SecuriTIC
Latinoamérica

Información de Valor para Integradores de Seguridad Electrónica y Ciberseguridad

Mercado de ciberseguridad en crecimiento, A PESAR DEL DETERIORO DE LAS CONDICIONES ECONÓMICAS: Canalys

VIDEOVIGILANCIA
Hikvision lanza en México la serie eDVR evolutiva con tecnología eSSD

VIDEOVIGILANCIA
Las 6 tendencias tecnológicas que afectarán al sector de la seguridad en 2023

Febrero 2023 Año 10 Número 116 www.securitic.lat

ColorVu+X

HIKVISION®

Explore Nuevas Posibilidades Con la Tecnología ColorVu

Los modelos de Red y Turbo HD están disponibles

+X

Incluso más que ColorVu

Ver en Color, Incluso en la Oscuridad

@HikvisionMx
www.hikvision.com/es-la

Aprende más sobre Color Vu+X

Hikvision México
sales.mexico@hikvision.com

Índice

SecuriTIC Latinoamérica

Carlos Alberto Soto
carlos@securitic.com.mx
Director General
Editor

Gabriela Pérez
Atención
Corporativa

Alejandro Teodores
webmaster@securitic.com.mx
Diseño Gráfico
Webmaster

Alfredo Escobedo
Telemarketing

Karla Soto
Social Media

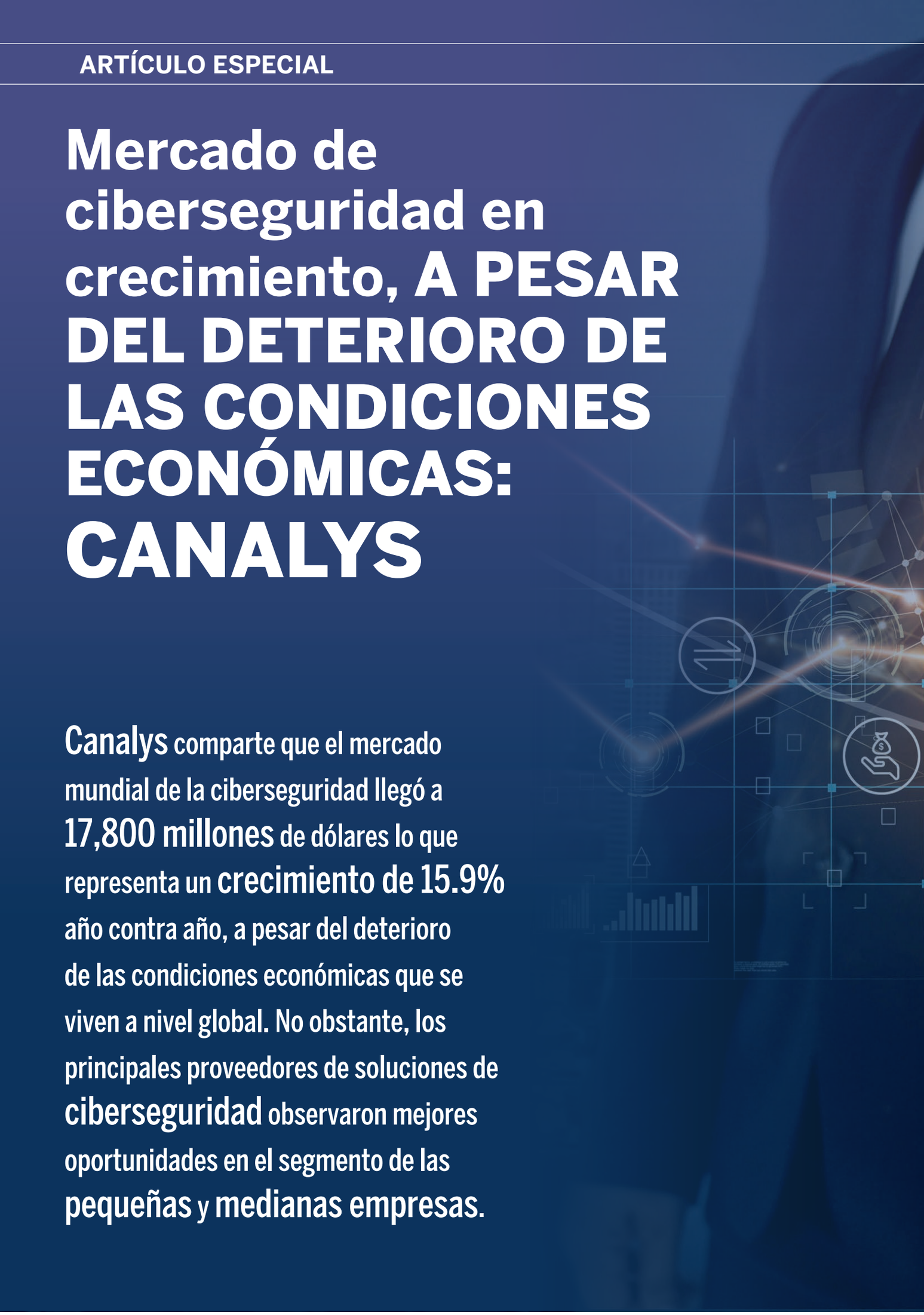
Contacto Editorial
y de ventas
carlos@securitic.com.mx

Contacto de Ventas
ventas@securitic.com.mx

www.securitic.lat facebook/SecuriTIC linkedin/securitic twitter/@SecuriTICMX
Visita nuestro aviso de privacidad en: www.securitic.lat

SecuriTIC, revista con periodicidad mensual. Febrero de 2023. Editor responsable: Carlos Alberto Soto Benítez. Número del Certificado de Reserva de Derechos al Uso Exclusivo del Título que expide el Instituto Nacional del Derecho de Autor: En Trámite. Número del Certificado de Licitud de Título y Contenido: En Trámite. Domicilio de la publicación: Valle de Ceylán 9-B, Col. El Olivo II, Tlalnepantla, Estado de México, C.P. 54110. Imprenta: Gráfica Romero con domicilio en Calle 3A Oriente, Mz. 7, L 4, colonia Isidro Fabela, Ciudad de México, C.P. 14030. Distribuidor: SEPOMEX. Registro Postal en Trámite.

