identificar puntos que pueden ser ciegos como también vulnerabilidades en todo el contexto digital: empresa, clientes y proveedores.
- El funcionar 24 horas al día, 7 días a la semana.
- El proporcionar notificación inmediata de actividad no autorizada.
- El habilitar la reparación rápida y detención de las amenazas potenciales antes de que se pierdan los datos privilegiados.
- Estar basados en la nube y tener que instalar ninguna clase de software.
- Ser sencilla la implementación.
- Los administradores pueden cargar sus activos conectados a Internet en un tablero, y la Solución lo toma desde allí.

Las tendencias nos dicen que el movimiento hacia el monitoreo en tiempo real se acelerará. Esto se debe a la demanda de interconexión digital, la creciente sofisticación de las amenazas cibernéticas y la relevancia cada vez menor de la atribución de amenazas.

Interconexión digital

La necesidad de conexiones digitales entre empresas, clientes y proveedores seguirá creciendo. Esto subyace en el mandato estratégico de la transformación digital. La nube satisface esta necesidad al hacer que la creación de sitios web y bases de datos sea barata y fácil.

Sin embargo, la transformación digital expone a las empresas a un panorama de amenazas más amplio. Si bien los ecosistemas digitales son una necesidad empresarial estratégica, también introducen una gama más amplia de riesgos cibernéticos.

Los niveles de amenazas cibernéticas seguirán aumentando más rápido que las capacidades de defensa empresarial, lo que generará

crecientes riesgos de ciberseguridad. Los actores de amenazas, que van desde individuos autónomos hasta estados-nación, continuarán encontrando y explotando con éxito las brechas en el panorama global cada vez más conectado.

Existen atacantes financiados por diversos Estados, que ahora emplean a algunas de las mejores mentes del mundo. Secuestran protocolos inalámbricos patentados y dispositivos conectados (IoT, smartphones, VoIP, mouse como teclados wireless, impresoras, etc.) para intrusar en las redes corporativas o capturar las pulsaciones de teclas y las acciones del mouse. Incluso utilizan la infraestructura del estado-nación rival para albergar, desplegar y disfrazar sus ataques.

> “Si bien los ecosistemas digitales son una necesidad empresarial estratégica, también introducen una gama más amplia de riesgos cibernéticos.”

Reducción de la “atribución” de amenazas

Cada vez es más difícil atribuir amenazas cibernéticas a actores específicos. Las amenazas avanzadas se originan cada vez más a partir de malware de usuario. La experiencia en tácticas, técnicas y procedimientos del espacio de usuario es mucho más relevante que la capacidad de identificar a los creadores de malware. Cada nodo del ecosistema digital, desde la empresa hasta el cliente y el proveedor, es un punto potencial de incursión. La anticipación, detección y respuesta de amenazas en tiempo real en cualquier punto final son ahora la primera línea de la ciberseguridad.

Implicaciones estratégicas

La ciberseguridad se está adaptando al panorama globalmente conectado y las amenazas asociadas de seis formas. Estas seis formas son las siguientes:

- Velocidad: cada vez más, el factor que impulsa el éxito en la ciberseguridad es la velocidad. ¿Con qué rapidez podemos detectar y responder a una amenaza emergente? Mejor aún, ¿con qué rapidez podemos detectar anomalías en nuestro escenario tecnológico, como también lanzar respuestas efectivas antes de que se propague la amenaza?
- Monitoreo en tiempo real y análisis de transmisión: la clave para la velocidad de la ciberdefensa es el monitoreo de endpoints y el análisis de transmisión en tiempo real. Las pruebas periódicas, las encuestas de ciberseguridad de los proveedores y la puntuación de riesgo de los proveedores perderán relevancia. Son lentos en relación con la detección y evaluación de riesgos en tiempo real en un panorama de riesgos en constante cambio.
- Incremento del papel de la IA: las empresas no pueden responder rápidamente a todas las alertas cibernéticas que reciben. Los procesos de triaje de alertas manuales a menudo se ven abrumados por los volúmenes de alertas. La IA es una solución cada vez más viable, especialmente para el análisis de transmisión en tiempo real. Se puede utilizar para automatizar la

búsqueda de amenazas y la clasificación de alertas de primera ronda. Esto, a su vez, reduce el número de falsos positivos y ayuda a los equipos de operaciones de seguridad a centrarse en las amenazas de alta prioridad.

- Integración de la ciberseguridad: la complejidad de la ciberseguridad requiere la utilización de una amplia gama de tecnologías. Los procesos de gestión de ciberamenazas en los activos de la información varían para la empresa frente a los clientes frente a los proveedores externos. Dentro de la empresa, la gestión de amenazas varía para los empleados, los dispositivos de los empleados, los sistemas de control de fabricación y distribución, los productos habilitados para IoT, etc. Estos diversos subsistemas de ciberseguridad se integrarán cada vez más. La ingesta de datos se integrará a través de lagos de datos. La inteligencia artificial y el análisis de transmisión se aplicarán a estos lagos de datos. El seguimiento y los conocimientos del ecosistema digital se agregarán mediante la unificación de plataformas.

- Organismos, Concilios, Entidades y Asociaciones de ciberseguridad: las empresas establecerán cada vez más acuerdos con proveedores y clientes para detectar y responder a las amenazas cibernéticas. Los contratos comerciales requerirán cada vez más que ambas partes compartan inteligencia sobre amenazas en tiempo real.

- Outsourcing: Los centros de operaciones de seguridad (SOC) ya luchan con la dotación de personal. Pueden verse abrumados por los volúmenes de alerta y los procesos manuales. Los problemas de personal de SOC se intensificarán con la creciente importancia de los análisis de transmisión en tiempo real y habilitados para IA. Como resultado, más empresas subcontratarán aspectos de sus necesidades de monitoreo de seguridad en tiempo real que no pueden contar con suficiente personal interno.

Conclusión

A medida que las amenazas cibernéticas se vuelven más numerosas y sofisticadas debido a la migración a la nube y el coronavirus, las empresas buscarán cada vez más el monitoreo en tiempo real para la protección cibernética. En términos más generales, la ciberseguridad desempeñará un papel cada vez más importante en la creación y protección de una ventaja competitiva. Las empresas que comprendan mejor y respondan a su panorama de amenazas cibernéticas en constante cambio se verán favorecidas por clientes, proveedores, empleados e inversores. Experimentarán menores costos de violación de datos y mayores retornos en sus esfuerzos de gestión de riesgos cibernéticos. La estrategia de ciberseguridad debe abarcar el monitoreo de terminales en tiempo real y el análisis de transmisión. Las empresas que se quedan atrás entregan una poderosa oportunidad competitiva. Los presupuestos de TI en 2022 no sólo deberían favorecer la computación en la nube. También deben financiar mejoras de monitoreo en tiempo real.