Mercado de ciberseguridad en crecimiento, A PESAR DEL DETERIORO DE LAS CONDICIONES ECONÓMICAS: CANALYS



Canalys comparte que el mercado mundial de la ciberseguridad llegó a 17,800 millones de dólares lo que representa un crecimiento de 15.9% año contra año, a pesar del deterioro de las condiciones económicas que se viven a nivel global. No obstante, los principales proveedores de soluciones de ciberseguridad observaron mejores oportunidades en el segmento de las pequeñas y medianas empresas.

En el caso de los fabricantes con mayor crecimiento, Palo Alto Networks se colocó en la posición número 1 con un crecimiento interanual de 24.9% y una participación de mercado de 8.4% en el tercer cuarto de 2022; el segundo lugar lo ocupó Cisco con un porcentaje de 16.7 puntos de crecimiento y 6.9% de cuota de mercado; en tercer lugar, se ubicó Fortinet con niveles de crecimiento de 29.9% y una participación de mercado de 6.7%.

En crecimiento por categoría, el segmento de endpoints fue el de más rápido desarrollo con 18.7%, que implicó un monto alrededor de los 2,700 millones de dólares; en segundo lugar, se ubicaron las soluciones de seguridad de la red con 5,100 millones de dólares y un porcentaje de crecimiento de 14.8 puntos porcentuales.

De acuerdo con los especialistas de Canalys el sector de la tecnología enfrenta condiciones económicas en deterioro, una mayor incertidumbre y un mayor escrutinio del gasto en TI, factores que la mayoría de los proveedores consideraron en sus pronósticos. Las caídas en los nuevos negocios, las reducciones en los compromisos de gasto y los retrasos en las fechas de inicio de suscripción fueron peores de lo esperado, lo que se hará evidente en los resultados futuros.

VENTAS DE CANAL

Respecto a las ventas realizadas por canales, Canalys considera que representaron el 90.6% del mercado en general, lo que implica que el 9.4% restante se hizo de manera directa a clientes finales. En porcentaje de crecimiento se expone que las ventas por canal alcanzaron niveles de 15.9% comparado año contra año.

En este sentido los socios de canal se mantienen optimistas acerca de las oportunidades en ciberseguridad. El 27% espera que sus ingresos por ciberseguridad crezcan más del 20% en 2023; otro 27% tiene una expectativa de crecimiento del 11 al 20% para el próximo año; y solo el 10% de los socios esperan que las ventas de ciberseguridad disminuyeran. Esta información está basada de acuerdo con una encuesta de Canalys realizada a 393 encuestados, hecha entre el 21 de noviembre y el 9 de diciembre de 2022.

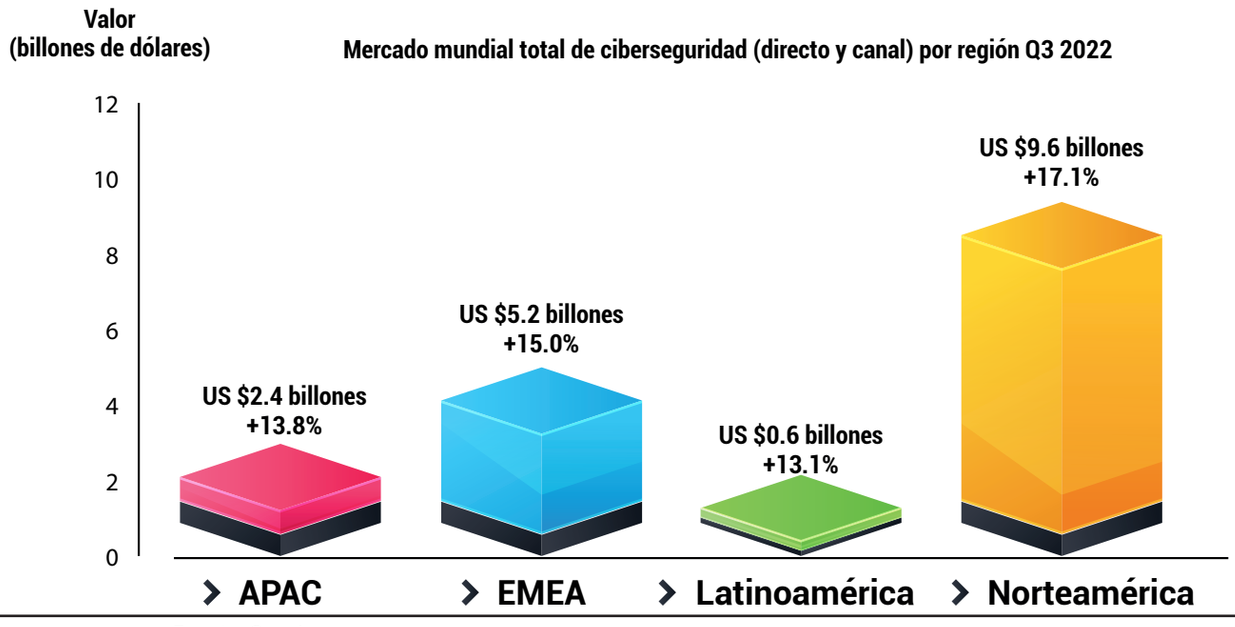
A nivel global el mercado de ciberseguridad más grande es el de América de Norte con ventas de 9,600 millones de dólares que representan el 53.8% del gasto global; seguidos de EMEA con 5,200, APAC con 2,400 y América Latina con 600 (millones de dólares).

Muchos proveedores de ciberseguridad se han desplazado hacia modelos comerciales basados en suscripciones, lo que también ayudó a protegerlos del impacto inmediato de la desaceleración económica", dijo Matthew Ball, analista jefe de Canalys. "El cambio a plataformas basadas en suscripción y un mayor enfoque en la venta de cuentas existentes sostendrán el crecimiento de los ingresos para los proveedores de ciberseguridad durante los próximos 12 meses".

MARKET SHARE A NIVEL GLOBAL EN CIBERSEGURIDAD

- Palo Alto Networks / 8.4%
- Cisco / 6.9%
- Fortinet / 6.7%
- Check Point / 3.8%
- CrowdStrike / 3.2%
- Okta / 3.1%
- Trellix / 3.1%
- Symantec / 2.9%
- Microsoft / 2.9%
- Trend Micro / 2.4%
- IBM / 2.3%
- Zscaler / 2.1%
- Otros / 52.2%

LA CIBERSEGURIDAD ES UNA PRIORIDAD EN TODAS LAS REGIONES



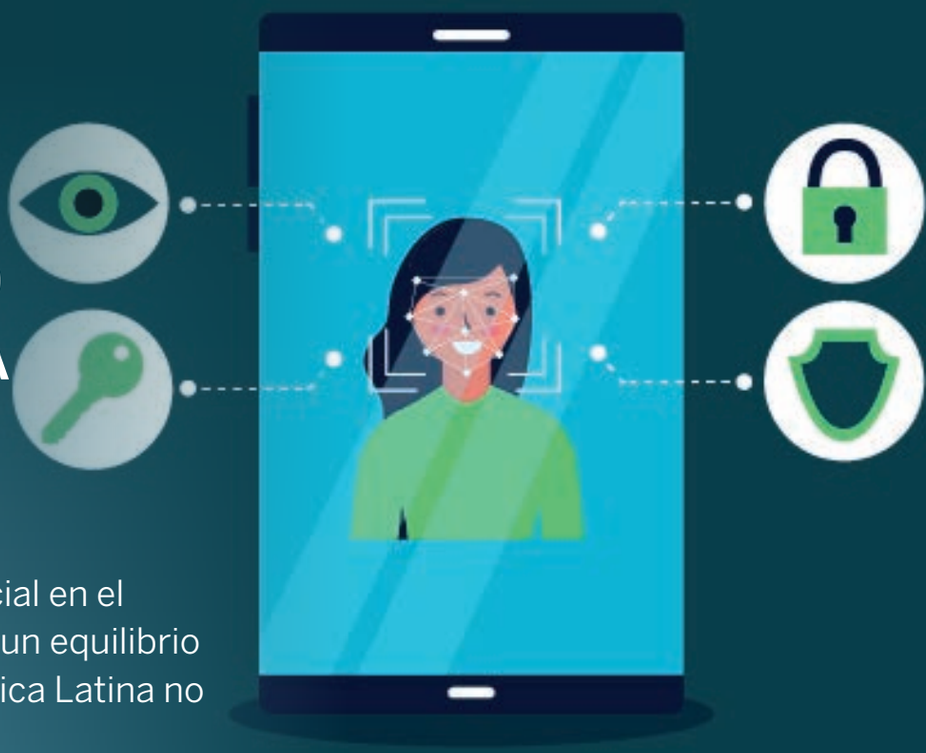
Fuente: Canalys.

OPINIÓN

Por Ignacio Gil-Barez, especialista en Autenticación de Consumidores en la unidad de Gestión de Acceso e Identidad de HID

CIBERSEGURIDAD Y LA EXPERIENCIA DE USUARIO SIN CONTRASEÑA

La ciberseguridad resulta esencial en el mundo digital y debe mantener un equilibrio con la facilidad de uso, en América Latina no es la excepción.



En la región, hoy en día tanto los empleados como los consumidores viven en entornos protegidos por las contraseñas, sin embargo, estas son un inconveniente y no siempre son seguras. ¿Cómo pueden las empresas aumentar sus esfuerzos en ciberseguridad, ofreciendo al mismo tiempo comodidad y garantizando la protección de los datos?

En el mundo de la gestión de acceso e identidad (IAM), la autenticación sin contraseña señala el camino a seguir.

LAS CONTRASEÑAS YA NO FUNCIONAN

Entre los profesionales de seguridad es sabido que las contraseñas no son la mejor manera de proteger los datos o activos, pero estos especialistas deben aceptar la difícil realidad que siguen siendo el método de autenticación más usado por muchos consumidores.

Las contraseñas generan fatiga, conformismo y pereza entre los compradores. Esto significa, entre otras cosas, que las contraseñas elegidas tienden a ser demasiado cortas y sencillas, lo que las hace fáciles de descifrar. Al menos 2/3 de los usuarios de smartphones (66 %) afirma que su contraseña más corta tiene 10 caracteres o menos, según lo indica el informe State of Consumer Authentication de Forrester del 1er. trimestre de 2022.

Asimismo, un estudio del Registro de Direcciones de Internet de América Latina y el Caribe, Lacnic, arrojó que los latinoamericanos usan contraseñas débiles para proteger el acceso de aplicaciones o identificarse como usuarios en sitios web.

Es así que cada vez son necesarias contraseñas más seguras y largas, que incluyan mayúsculas, números y caracteres especiales, lo cual ayuda. Pero esta complejidad adicional también significa que los consumidores escriben sus contraseñas en sitios donde se pueden ver. Además, las personas reutilizan claves en dispositivos y aplicaciones, lo que facilita a los hackers adivinar, espiar y obtener acceso a las cuentas del usuario.

Se habla mucho de la experiencia de usuario «sin fricción» y con razón. Los consumidores esperan una experiencia de la misma calidad en cada interacción digital, ya sea personal o laboral. Para casi todas las empresas, es importante que la experiencia de usuario sea lo más sencilla y fluida posible para que puedan realizar la acción o cumplir el objetivo que desean.

Por otra parte, los usuarios son cada vez más conscientes y están más interesados en alternativas de autenticación sin contraseña, como las que permiten los datos biométricos.

¿ES LA RESPUESTA UNA EXPERIENCIA SIN FRICCIÓN?

Según datos de Kaspersky, un cuarto de empresas latinas sufren ciberataques por contraseñas y políticas de seguridad débiles. Por esta razón las compañías deben optimizar y simplificar la experiencia de usuario mientras abordan la amenaza de que las contraseñas están desfasadas y ya no son seguras.

Esto es especialmente cierto en el caso de los servicios bancarios y financieros. En una encuesta conjunta de HID y FS Tech se puso de manifiesto que para los clientes bancarios, la seguridad supera a una experiencia sin fricción. Esto sugiere que, aunque la facilidad y la velocidad ocupan los primeros puestos en la lista de prioridades, los clientes se sienten cómodos con algo de fricción como parte del proceso de

inicio de sesión y autenticación, si esto contribuye a la seguridad de sus datos.

Las soluciones de autenticación sin contraseña transforman el panorama de la seguridad al ofrecer una mejor experiencia de usuario, ayudando al mismo tiempo a gestionar el riesgo con la cantidad adecuada de fricción.

EL PAPEL DE LA AUTENTICACIÓN MULTIFACTOR (MFA)

La autenticación multifactor (MFA) lidera el camino hacia una seguridad sólida a la vez que es fácil de usar mediante la combinación de tres factores: algo que sabe, algo que tiene y algo que es. Es importante tener en cuenta que los métodos de autenticación no seguros, como la contraseña de un solo uso (OTP, por sus siglas en inglés) que se envía por SMS (mensaje de texto) o correo electrónico, y el uso de preguntas y respuestas secretas, están aún muy extendidos.