“Las empresas establecerán cada vez más acuerdos con proveedores y clientes para detectar y responder a las amenazas cibernéticas.”

Consejos y tácticas de NIST para lidiar con ransomware

Utilizado en ataques cibernéticos que pueden paralizar organizaciones, el ransomware es un software malicioso que cifra los datos de un sistema informático y exige un pago para restaurar el acceso.

Para ayudar a las organizaciones a protegerse contra los ataques de ransomware y recuperarse de ellos si ocurren, el Instituto Nacional de Estándares y Tecnología (NIST) ha publicado una infografía que ofrece una serie de consejos y tácticas simples.

Los consejos de NIST incluyen:

- Utilizar software antivirus en todo momento y asegurarse de que esté configurado para escanear automáticamente sus correos electrónicos y medios extraíbles (por ejemplo, unidades flash) en busca de ransomware y otro malware.
- Mantener todas las computadoras completamente parcheadas con actualizaciones de seguridad.
- Utilizar productos o servicios de seguridad que bloqueen el acceso a sitios de ransomware conocidos en Internet.
- Configurar sistemas operativos o usar software de terceros para permitir que sólo las aplicaciones autorizadas se ejecuten en las computadoras, evitando así que el ransomware funcione.
- Restringir o prohibir el uso de dispositivos de propiedad personal en las redes de la organización y para el trabajo a distancia o el acceso remoto, a menos que se esté tomando medidas adicionales para garantizar la seguridad.

NIST también aconseja a los usuarios que sigan estos consejos para sus computadoras de trabajo:

> “Incluso con medidas de protección implementadas, eventualmente un ataque de ransomware aún puede tener éxito.”

- Utilizar cuentas de usuario estándar en lugar de cuentas con privilegios administrativos siempre que sea viable.
- Evitar el uso de aplicaciones y sites personales, como correo electrónico, chat y redes sociales, en las computadoras del trabajo.
- Evitar abrir archivos, hacer clic en enlaces, etc. de fuentes desconocidas sin antes verificarlos en busca de contenido sospechoso. Por ejemplo, puede ejecutarse un análisis antivirus en un archivo e inspeccionar los enlaces con atención.

Desafortunadamente, incluso con medidas de protección implementadas, eventualmente un ataque de ransomware aún puede tener éxito. Las organi-

zaciones pueden prepararse para esto tomando medidas para garantizar que su información no se corrompa o se pierda, y que las operaciones normales se puedan reanudar rápidamente.

NIST recomienda que las organizaciones sigan estos pasos para acelerar su recuperación: Desarrollar e implementar un plan de recuperación de incidentes con roles y estrategias definidos para la toma de decisiones.

Planificar, implementar y probar cuidadosamente una estrategia de copia de seguridad y restauración de datos. Es importante no sólo tener copias de seguridad seguras de todos sus datos importantes, sino también asegurarse de que las copias de seguridad se mantengan aisladas para que el ransomware no pueda propagarse fácilmente a ellos.

Mantener una nómina actualizada de contactos internos y externos para ataques de ransomware, incluida la aplicación de la ley.

El NIST también ha publicado un informe más detallado sobre cómo mantenerse preparado contra los ataques de ransomware en https://csrc.nist.gov/CSRC/media/Projects/ransomware-protection-and-response/documents/NIST_Tips_for_Preparing_for_Ransomware_Attacks.pdf.

> “Incluso con medidas de protección implementadas, eventualmente un ataque de ransomware aún puede tener éxito.”

¿Qué es el Seguro de Cibernética?

El seguro de cibernética (también llamado "seguro de responsabilidad civil cibernética") es una forma de cobertura diseñada para proteger la empresa de las amenazas en la era digital, como violaciones de datos o ataques cibernéticos malintecionados en sistemas informáticos del trabajo.

Una empresa es responsable de su propia seguridad cibernética, pero en caso de un ataque cibernético, tener el seguro adecuado significará que no está solo. La cobertura de responsabilidad cibernética brindará un apoyo crucial para ayudar a que su negocio se mantenga a flote.

¿Qué cubre el ciberseguro?

En caso de un ataque cibernético, la mayoría de las pólizas de seguro cibernético cubrirán los costos financieros y de reputación propios y de terceros, en el caso de que los datos o los sistemas electrónicos se han perdido, dañado, robado o corrompido.

Para la empresa involucrada, la primera parte, la cobertura incluye el costo de investigar un delito cibernético, recuperar los datos perdidos en una violación de seguridad y la restauración de los sistemas informáticos, la pérdida de ingresos sufrida por el cierre de una empresa, la gestión de la reputación, los pagos de extorsión exigidos por los piratas informáticos, gastos de notificación, etc., en el caso de que esté obligado a notificar a los terceros afectados.

Las coberturas de terceros (que resultan de reclamos en su contra) incluyen daños y acuerdos, y el costo de defenderse legalmente contra reclamos por incumplimiento del RGPD.

¿Quién necesita un seguro cibernético?

Si la empresa usa, envía o almacena datos electrónicos, puede beneficiarse de un seguro cibernético. Esos datos, ya sea que pertenezcan a la empresa o sean información confidencial del cliente, son vulnerables a ataques cibernéticos y filtraciones de datos; el seguro cibernético puede ayudar con el costo de la recuperación.

> "Una empresa es responsable de su propia seguridad cibernética, pero en caso de un ataque cibernético, tener el seguro adecuado significará que no está solo."

Es por eso que el seguro cibernético es una parte importante del seguro para pequeñas empresas, ya que ofrece apoyo financiero si sucede lo peor.

El costo del seguro cibernético depende de varios factores, incluidos los ingresos anuales de la empresa, la industria en la que funciona, el tipo de datos almacenados y el nivel de seguridad de la red. Ciertos sectores son más vulnerables al ciberdelito y, por lo tanto, requerirán un mayor nivel de cobertura.

La mejor manera de averiguar cuánto costaría cubrir su negocio es ejecutar una cotización de seguro cibernético y de datos en línea.

¿Cuáles son los delitos cibernéticos más comunes?