El método de autenticación por notificación push es más seguro y fácil de usar, si al mismo tiempo se utiliza un dispositivo móvil como segundo factor de autenticación multifactor. Este emplea técnicas criptográficas para vincular un dispositivo específico a la identidad de su propietario, lo que hace imposible que los atacantes le suplanten sin disponer de acceso físico al dispositivo.

La experiencia de usuario del método de autenticación por notificación push es fluida y sencilla; los usuarios validan la solicitud haciendo una elección binaria: «aprobar» o «rechazar», en lugar de consultar y volver a escribir una OTP recibida por SMS. De hecho, las soluciones de autenticación por notificación push más flexibles, que aprovechan por igual tanto las empresas como las instituciones financieras, son las capacidades biométricas de los dispositivos móviles para no usar contraseñas.

Los usuarios son receptivos a esta experiencia, reconociendo que ofrecen un mayor nivel de seguridad y mejoran al mismo tiempo la comodidad del proceso general de autenticación. Los datos adicionales de la encuesta realizada por HID y FS Tech arrojaron que el 56 % de los usuarios demostraba una actitud positiva hacia las medidas de seguridad actuales para la prevención de fraudes, incluso cuando se requería fricción.

El 44 % restante tuvo una actitud neutral frente a esto. Las soluciones de autenticación multifactor también están en auge a medida que cada vez más empresas eligen tecnologías de autenticación avanzadas, incluidos tokens de hardware o software.

UNA MIRADA A LA VERIFICACIÓN DE IDENTIDAD (IDV)

Las empresas también estudian las soluciones de verificación de identidad (IDV), especialmente como un medio para garantizar una incorporación digital fluida para sus usuarios y para mejorar la experiencia sin contraseñas a lo largo de todo el recorrido. La IDV combina la correspondencia facial biométrica con comprobaciones cruzadas con documentos de identificación con fotografía expedidos por el gobierno, verificación de documentos en segundo plano, verificación de direcciones y otras validaciones automatizadas.

La IDV facilita un recorrido de usuario fluido, reduciendo notablemente las tasas de abandono de clientes en una etapa temprana, llevándolos a ejecutar el recorrido completo. Las mejores soluciones IDV de su clase ofrecen una arquitectura prediseñada y una entrega basada en la nube que facilita y agiliza la implementación.

EL FUTURO DE LA AUTENTICACIÓN SIN CONTRASEÑA: BIOMETRÍA CONDUCTUAL

Las empresas están sometidas a una intensa presión para adoptar soluciones de gestión de acceso e identidad fáciles de usar, pero seguras. Mientras tanto, los consumidores tienen dificultades para gestionar sus propias credenciales en una esfera cada vez más amplia de actividades digitales, por lo que elegirán empresas que puedan ofrecer tanto seguridad, como simplicidad. Con la estrategia y herramientas adecuadas, es posible respaldar identidades digitales seguras con menos fricción.

En adelante, el futuro de la autenticación sin contraseña también incluirá la biometría conductual. A diferencia de la biometría física, que reconoce características como una huella dactilar o una cara, la biometría conductual identifica a las personas basándose en la coincidencia única de patrones mensurables en las actividades humanas. Piense en el movimiento de la mano a la hora firmar o en las pulsaciones de las teclas de un teclado, en el patrón de voz o la manera de caminar.

Junto con la biometría física, la biometría conductual brinda la posibilidad de crear una experiencia de usuario más fluida que ofrece una verificación continua, abriendo el camino hacia un mundo digital más seguro y sin fraudes. [*]

Hikvision ahora utiliza energía eólica y solar para hacer funcionar sus cámaras en lugares remotos

En la actualidad, tener un suministro de energía que se alimente por medio de cables en sitios remotos e inaccesibles, tales como plantas de generación eléctrica, gasoductos, oleoductos, hasta instalaciones científicas remotas -como complejos de telescopios de alta potencia- resulta demasiado difícil y muy costoso.

Para proyectos en instalaciones remotas que necesitan sistemas inteligentes de seguridad y monitoreo, así como un suministro de energía que los alimente, la opción a implementar es una solución "off-the-grid" es decir, de generación independiente a cualquier red eléctrica, como generación de energía eólica y solar en sitio. Sin embargo, muchos sitios no pueden depender en su totalidad de la luz solar o únicamente del viento, que finalmente son fuentes de energía intermitentes.

De acuerdo con Rodolfo Alanis, Gerente Sr. de Desarrollo de Negocios para el sector energético en Hikvision México, elegir una única fuente de generación de energía no es lo suficientemente confiable para garantizar el suministro continuo y permanente de la misma, por lo cual se puede comprometer el funcionamiento continuo de cualquier solución de seguridad, monitoreo y operación que se haya implementado en el sitio.

"Sabemos que abastecer de energía a ubicaciones "off-the-grid" y aisladas es fundamental. Por ello contamos con Wind & Solar Supply, una solución híbrida de abastecimiento de energía eólica y solar que garantiza una generación de energía constante, incluso en los lugares más inaccesibles; nuestra solución también incluye un sistema de almacenamiento de energía con la opción de extender de 3 a 5 días el aseguramiento de la operación del sistema, independientemente del clima que se presente en sitio."

La solución Hikvision Wind & Solar Supply se ha implementado en muchas ubicaciones remotas y aisladas, proporcionando un suministro seguro y constante de energía para una amplia gama de aplicaciones; como lo es el monitoreo de carreteras, sistemas de seguridad agrícola, video vigilancia remota y monitoreo para plantas de generación fotovoltaica y parques eólicos, hasta el monitoreo de temperaturas en instalaciones de transporte de gas natural o petróleo como poliductos.

Con esta solución, disminuyen drásticamente los costos asociados con el cableado e instalación necesaria para un sistema dependiente o interconectado a cualquier red de energía eléctrica y además se recopilan datos en tiempo real sobre el estado de las instalaciones, así como su seguridad y operación; cruciales para una mejor toma de decisiones en cualquier momento.[*]

Genetec comparte algunos tips de mejores prácticas de seguridad electrónica

Genetec compartió las mejores prácticas de protección de datos para ayudar a los líderes de seguridad electrónica a proteger la privacidad, salvaguardar los datos y brindar confianza sin comprometer la seguridad.

La privacidad de los datos se ha convertido en una prioridad global. Actualmente, el 71% de los países han iniciado legislaciones sobre privacidad de datos, y las empresas que no han tomado las medidas adecuadas para proteger los datos se enfrentan a decenas de millones de dólares en multas por violaciones. En la industria de la seguridad electrónica, la adquisición de información digital, como imágenes de videovigilancia, fotos e información de matrículas, es necesaria para ayudar a proteger a las personas y los activos, y proporcionar una fuente valiosa de inteligencia de negocios accionable.

"La seguridad y la privacidad no son mutuamente excluyentes", afirmó Christian Morin, Director de Seguridad de Genetec Inc. "Al seguir las mejores prácticas y garantizar que la privacidad sea parte del diseño de sus soluciones de seguridad electrónica, las organizaciones pueden tener los más altos niveles de seguridad mientras respetan la privacidad personal y cumplen con las leyes de privacidad".

Las mejores prácticas para garantizar que los sistemas de videovigilancia, control de acceso y reconocimiento de placas vehiculares cumplan con los estándares de privacidad de datos incluyen:

Recopilar y almacenar solo los datos que tu organización realmente necesita. Reduce la exposición al riesgo en caso de una violación de datos con pasos simples. Considera ajustar el campo de visión de una cámara para que no grabe áreas que no requieran monitoreo. Establece protocolos para guardar o eliminar automáticamente los datos de seguridad electrónica en función de la relevancia. Controla cuidadosamente qué datos, cuánto y durante cuánto tiempo se pueden compartir con otras organizaciones.

Limitar el acceso a los datos confidenciales. Otorga acceso a los datos solo a aquellos que los necesiten para hacer su trabajo y supervisa esas actividades para garantizar que la información de identificación, como imágenes y eventos de acceso, se usen solo según lo previsto. Revisa los derechos de acceso regularmente para que los privilegios se alineen con los requisitos del usuario. El uso de un proveedor de identidades, como Microsoft Active Directory, también puede ayudar a eliminar el error humano mediante la automatización de los procesos de agregar o eliminar cuentas de usuario de seguridad, conceder derechos o eliminar usuarios que se han retirado de la organización.

Anonimizar la recopilación de datos automáticamente. Las nuevas tecnologías pueden restringir y proteger automáticamente el acceso a los datos personales. Considera implementar un enmascaramiento de privacidad, como KiwiVision™ Privacy Protector de

Christian Morin, Director de Seguridad de Genetec Inc.

Genetec que anonimiza automáticamente las imágenes de las personas, para que puedas continuar revisando las imágenes de vigilancia respetando la privacidad. Esta tecnología también ofrece una capa adicional de seguridad que garantiza que solo los usuarios autorizados puedan "desbloquear" y ver imágenes sin enmascaramiento mientras conservan un registro de auditoría.

Unificar las soluciones de seguridad. Cuando la videovigilancia, el control de acceso, la gestión de evidencias y otros sensores operan bajo una sola plataforma, es mucho más fácil acceder y gestionar todos tus datos y crear reportes para una variedad de sistemas y sensores desde una sola interfaz. Un sistema unificado simplifica el proceso de rastreo del estado del sistema y del dispositivo y agiliza las actualizaciones de software y firmware, que son la clave para mitigar la amenaza de violaciones de datos.

Trabajar con socios certificados. Asegúrate de que tus proveedores de sistemas estén debidamente certificados (normas ISO 27001, 27017, certificación de ciberseguridad UL 2900-2-3 nivel 3 y cumplimiento de SOC2) y que desarrollen toda su tecnología basada en principios de privacidad. Un sistema de seguridad electrónica ciberresiliente contribuirá a mantener privados los datos recopilados de los dispositivos y sensores IoT en toda la red de seguridad electrónica. [*]

Hanwha Techwin Latinoamérica muestra su visión acerca de las tendencias en videovigilancia 2023

El futuro de la videovigilancia apunta mucho más alto. Las innovaciones en Inteligencia Artificial, los servidores en la nube, el Internet de las cosas y las tecnologías convergentes marcan la pauta en un año donde las tendencias tienen un enfoque hacia la tecnología.

#1 CÓMO UTILIZAR LA INTELIGENCIA ARTIFICIAL DE MANERA EFECTIVA.

En el sector de la videovigilancia, la IA ha evolucionado hasta el punto de reducir la frecuencia de las falsas alarmas y permitir búsquedas forenses precisas centradas en los atributos de los objetos. Sin embargo, la IA basada en metadatos básicos se ha convertido en algo habitual y ya no resulta tan llamativa como lo era anteriormente. Ahora, los clientes prefieren información reprocesada y orientada desde la perspectiva del usuario: como estadísticas del tipo de vehículo por periodo o el sexo y la edad de un cliente, en lugar de datos más sencillos. Esto permite a los clientes encontrar perspectivas más interesantes y tomar decisiones empresariales gestionando directamente la información.

La información adquiere valor cuando los usuarios son capaces de utilizarla de forma eficiente.

Actualmente, el sector de la videovigilancia se centra en el desarrollo de soluciones para la gestión eficiente de enormes cantidades de metadatos recopilados por la IA. A partir de ahora, se incrementará un cuadro de mandos o un informe que pueda recopilar y reproducir metadatos de IA que faciliten la toma de decisión final de los usuarios.

#2 SOLUCIONES UNIFICADAS EN SERVIDORES LOCALES Y LA NUBE

A medida que se generalizan los servicios basados en la nube, aumenta el número de empresas que los ofrecen. Los usuarios pueden integrar fácilmente dispositivos y sistemas utilizando servicios en la nube sin necesidad de adquirir o instalar servidores adicionales.

Sin embargo, debido a las políticas de seguridad, el estado de la red o el presupuesto, muchas empresas prefieren mantener su infraestructura convencional in situ instalando servidores y software directamente. Por este motivo, cada vez es más común un sistema híbrido que combine las instalaciones locales y la nube. Por ejemplo, una empresa puede utilizar un método o una combinación de dos formas según los requisitos del entorno (un servidor para la gestión general y copia de seguridad basada en la nube para los datos críticos).

#3 NUEVAS POSIBILIDADES CON LA TECNOLOGÍA EDGE AI

La tecnología Edge AI, que se utilizaba simplemente para la detección y clasificación de objetos, se ha mejorado con la Unidad de Procesamiento Neuronal (*NPU por sus siglas en inglés). A medida que la NPU se hace más avanzada tecnológicamente, las

* NPU indica semiconductores de IA que pueden aprender de forma independiente y procesar vídeo, audio, texto o imágenes al mismo tiempo, imitando la red nerviosa de un ser humano.

funciones de Edge AI se amplían para incluir, por ejemplo, el análisis del comportamiento y la detección de comportamientos anómalos. Además, también es posible que los usuarios aprendan algoritmos de IA directamente según las necesidades de sus clientes.