Desafortunadamente, incluso algunas de las personas más expertas en tecnología pueden ser víctimas del ciberdelito. Si bien existen numerosos tipos de actividades delictivas que ocurren en línea, hay algunos delitos cibernéticos comunes que debe tener en cuenta:

Malware. Una forma de software malicioso que puede instalarse en sus sistemas a través de estafas de phishing y explotando vulnerabilidades de software. Una vez instalado, el atacante puede espiar las actividades en línea y robar datos privados.

Ransomware. Esta es una forma de malware que ataca su sistema informático y cifra los datos. El atacante luego exigirá el pago de un rescate a cambio de la devolución de los datos. Vale la pena formular un plan de recuperación de datos como medida de precaución y mantener al menos una copia de seguridad de sus datos.

Hacking. El hacking es un término utilizado para la adquisición parcial o completa de un sistema informático o ciertas funciones dentro de él. Hay varios métodos para hacerlo, pero el objetivo generalmente es acceder a datos importantes.

Desarrollar software de manera segura

El ciclo de vida de desarrollo de software seguro (SSDLC) generalmente se refiere a un proceso sistemático de varios pasos que agiliza el desarrollo de software desde el inicio hasta el lanzamiento.

Es un modelo de procedimiento paso a paso fácil de seguir que permite a las organizaciones:

- Desarrollar software a tiempo
- Reforzar el cronograma de planificación inicial del producto
- Diseñar, y eventualmente desplegar

En esta nota tendremos una descripción completa del ciclo de vida del desarrollo de software seguro. Comprenderemos sus implicaciones mutuas en el desarrollo tecnológico-empresarial.

La idea es tener presente sta información para implementar las mejores prácticas y establecer una columna vertebral de desarrollo de software que conducirá a mejores resultados de productos.

El ciclo de vida de desarrollo de software seguro (SSDLC)

Establecido a fines de la década de 1960, el ciclo de vida de desarrollo de software seguro (SDLC) se ha implantado en casi todas las compañías de software modernas. El ciclo de vida de desarrollo de software seguro es un procedimiento paso a paso para desarrollar software con varios objetivos, que incluyen:

- Agilizar de forma escalable la cadena de productos/software
- Optimizar el diseño, despliegue y mantenimiento de dicho software.

Con el crecimiento multifacético de las demandas modernas de desarrollo, es crucial contar con una metodología todo en uno que agilice y estructure las fases del proyecto.

“Con el crecimiento multifacético de las demandas modernas de desarrollo, es crucial contar con una metodología todo en uno que agilice y estructure las fases del proyecto.”

Imagínese que es un director de proyecto que se acerca sin pensar a un equipo de desarrollo de software con una vaga visión de los resultados y el proyecto final. Suena aterrador ¿verdad?

Independientemente de las capacidades técnicas y los talentos del equipo, SDLC es esencial para regular cada fase del ciclo de desarrollo.

Quizás la ventaja más pragmática del SDLC es que proporciona control del pipeline de desarrollo al mismo tiempo que garantiza que el sistema de software cumpla con todos los requisitos estimados en todas y cada una de las fases.

Aunque el SDLC puede parecer una salsa mágica para el cronograma de gestión de proyectos de una organización, no funciona bien cuando hay incertidumbre sobre las expectativas y la visión del proyecto de software.

Más importante aún, SDLC no permite que los miembros del equipo agreguen aportes creativos, ya que todo el ciclo de vida se basa en la fase de planificación.

Debido a la estructura regulatoria y bastante rígida del SDLC, muchas empresas optan por un enfoque de desarrollo de software ágil con cumplimientos y fases incrementales hacia la implementación del producto final.

Sin embargo, el enfoque de SDLC es quizás una de las metodologías más seguras, ya que garantiza que cada requisito del proyecto se cumpla estrictamente sin problemas ni inconsistencias durante cada paso, desde la planificación hasta la implementación del producto.

Los 6 pasos de un ciclo de vida de desarrollo de software seguro

Con asegurarse de que la organización cumpla con el ciclo de vida de desarrollo de software seguro, establecerá un modelo sostenible para la planificación/inicio y lanzamiento final del producto.

El ciclo de vida del desarrollo de software seguro es progresivo y estructurado sistemáticamente, simplificado con 6 pasos:

1. Planificación y análisis de requisitos

La planificación preliminar y el análisis de requisitos es la etapa más fundamental del ciclo de vida del desarrollo de software seguro.

El análisis de los requisitos suele ser realizado por los miembros más veteranos del equipo, junto con los correspondientes comentarios

de los clientes y la cooperación con el departamento de ventas, las encuestas de marketing realizadas y los expertos en el sector.

Una vez que se ha reunido el marketing, los comentarios de los clientes y los requisitos del producto, la información se utiliza para planificar un enfoque básico del proyecto y realizar un estudio de viabilidad preliminar.

Un estudio de factibilidad estima la viabilidad del proyecto a corto y largo plazo desde un punto de vista económico, operativo y técnico.

Además, los gestores de proyectos pueden estimar, planificar y crear requisitos de garantía de calidad durante esta fase.

Al final de la planificación y el análisis de requisitos, el equipo debe tener un resultado de su estudio de viabilidad técnica con el que trabajar.
A partir de ahí, pueden definir una serie de enfoques técnicos para poner en marcha el proyecto sin problemas, con riesgos mínimos y optimizados.

Una vez que los miembros senior han realizado un análisis de requisitos y viabilidad de referencia, deben definir y documentar claramente los requerimientos específicos del producto y abordarlos con los analistas del cliente/mercado.

Este proceso de aprobación puede ejecutarse, en última instancia, a través de un documento de especificación de requisitos de software (SRS), un delineado exhaustivo de los requisitos del producto que se diseñará y desarrollará a lo largo del ciclo de vida del proyecto.

> “La planificación preliminar y el análisis de requisitos es la etapa más fundamental del ciclo de vida del desarrollo de software seguro.”

2. Arquitectura y diseño del producto

Utilizando un SRS como plantilla base para la arquitectura del producto, los arquitectos pueden ofrecer de forma eficaz un diseño de producto backend de acuerdo con la viabilidad y los requisitos preliminares.

Basándose en los requisitos expuestos en el SRS, normalmente se propone más de un enfoque de diseño y se documenta en la especificación del documento de diseño (DDS).
Finalmente, el DDS es revisado por todos los principales interesados en el proyecto y, basándose en parámetros críticos como la evaluación de riesgos, la solidez del producto, las limitaciones de presupuesto y tiempo y la modularidad del diseño, se selecciona el enfoque arquitectónico más viable.