#4 TECNOLOGÍAS CONVERGENTES PARA EL FUTURO

Las soluciones convencionales de seguridad física, como la videovigilancia, el control de accesos o las alarmas de intrusión, se están ampliando mediante la integración con el Internet de las cosas (IoT), la IA o la nube. Por ejemplo, los sensores habilitados para IoT que detectan humo, temperatura, humedad o movimiento se están convirtiendo en parte de una sofisticada solución de vigilancia total a través de la integración con un sistema de seguridad de IA. En concreto, este tipo de soluciones completas ofrecen información a los usuarios basada en el análisis de datos con el sistema en la nube.

#5 CONFIANZA CERO Y CIBERSEGURIDAD

La concienciación sobre la información personal y los riesgos de ciberseguridad aumenta a medida que se extienden nuevos modelos de negocio y soluciones a través de integraciones tecnológicas con IA, la nube y el IoT. Recientemente, la "Confianza Cero" está creciendo como tendencia en la industria de la ciberseguridad. La "confianza cero" exige que todos y cada uno de los dispositivos y aplicaciones de una red se sometan a un proceso de cualificación, partiendo de la base de que no existe seguridad inherente en dichos dispositivos y aplicaciones, y de que una empresa debería tener "confianza cero" en ellos. [*]

LAS 6 TENDENCIAS TECNOLÓGICAS QUE AFECTARÁN AL SECTOR DE LA SEGURIDAD EN 2023

Que la tecnología se ha convertido en algo omnipresente en nuestra vida personal y laboral no es ninguna novedad.

Esto se debe en gran medida a los beneficios que las nuevas tecnologías aportan a las empresas y los ciudadanos de todo el mundo en la prestación de servicios nuevos, más eficaces y cada vez más eficientes. Sin embargo, la profundidad de la integración de la tecnología en nuestras vidas, los avances en sus capacidades y la mayor conciencia de sus implicaciones en la sociedad son también mayores que nunca y siguen acelerándose.

Por ello, muchas de las grandes macrotendencias mundiales -que abarcan cuestiones geopolíticas, incertidumbre económica, preocupaciones medioambientales y derechos humanos- tienen implicaciones para todos los sectores tecnológicos, incluido el de la seguridad.

El nuestro es un sector que hace uso de una tecnología cada vez más inteligente, inherentemente implicado en la recopilación de datos sensibles, y tan afectado por las cuestiones geopolíticas que afectan al comercio internacional como cualquier otro. Sin embargo, seguimos convencidos de que nuestras innovaciones crearán un mundo más inteligente y seguro.

Estas son las seis tendencias tecnológicas clave que creemos que afectarán al sector de la seguridad en 2023:

1. HACIA UNA VISIÓN PRÁCTICA

En los últimos años, la creciente aplicación de la IA y el aprendizaje automático o deep learning ha hecho que se preste más atención a las oportunidades que ofrecen los análisis avanzados. En el futuro, el foco de atención se desplazará de los propios análisis a la información práctica que ofrecen en casos de uso específicos. No se trata tanto de decirle que algo va mal como de ayudarle a decidir qué medidas tomar.

Un factor clave a la hora de emplear la analítica para ofrecer información práctica es el enorme aumento de datos que generan las cámaras de vigilancia, junto con otros sensores integrados en una solución. Los datos (y metadatos) que se crean serían imposibles de interpretar por operadores humanos y actuar en consecuencia con la suficiente rapidez, incluso con enormes y costosos aumentos de recursos.

El uso de análisis puede impulsar acciones en tiempo real que favorezcan la seguridad y la eficacia operativa. Desde avisos para llamar a los servicios de emergencia en caso de incidentes hasta la redirección del tráfico en las ciudades para aliviar el tránsito, pasando por la redistribución del personal en puntos de venta concurridos o el ahorro de energía en los edificios mediante una iluminación y calefacción más eficientes, la analítica está recomendando, incitando e incluso empezando a tomar las medidas que apoyan a los operadores humanos.

Más allá de la información práctica "en vivo", la analítica puede ayudar en el análisis forense posterior al incidente. De nuevo, dada la enorme cantidad de datos que generan las cámaras de vigilancia, encontrar las vistas relevantes de una escena puede llevar mucho tiempo. Esto puede obstaculizar las investigaciones y reducir la probabilidad de encontrar a los sospechosos. La búsqueda asistida aborda este problema, ayudando a los operadores a encontrar rápidamente personas y objetos de interés entre horas de grabación.

Por último, las acciones propuestas promovidas por la analítica son cada vez más prospectivas. El tiempo de inactividad en las instalaciones industriales y fábricas puede ser costoso. Una combinación de sensores permite que la analítica inteligente proponga un mantenimiento preventivo antes de que se produzca un fallo.

2. ARQUITECTURAS HÍBRIDAS DEFINIDAS POR CASOS DE USO

Como hemos destacado en anteriores entradas sobre tendencias tecnológicas, ahora se acepta comúnmente que una arquitectura tecnológica híbrida es la más adecuada para los sistemas de seguridad, ya que combina servidores locales, computación basada en la nube y potentes dispositivos periféricos.

Sin embargo, no hay una arquitectura que se adapte a todos los escenarios. Pero aquí está la solución: primero evalúe lo que debe abordarse en su caso de uso específico y, a continuación, defina la solución híbrida que satisfaga sus necesidades. Hay que tener en cuenta una serie de factores.

Sin duda, las ventajas de la analítica avanzada integrada en las cámaras de vigilancia en el borde de la red son evidentes. El análisis de las imágenes de mayor calidad en el instante en que se capturan ofrece a las organizaciones la mejor oportunidad de reaccionar en tiempo real.

Del mismo modo, los datos generados por las cámaras de vigilancia son ahora útiles más allá de la visión en tiempo real. El análisis de las tendencias a lo largo del tiempo puede aportar información que conduzca a una mayor eficiencia operativa. Este análisis suele requerir la potencia de procesamiento de los servidores locales o de la nube.

Y, por supuesto, están los requisitos -a menudo definidos por la normativa- en torno a la privacidad y el almacenamiento de datos, que varían de un país a otro y de una región a otra. Estos requisitos pueden marcar la diferencia entre el almacenamiento in situ y el uso de la nube.

Lo esencial es no atarse a una única arquitectura. Mantente abierto, date la flexibilidad de crear la arquitectura híbrida que mejor se adapte a tus necesidades específicas.

3. LA APARICIÓN DE SUBTENDENCIAS DE CIBERSEGURIDAD

La importancia de la ciberseguridad también se pone de relieve a través de la exigencia de cumplir las normas. Por ejemplo, la propuesta de Ley de Ciberresiliencia de la Comisión Europea impondrá mayores exigencias a los productores de hardware y software de todos los sectores para garantizar la ciberseguridad de sus productos, a través de menos vulnerabilidades en el lanzamiento y una mejor gestión de la ciberseguridad a lo largo del ciclo de vida de los productos. El sector de la seguridad y la vigilancia estará, por supuesto, incluido.

La Ley demuestra tanto la importancia como la complejidad de la ciberseguridad. Ya no puede considerarse un solo tema, sino varios ámbitos interrelacionados. Algunos de ellos están bien establecidos, pero otros están surgiendo.

En el sector de la videovigilancia, las medidas de ciberseguridad que garanticen la autenticidad y seguridad de los datos a medida que se capturan y transfieren de la cámara a la nube y al servidor serán esenciales para mantener la confianza en su valor.

Veremos un enfoque más proactivo por parte de los proveedores de tecnología a la hora de identificar vulnerabilidades, con programas de "recompensas por fallos" que se convertirán en algo habitual para incentivar a las partes externas.

Y los clientes esperarán transparencia en relación con la ciberseguridad de las soluciones de seguridad, con una lista de materiales de software que se convertirá en estándar para evaluar la seguridad del software y la gestión de riesgos.

4. MÁS ALLÁ DE LA SEGURIDAD

Una de las tendencias más significativas para el sector de la seguridad, y con ella una oportunidad igualmente significativa, es el paso más allá de la seguridad.

Las cámaras de vigilancia se han convertido en

potentes sensores. La calidad de la información de video que captan, en todas las condiciones, ha aumentado año tras año durante décadas. Hoy en día, gracias a los análisis avanzados, también crean metadatos -información sobre los datos de video- que añaden otra capa de información y valor.

Esto, por supuesto, mejora y potencia su capacidad para respaldar casos de uso relacionados con la seguridad y la eficiencia operativa, además de la seguridad. Ahora existe la oportunidad de combinar los datos creados por las cámaras de vigilancia con los de otros sensores (temperatura, ruido, calidad del aire y del agua, vibraciones, condiciones meteorológicas, etc.) para crear una red sensorial avanzada que permita tomar decisiones basadas en datos.

Ya estamos viendo algunos usos de estas redes en entornos industriales a través de la supervisión de procesos y el apoyo al mantenimiento proactivo. Pero los casos de uso en los que podrían aplicarse estas redes sólo están limitados por nuestra imaginación, pero sin duda pueden ayudar a mejorar casi todos los aspectos de nuestras vidas, incluida nuestra seguridad.

5. LA SOSTENIBILIDAD SIEMPRE, EL CAMBIO CLIMÁTICO EN PRIMER PLANO

La sostenibilidad ha figurado en varias de nuestras predicciones anuales sobre tendencias tecnológicas, y no vemos menos necesidad de mantener el impulso a las iniciativas de sostenibilidad en su sentido más amplio durante el próximo año. Garantizar que las organizaciones sigan midiendo y mejorando las prácticas medioambientales, sociales y de gobernanza empresarial de sus negocios será esencial para respetar a las personas, ser un socio comercial de confianza, innovar de forma responsable y proteger nuestro planeta. Todos estos aspectos serán objeto de un escrutinio cada vez mayor por parte de los clientes de soluciones de seguridad y protección.

Sin embargo, dadas las condiciones extremas del año pasado, esperamos que en 2023 se preste más atención específicamente a la lucha contra el cambio climático. Está claro que aún no estamos haciendo lo suficiente para detener la aceleración del calentamiento global, y se espera que todos los sectores redoblen sus esfuerzos.

Para Axis, un paso clave ha sido comprometerse con la Iniciativa de Objetivos Basados en la Ciencia (SBTi, por sus siglas en inglés), que nos permitirá establecer objetivos de reducción de emisiones, no sólo en nuestra propia empresa, sino en toda nuestra cadena de valor. Y este es un punto clave. Si bien las organizaciones pueden hacer grandes esfuerzos para reducir las emisiones de sus propias operaciones, estos pueden verse socavados si sus cadenas de valor ascendentes y descendentes no están alineadas con los mismos objetivos.

Para las empresas tecnológicas, sin embargo, el escrutinio de sus propias operaciones comerciales será sólo una cara de la moneda del cambio climático. También se espera que demuestren cómo sus productos y servicios apoyan los objetivos de sostenibilidad de sus propios clientes, creando eficiencias que también ayuden a esas organizaciones a reducir las emisiones.

6. UNA MAYOR ATENCIÓN REGULADORA

Inevitablemente, dada su omnipresencia y poder, el sector tecnológico en su conjunto y las tecnologías específicas están siendo objeto de un mayor escrutinio por parte de los reguladores y los responsables políticos. Seguimos creyendo que la atención debe centrarse siempre en la regulación de los casos de uso de la tecnología, no en la tecnología en sí, y siempre cumplirá la normativa local, regional e internacional. Pero puede ser un panorama complicado.

La Comisión Europea es una de las más activas a la hora de intentar regular la tecnología en un esfuerzo continuo por proteger la privacidad y los derechos de los ciudadanos. Su propuesta de Ley de IA, que forma parte de la Estrategia Europea de IA de la Comisión, pretende asignar categorías de riesgo específicas a los usos de la IA y sería el primer marco jurídico sobre IA. Al igual que la Directiva de la Comisión sobre responsabilidad de la IA, la Ley de IA será sin duda objeto de mucho debate antes de convertirse en ley.

Pero ya sea en relación con la IA, las demandas en torno a la ciberseguridad, la privacidad de los datos, el freno a la influencia de las "grandes tecnológicas" o el establecimiento de la soberanía tecnológica, está claro que las empresas tecnológicas del sector de la seguridad tendrán que adherirse cada vez más a normativas más estrictas. En términos generales, esto debe acogerse con satisfacción, ya que garantizar la transparencia empresarial y la práctica ética sigue siendo fundamental.