El enfoque de diseño en un ciclo de vida de desarrollo de software seguro es exhaustivo. Define claramente todos los módulos arquitectónicos del producto junto con su comunicación con módulos externos y de ter-

ceros fuera de la arquitectura interna mediante ilustraciones de flujo de datos.

3. Planificación de las pruebas

En un ciclo de vida de desarrollo de software seguro, un plan de pruebas esboza:

- La estrategia utilizada para probar una aplicación
- Los recursos que se utilizarán
- El entorno de las pruebas
- Las posibles limitaciones de las pruebas, y
- El calendario previsto de las actividades de prueba.

El jefe del equipo de control de calidad suele encargarse de la planificación de las pruebas y de la asignación/garantía de recursos durante esta fase.

Un plan de pruebas suele incluir lo siguiente:

- Una introducción o un breve resumen del documento del plan de pruebas
- Expectativas sobre las limitaciones empresariales y técnicas al probar el software
- Una lista exhaustiva de los casos de prueba que se incluirán en las pruebas de la aplicación
- Características probadas
- Enfoque que se utilizará durante las pruebas del software
- Productos que se deben cumplir y probar
- Recursos asignados para las pruebas de la aplicación
- Posibles riesgos generales durante el proceso de prueba
- Calendario de tareas e hitos que deben alcanzarse en el plazo de las pruebas

4. Codificación

Ahora es el momento de construir y desarrollar el producto.

En esta etapa del ciclo de vida, el desarrollo del código se ejecuta de acuerdo con el DDS. Siempre que el diseño/arquitectura se haya realizado de forma detallada y organizada, la generación del código puede llevarse a cabo sin muchos obstáculos logísticos.

Es imprescindible que los

desarrolladores sigan las directrices de codificación definidas por su organización y las herramientas específicas del programa, incluidos los compiladores, intérpretes y depuradores que se utilizan para agilizar el proceso de generación de código.

Para el desarrollo de aplicaciones se suelen utilizar varios lenguajes de programación de alto nivel, como C, C++, Pascal, PHP y Java. En cualquier caso, el lenguaje de programación elegido depende totalmente del tipo de software, de sus casos de uso en la industria y de las especificaciones técnicas del proyecto.

5. Pruebas y resultados del producto

Después de varias rondas de revisión del código y de garantía de calidad, se puede implementar la prueba del producto en el ciclo de vida del desarrollo de software seguro. Es importante señalar que esta etapa suele ser un subconjunto de todas las etapas en los modelos de SDLC modernizados.

En otras palabras, las pruebas deben agilizarse activamente en tiempo real a través de cada etapa del SDLC para garantizar un proceso de desarrollo sostenible. Sin embargo, esta quinta etapa sólo es una etapa de prueba del producto en la que los defectos críticos son efectivamente reportados, rastreados/localizados, corregidos y vueltos a probar para el despliegue final y la redistribución.

Este proceso de remoción y reproducción se repite hasta que se satisfagan los estándares de calidad definidos en el SRS.

6. Liberación en el mercado y mantenimiento

Una vez que el producto de su organización ha sido sometido a la garantía de calidad y a las pruebas, el producto está listo para ser lanzado formalmente en el mercado apropiado.

Dependiendo de la estrategia de su organización en el mercado, el producto puede ser lanzado primero en un segmento limitado del mercado primario antes de ser probado en un entorno empresarial real. De lo contrario, muchas empresas y startups lanzan su producto provisoriamente y revisan los comentarios de los clientes para optimizar continuamente las características del producto y la usabilidad del software.

¿Cómo hacer que un SDLC sea seguro?

Añadiendo medidas de seguridad adicionales a las bases existentes de su proceso de desarrollo de SDLC.

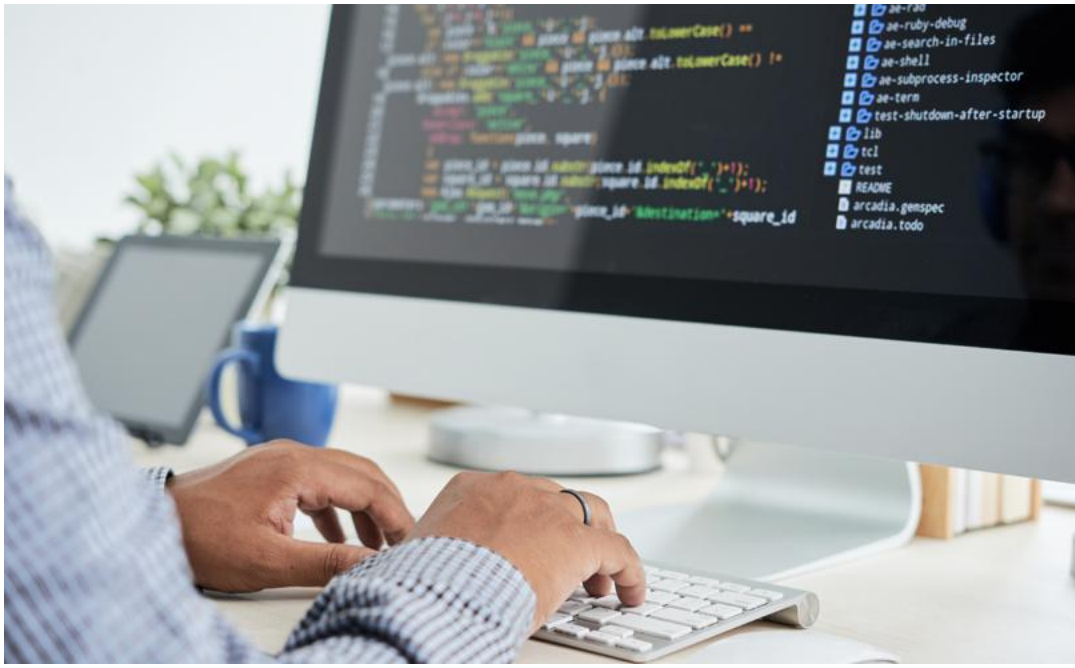
Por ejemplo, un líder tecnológico podría escribir, redactar y aplicar los requisitos de seguridad junto con la recopilación de requisitos funcionales en el SDLC. Y durante la fase de arquitectura y diseño, se puede realizar un análisis de riesgos para detectar vulnerabilidades específicas.

Se han propuesto diversos modelos de ciclo de vida de desarrollo de software seguro que se aplican eficazmente en los marcos de desarrollo modernos.
He aquí algunos de ellos:

- NIST 800-64: Desarrollado por los Institutos Nacionales de Estándares y Tecnología, las directrices proporcionan consideraciones y parámetros de seguridad dentro del SDLC que deben observar las agencias federales de Estados Unidos.

- MS Security Development Lifecycle (MS SDL): Propuesto por Microsoft en asociación con las fases de un SDLC clásico, el MS SDL es uno de los primeros de su clase y proporciona consideraciones de seguridad fiables que funcionan para la mayoría de los conductos de desarrollo modernos.

- OWASP CLASP (Comprehensive, Lightweight Application Security Process): Basado en el MS SDL, OWASP es muy fácil de integrar en su plan de arquitectura de software existente. Asigna las actividades de seguridad a los roles en una organización.



Ante la creciente demanda de crear modelos de desarrollo más ágiles y sostenibles con arquitecturas seguras, es fundamental comprender los seis pasos del SDLC y sus factores de seguridad.
Un SDLC es metodológico y garantiza que usted, su organización y las partes interesadas planifiquen, creen y desplieguen un producto final de manera oportuna y programáticamente eficiente.

Sin embargo, la creación de un SDLC adecuado requiere los mejores desarrolladores que pueda tener en sus manos.

Por ello, necesita contratar a desarrolladores cualificados y de confianza que garanticen la calidad e integridad de sus proyectos.

> “Un SDLC es metodológico y garantiza que usted, su organización y las partes interesadas planifiquen, creen y desplieguen un producto final de manera oportuna y programáticamente eficiente.”

Resolver el reto de la interoperabilidad de la seguridad

La mayoría de los equipos de seguridad utilizan varias herramientas para gestionar la infraestructura de seguridad de su organización. Cada una se adquirió para resolver un problema específico y plantea un reto diferente. Casi el 50% de las herramientas de seguridad recién adquiridas requieren integraciones codificadas individualmente. ¿Qué tan malo es?

> “Las principales repercusiones que experimentan las empresas con múltiples soluciones puntuales son los costes excesivos y la menor eficacia de las respuestas a las amenazas.”

La mayoría de los grandes equipos de seguridad están representados a partes iguales por analistas e integradores. Se necesita mucho tiempo y esfuerzo para implementar una herramienta correctamente. Además de la instalación, las pruebas, la puesta a punto, los parches y la conformidad, la herramienta debe incorporarse a su entorno y a sus procesos. Lo ideal sería también formar a su equipo en el uso de la nueva herramienta. Estas actividades restan tiempo y atención a las tareas de seguridad y pueden reducir considerablemente la eficacia de su equipo.

Además, el creciente número de productos de seguridad o la proliferación de herramientas, aumenta la complejidad. Aunque la falta de gestión de las herramientas no se produce de la noche a la mañana, sucede poco a poco con cada adición de una nueva. La recopilación de información a través de múltiples herramientas y fuentes de datos dispares lleva tiempo, un bien preciado, especialmente en el SOC, donde los segundos importan.

En lugar de solucionar un problema, las empresas se encuentran de repente con complicaciones de orquestación añadidas. La proliferación de herramientas es una preocupación bien documentada. Analistas como Forrester y 451 Research han informado sobre la proliferación de herramientas de seguridad en los últimos años, señalando que hasta el 40% de las organizaciones admiten que sus equipos de desarrollo están tan abrumados por las alertas de seguridad que no pueden responder al menos al 25% de ellas. Las principales repercusiones que experimentan las empresas con múltiples soluciones puntuales son los costes excesivos y la menor eficacia de las respuestas a las amenazas.

Se trata de un problema doble. No sólo es exigente la integración de las herramientas, sino que la proliferación de éstas agrava el problema. La mayoría de las veces, los equipos de seguridad han funcionado como el pegamento humano para unir herramientas dispares. El ecosistema de seguridad actual necesita buscar mejores formas de trabajar juntos y dejar de trabajar en silos.

Comprendiendo la norma ISO 27018:2020

Por Leonardo Devia

ISO 27018 es el código de práctica para la protección de información de identificación personal (PII) en nubes públicas. Vamos a explorar lo que significa tanto para los proveedores como para los clientes.

> La norma ISO/IEC 27018 es el estándar internacional para proteger la información personal en el almacenamiento en la nube.

La norma ISO/IEC 27018 es el estándar internacional para proteger la información personal en el almacenamiento en la nube. El término para los datos personales que cubre es Información de Identificación Personal o PII. ISO 27018 es un código de práctica para proveedores de servicios de nube pública.

ISO 27018 hace dos cosas:

- Brinda más orientación de implementación útil (que se agrega a ISO 27002) para los controles publicados en ISO/IEC 27001
- Establece orientación adicional sobre los requisitos de protección de PII para la nube pública

Estos controles adicionales no están cubiertos en ISO 27002.

¿Cuáles son los objetivos de ISO 27018?

ISO 27018 brinda una guía genérica acordada sobre las categorías de seguridad de la información. El estándar se dirige a los proveedores de servicios de nube pública que actúan como procesadores de PII.

Sus objetivos son:

- Orientar al procesador de PII de la nube pública a cumplir con sus obligaciones, incluso cuando están bajo contrato para proporcionar servicios de nube pública
- Habilitar la transparencia, para que los posibles clientes de servicios en la nube puedan acceder a servicios de procesamiento de PII basados en la nube seguros y bien administrados
- Ofrecer a los usuarios y servicios en la nube a establecer acuerdos contractuales para el procesamiento de PII
- Brindar a los clientes de servicios en la nube una metodología de auditoría y cumplimiento

La importancia de asegurar la información de identificación personal

Según el Informe de violación de datos de 2020 de CSA (Cloud Security Alliance), el el

80% de todas las violaciones de datos involucran PII. Proteger la PII cubre una variedad de medidas, algunas de las cuales son muy familiares. Éstas incluyen:

- Minimizar la recopilación y retención de datos
- La adopción de un programa seguro de destrucción de datos
- Cifrado de datos para almacenamiento y transmisión
- Limitación del acceso a los datos
- Formación de los empleados
- Cumplimiento de las reglamentaciones pertinentes Implementación de una estrategia de gobierno de la información

Cómo se relaciona la ISO 27018 con otras normas

ISO 27018 es uno de los estándares de gestión de seguridad de la información de la familia ISO 27000. Los estándares ISO 27000 proporcionan un marco de seguridad de la información reconocido internacionalmente.

ISO 27001 establece los requisitos técnicos para establecer un SGSI. El cumplimiento de la norma ISO 27001 es el estándar básico para la seguridad de los datos. ISO 27018 agrega orientación sobre la protección de datos de servicios en la nube a ISO 27001.

En lugar de elegir entre ISO 27001 o la 27018, piensar en implementarlos juntos. ISO 27001 es el mejor marco para crear un SGSI que se centre en la gestión de riesgos. ISO 27018 agrega orientación para lograr una seguridad sólida en la nube.

ISO 27701 cubre la gestión de la información de privacidad, estableciendo requisitos y orientación para implementar un sistema de gestión de la información de privacidad (PIMS). El estándar también brinda orientación para los controladores y procesadores de PII, incluidos los consejos de implementación según:

- La ubicación
- Cualquier legislación o reglamento nacional

ISO 27701 se corresponde con ISO 27018 y la legislación GDPR de la UE. Es una extensión de ISO 27001, el estándar básico para la seguridad de los datos.

Si la organización trabaja en la Unión Europea, debe cumplir y, por lo tanto, debe conocer el RGPD (Reglamento General de Protección de Datos). Es una ley de la UE (y del Reino Unido, posterior al Brexit) que rige el procesamiento de datos personales. GDPR no sólo se aplica a los países de la UE. La ley también se aplica a cualquier organización que proporcione bienes o servicios a la UE.

GDPR e ISO 27018 cumplen funciones ligeramente diferentes. GDPR establece las normas de privacidad y protección de datos. ISO 27018 le brinda un marco práctico para administrar la protección de datos y los riesgos de seguridad de la información. La implementación de ISO 27001, junto con 27018, le brinda una base sólida para el cumplimiento de GDPR.

ISO 27018, además, vincula a ISO/IEC 29100, que proporciona:

- Principios de privacidad para el entorno de la nube pública
- Un marco general para proteger la PII dentro de un sistema de TIC

Por su parte, ISO 29100 vincula a ISO 27018 por:

- Guiar a definir los requisitos de privacidad de PII
- Explicar los diferentes roles en el procesamiento de PII

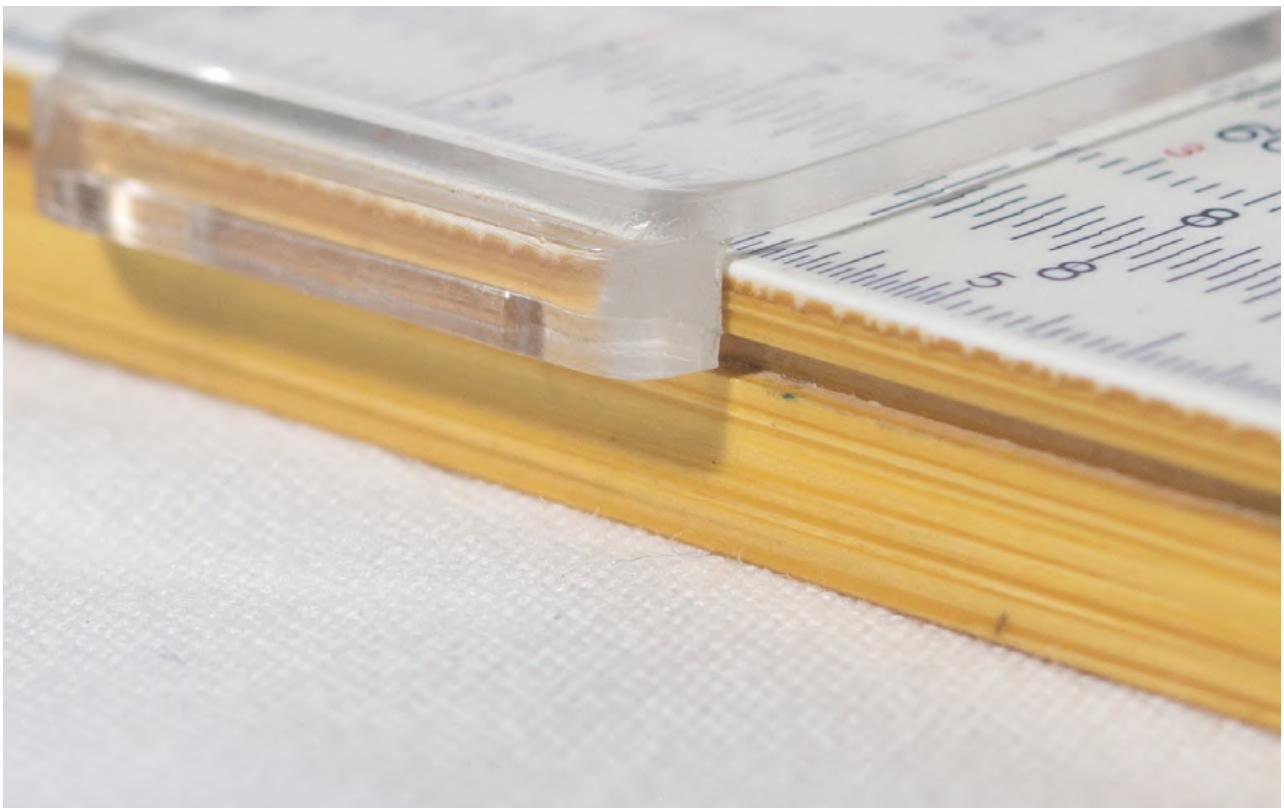
ISO 29100 también establece principios y terminología de privacidad clave. Beneficios de la ISO 27018

La ciberseguridad es un problema enorme para la confianza empresarial. En el mercado global actual, proteger los datos de los clientes nunca ha sido tan crítico. ISO 27018 crea un sólido marco de cumplimiento global.

ISO 27018 es especialmente útil para los clientes de servicios en la nube. Da soporte a la auditoría del cumplimiento de las responsabilidades internas. Esto es especialmente útil cuando el procesador de datos es un proveedor de nube de terceros.

Otros beneficios de ISO 27018 son que:

- Reduce los riesgos de violaciones de datos en la nube y multas regulatorias relacionadas
- Inspira confianza en la organización
- Los clientes y consumidores sabrán que estás protegiendo sus datos personales.
- Protege la reputación de la marca



Futuros usos de Blockchain para la ciberseguridad (segunda parte)

La tecnología Blockchain es un sistema de contabilidad distribuido y descentralizado que puede registrar transacciones entre múltiples computadoras. Blockchain comenzó como la tecnología detrás de bitcoin, pero popularmente se ha convertido en una tecnología de mitigación prometedora para la ciberseguridad.

“Blockchain se puede aplicar para verificar actividades, como actualizaciones de firmware, instaladores y parches, para evitar la entrada de software malicioso en las computadoras.”

En la primera parte de este artículo, en nuestro número anterior, vimos algunos casos de uso de Blockchain para la ciberseguridad: Protección de la mensajería privada, IoT Security y Protección de DNS y DDoS. En esta segunda parte veremos el resto.

Descentralización del medio de almacenamiento

La piratería y el robo de datos comerciales se están convirtiendo en la principal causa evidente de preocupación para las organizaciones. La mayoría de las empresas todavía utilizan la forma centralizada del medio de almacenamiento. Para acceder a todos los datos almacenados en estos sistemas, un hacker simplemente explota un solo punto vulnerable. Un ataque de este tipo deja datos sensibles y confidenciales, como registros financieros comerciales, en posesión de un delincuente.

Al usar blockchain, los datos confidenciales pueden protegerse asegurando una forma descentralizada de almacenamiento de datos. Este método de mitigación haría más difícil e incluso imposible para los piratas informáticos penetrar en los sistemas de almacenamiento de datos. Muchas empresas de servicios de almacenamiento están evaluando formas en que blockchain puede proteger los datos de los piratas informáticos.

La procedencia del software

Blockchain se puede utilizar para garantizar la integridad de las descargas de software para evitar intrusiones externas. Así como se utilizan los hashes MD5, blockchain se puede aplicar para verificar actividades, como actualizaciones de firmware, instaladores y parches, para evitar la entrada de software malicioso en las computadoras. En el escenario MD5, la nueva identidad del software se compara con los hashes disponibles en los sitios web de los proveedores. Este método no es completamente infalible, ya que es posible que los hashes disponibles en la plataforma del proveedor ya estén comprometidos.

Sin embargo, en el caso de la tecnología blockchain, los hashes se registran perma-

nentemente en la blockchain. La información registrada en la tecnología no es mutable ni cambiante; por lo tanto, blockchain puede ser más eficiente para verificar la integridad del software comparando los hashes con los registros de blockchain.

Verificación de infraestructuras ciberfísicas

La manipulación de datos, la mala configuración de los sistemas junto con la falla de los componentes ha estropeado la integridad de la información generada a partir de los sistemas ciberfísicos. Sin embargo, las capacidades de la tecnología blockchain en la integridad y verificación de la información pueden utilizarse para autenticar el estado de cualquier infraestructura ciberfísica. La información generada sobre los componentes de la infraestructura a través de blockchain puede ser más segura para la cadena de custodia completa. Protección de la transmisión de datos

Blockchain se puede utilizar en el futuro para evitar el acceso no autorizado a los datos mientras están en tránsito. Al utilizar la función de cifrado completa de la tecnología, la transmisión de datos se puede asegurar para evitar que los actores malintencionados accedan a ella, ya sea un individuo o una organización. Este enfoque conduciría a un aumento general de la confianza y la integridad de los datos transmitidos a través de blockchain. Los piratas informáticos con intenciones maliciosas aprovechan los datos en medio del tránsito para alterarlos o eliminar por completo su existencia. Esto deja una gran brecha en los canales de comunicación ineficientes, como los correos electrónicos.

Disminuir el contratiempo de la seguridad humana causada por ataques cibernéticos

Gracias a los innovadores avances tecnológicos, recientemente hemos visto el despliegue de equipos militares no tripulados y transporte público. Estos vehículos y armas automatizados son posibles gracias a Internet que facilita la transferencia de datos de los sensores a las bases de datos de control remoto. Sin embargo, los hackers han estado trabajando para romper y obtener acceso a redes, como Car Area Network (CAN). Cuando se aprovechan, estas redes ofrecen un acceso de control completo a funciones automotrices vitales para los piratas informáticos. Tales ocurrencias tendrían un impacto directo en la seguridad de los seres humanos. Pero a través de la verificación de datos realizada en blockchain para cualquier dato que entre y pase por dichos sistemas, se evitarían muchas adversidades.

Conclusión

No importa cómo se utilice, el componente clave de la tecnología blockchain es su capacidad de descentralización. Esta característica elimina el único punto de destino que puede verse comprometido. Como resultado, se vuelve completamente imposible infiltrarse en sistemas o sitios cuyo control de acceso, almacenamiento de datos y tráfico de red ya no están en una sola ubicación. Por lo tanto, blockchain puede ser una de las estrategias de mitigación más eficientes para las amenazas cibernéticas en los próximos días. Sin embargo, blockchain, al igual que con cualquier otra nueva tecnología, se enfrenta a muchos desafíos de inicio a medida que experimenta el doloroso proceso de crecimiento.

Principales riesgos de seguridad de IAM (Primera parte)

Mucho antes de que COVID-19 tomara al mundo por sorpresa, las empresas comprendieron las ventajas y las infinitas posibilidades de transferir datos y servicios a la nube. A medida que los empleados comenzaron a trabajar de forma remota, las demandas sin precedentes de la pandemia obligaron a las organizaciones a migrar sus datos a la nube, incluso más rápido de lo esperado.

Esta transición entre los tres modelos principales de implementación en la nube (SaaS, IaaS y PaaS) no sólo mejoró la flexibilidad y la eficiencia dentro de las organizaciones, sino que también presentó nuevos riesgos. A medida que las brechas de seguridad se vuelven una realidad aún mayor, es crucial que los protectores de la nube consideren la importancia de salvaguardar su información y fortalecer su Gestión de Identidad y Acceso (IAM por sus siglas en inglés), al tiempo que reconocen los principales riesgos de seguridad que han surgido a la superficie.

Permisos excesivos

Los permisos excesivos son políticas que se otorgan en exceso a los usuarios más allá de lo necesario. Controlar cada permiso de identidad (identidad humana y no humana) en la nube es extremadamente difícil debido a su naturaleza dinámica. Además, cada aplicación y sistema en la nube tiene su modelo de permisos único, lo que complica aún más la asignación y eliminación de permisos. Los permisos excesivos se pueden dividir en dos niveles: permisos excesivos utilizados y permisos excesivos no utilizados.

Ejemplos de permisos excesivos:

El acceso desde un departamento anterior persiste después de que un empleado se ha mudado a un nuevo departamento.

El privilegio de administrador temporal de un usuario nunca fue revocado.

> “Controlar cada permiso de identidad (identidad humana y no humana) en la nube es extremadamente difícil debido a su naturaleza dinámica.”

Cómo mitigar este riesgo:

Esta solución se basa en la noción de que, si bien no se necesitan todos los permisos otorgados, no todos los permisos que se usan con poca frecuencia deben eliminarse. Como resultado, las empresas deberían considerar el uso de una herramienta de análisis de derechos basada en inteligencia artificial que otorgue privilegios exactos de manera automática y consistente en función de lo que los usuarios realmente necesitan. Además, esta solución debe asegurar el ciclo de vida y la gobernanza de los activos de una empresa al asegurar los cambios en quién tiene acceso y garantizar que se gobierne adecuadamente.

Intercambio externo de datos
Controlar el acceso a los recursos compartidos es extremadamente difícil debido a la simplicidad del

intercambio de datos a través de los servicios en la nube. En consecuencia, las organizaciones desconocen los datos y recursos confidenciales que se comparten. Las aplicaciones de terceros como Google Drive, Dropbox, etc. facilitan el intercambio de datos que, en muchos casos, cuando se comparten fuera del entorno de TI de la empresa, la configuración de privacidad de los datos ya no está bajo el control de la empresa.

Ejemplos de permisos excesivos:

Un cliente todavía tiene acceso prolongado a un catálogo de productos de SharePoint, incluso dos años después de haber dejado la empresa (ejemplo de la vida real).

Los documentos confidenciales se guardan accidentalmente en la carpeta incorrecta.

Cómo mitigar este riesgo:

Las organizaciones deben buscar una solución que monitoree continuamente sus datos, identidades y permisos. Esta solución implica dar a las empresas una visibilidad profunda de lo que ha sido expuesto de forma intencionada o no intencionada. Además, las soluciones deben admitir sistemas de etiquetado internos o integrar sistemas de etiquetado

ya existentes como el sistema de etiquetado de Microsoft.

Además de ofrecer una visibilidad profunda, la mejor solución también debería alertar automáticamente a las empresas de cualquier comportamiento anormal fuera de su "perímetro de identidad". Al implementar estas soluciones, las organizaciones obtendrán una mejor comprensión de dónde se han compartido sus datos y, como resultado, podrán mitigar mejor los riesgos potenciales.

Configuraciones incorrectas

Las configuraciones incorrectas son el resultado de una supervisión o implementación insuficiente de los controles de seguridad en servidores o aplicaciones web. Debido al mal manejo o la falta de controles de seguridad, lo que se supone que es un entorno impenetrable, tiene agujeros peligrosos que ponen en peligro a las empresas. La mayoría de las configuraciones incorrectas son indetectables a simple vista y son más comunes de lo que muchos quisieran admitir. Las configuraciones incorrectas son más comunes que nunca en la era de la nube y son un problema frecuente que puede tener lugar en cualquier nivel de la pila de aplicaciones. A medida que la nube múltiple continúa complejizándose, los errores humanos aumentan y las configuraciones incorrectas se vuelven más frecuentes.

Ejemplos de permisos excesivos:

No habilitar el "paso a través de IAM" en Databricks puede generar permisos imprecisos, lo que garantiza un acceso excesivo al depósito. Cuando esto ocurre, el depósito queda expuesto más allá de los parámetros de la or-

ganización.

Configuración de Grupos de Google mal configurada

Cómo mitigar este riesgo:

Las empresas deben implementar una solución que sea capaz de detectar configuraciones erróneas tanto accidentales como maliciosas en la configuración de la nube desde cualquier punto de acceso, al mismo tiempo que admite un entorno de múltiples nubes. Esta solución no sólo debe poder detectar una configuración incorrecta, sino que también debe recomendar cómo solucionarla correctamente.

Falta de visibilidad

La nube es un entorno dinámico y complejo en el que operar. A medida que las aplicaciones y la infraestructura maduran y se vuelven sofisticadas, generan cantidades masivas de datos que se necesitan monitorear. Se vuelve aún más difícil lograr visibilidad cuando los proyectos se crean y completan en un breve período. La falta de herramientas proporcionadas por los proveedores de la nube para ver el nivel más bajo de datos, aplicaciones y activos de una empresa, hace que sea imposible para las empresas descifrar correctamente quién

> “Las configuraciones incorrectas son el resultado de una supervisión o implementación insuficiente de los controles de seguridad en servidores o aplicaciones web.”

tiene acceso a los activos entre diferentes nubes o si se expuso material sensible. Además, esta falta de visibilidad también impide que las empresas establezcan y mantengan la segmentación en las políticas consideradas las mejores prácticas por la mayoría de las metodologías de seguridad como Zero Trust, NIST y MITRE.

Ejemplos de permisos excesivos:

Las soluciones existentes no pueden mostrar cómo y dónde se otorga el acceso. Por ejemplo, el acceso a un determinado archivo se puede otorgar mediante asignación directa, pertenencia a un grupo o incluso, para empeorar las cosas, mediante una combinación de varias políticas. Obtener una vista centralizada de entornos de múltiples nubes como Azure, AWS y nubes privadas, es imposible con las herramientas de CSP.

Las herramientas existentes carecen de visibilidad de los activos de la joya de la corona, lo que impide que los equipos de TI establezcan microperímetros de confianza cero.

Cómo mitigar este riesgo:

Adoptar soluciones con una identidad gráfica y una vista de derechos es el camino a seguir. Este es un enfoque más óptimo para proporcionar una visión simplificada e intuitiva de la relación entre identidades y derechos (una imagen vale más que mil palabras). Dado que el acceso se puede otorgar tanto directa como indirectamente, las relaciones se caracterizan más fácilmente mediante modelos de gráficos. La capacidad de dividir y dividir datos libremente es esencial, ya que cada estructura y necesidades de la organización son únicas. Además, el mantenimiento continuo de un enfoque de microsegmentación de “confianza cero” se puede lograr mediante el uso de herramientas para obtener y aprovechar una visibilidad profunda.

En el próximo número, completamos esta nota.

emBlue

Hacemos que la **omnicanalidad sea simple**

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

NOTICIAS DEL SECTOR IT EN LATINOAMÉRICA

ITWARE
LATAM.COM

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

Manténgase informado suscribiendo a nuestros newsletter

@ITwareLatam
@ITwareLatam
ITware Latam
ITware Latam
ITware Latam

10 AÑOS