La mayor oportunidad para nuestro sector sigue estando en alinear el éxito comercial continuado con nuestra responsabilidad de abordar los problemas críticos a los que se enfrentan el planeta y nuestra población. Como siempre, somos optimistas en cuanto a que la combinación de nuestra inventiva humana, los avances tecnológicos y la práctica empresarial ética pueden combinarse para hacer del mundo un lugar mejor.

Johan Paulsson, Chief Technology Officer, Axis Communications. [*]

Hikvision lanza en México la serie eDVR evolutiva con tecnología eSSD

Como parte de sus avances tecnológicos de 2023, Hikvision agrega la serie eDVR a su cartera en expansión de soluciones de seguridad para pymes mexicanas y aplicaciones residenciales y comerciales.

Con tecnología de unidad de estado sólido integrada (eSSD), los usuarios se benefician de un proceso de instalación fácil y flexible, bajo consumo de energía, requisitos mínimos de mantenimiento y captura, almacenamiento y procesamiento de video de alto rendimiento.

"La serie eDVR ayuda a minimizar los impactos ambientales negativos, al brindar importantes ahorros de energía y costos. Las unidades de almacenamiento de los dispositivos también funcionan prácticamente sin ruido ni vibraciones y generan muy poco calor, lo que las hace ideales para aplicaciones residenciales. Estas ventajas, junto con la asequibilidad, la funcionalidad y la sostenibilidad de los eDVR, también hacen que la gama de productos sea una opción ideal para las Pymes, como tiendas de conveniencia, supermercados, restaurantes, talleres, bares, entre otros", menciona Miguel Arrañaga, Director Regional de Ventas de Hikvision México.

EFICIENCIA Y SOSTENIBILIDAD

1) Respeto al medio ambiente y ahorro de energía del 45%: El consumo de energía ultrabajo de los eSSD de nivel de chip hace que los eDVR de Hikvision sean más sustentables. Dado que estos dispositivos no tienen partes móviles incorporados, su consumo de energía es un 45% más bajo que el de los DVR convencionales, lo que no solo ayuda a los usuarios a ahorrar a largo plazo en sus facturas de electricidad, sino que también les permite reducir las emisiones de carbono.

2) Almacenamiento duradero con una mejora del 25 % en la eficiencia: La eficiencia de almacenamiento de la serie eDVR se mejora aún más con la "tecnología de control de tasa de bits adaptable a la escena", que optimiza automáticamente la codificación de secuencias de video y mejora la eficiencia de codificación en un 25 %. Específicamente, a las escenas complejas con movimientos humanos o de vehículos se les asignan tasas de bits más altas para garantizar una excelente calidad de video. Al mismo tiempo, a las escenas de baja complejidad con poco o ningún movimiento se les asigna una tasa de bits más baja para optimizar la eficiencia del almacenamiento.

3) Diseño compacto para facilidad de uso y simplicidad de instalación: Como los eDVR están integrados

con SSD y tienen un diseño "sin tornillos", es posible una instalación sin herramientas. Además, sin los requisitos de montaje horizontal tradicionales de los discos duros convencionales, los dispositivos también son más fáciles de montar y configurar.

4) detección de movimiento inteligente: Integrada con la tecnología de detección de movimiento 2.0, la serie eDVR puede distinguir seres humanos y vehículos de otros objetos en cualquier entorno dado, lo que permite a los propietarios responder mucho más rápida y eficazmente a posibles violaciones de seguridad. La tecnología también permite a los propietarios buscar secuencias de video en función de la apariencia de personas o vehículos durante un período de tiempo específico, ahorrando tiempo y reduciendo sus cargas de trabajo y costos. [*]

MÁS DE LA MITAD DE LOS MEXICANOS CONOCE LA CONTRASEÑA DE OTRA PERSONA EN INTERNET: AVAST

Avast da a conocer los resultados de una encuesta realizada entre 1,023 hombres y mujeres de México que comparten dispositivos, contraseñas, herramientas en línea, cuentas bancarias e incluso ubicaciones con sus parejas.

La investigación reveló que a menudo no se presta atención a estas cuestiones, tanto estando en una relación de pareja, como lo que es más preocupante, una vez que esta termina. Las principales conclusiones son las siguientes:

- Más de la mitad (59%) de los encuestados afirma conocer la o las contraseñas de otra persona en Internet, superando por 6 puntos a la media global del 53%. Además, el 64% de los que conocían la contraseña de otra persona, reconocieron conocer la de sus parejas actuales y 1 de cada 5 (21%), afirmaron conocer la de una expareja.
- Casi una tercera parte de los encuestados (30%) ha sido víctima de alguien que ha accedido a una cuenta y ha cambiado su(s) contraseña(s) sin su conocimiento o consentimiento.
- 1 de cada 5 encuestados (19%), dijo tener acceso a la ubicación de una expareja a través de aplicaciones como 'Find my friends', la función de compartir ubicación de Google o Snapchat.
- De quienes conocen la contraseña de su expareja sentimental, dos tercios (66%) de los mexicanos admitió que todavía tienen acceso a la cuenta de Facebook, rebasando la cifra global del 59%. Por su parte, la mitad (51%) admitió que todavía puede acceder a la cuenta de correo electrónico del trabajo de su ex.

De acuerdo con un artículo de Psychology Today, la tecnología desempeña un papel importante en la formación moderna de las parejas íntimas. Estas pueden provocar comportamientos de acoso y vigilancia por parte de parejas sentimentales abusivas, que van desde el uso de servicios de localización, así como el monitoreo de las redes sociales y el correo electrónico mediante el robo de contraseñas, programas espía o simplemente obligando a la pareja a "compartir" su cuenta contra su voluntad.

"Estas estadísticas son realmente preocupantes. Atrás quedaron los días en los que simplemente se devolvían los objetos personales y las llaves de la puerta del otro cuando se terminaba una relación. Aunque sabemos que la gente comparte contraseñas y dispositivos con su pareja, este comportamiento puede tener un lado muy oscuro, especialmente cuando las mujeres son obligadas a compartir sus contraseñas", concluyó Javier Rincón, Director Regional de Latinoamérica en Avast.

La encuesta fue realizada del 26 de agosto al 7 de septiembre de 2022 a una muestra de 1,023 mexicanos a través de la empresa de datos Dynata. [*]

AKAMAI COMPARTE SUS TENDENCIAS DE CIBERSEGURIDAD PARA 2023

El 2022 fue un año decisivo en las tendencias digitales, la ciberseguridad y las TI (Tecnologías de la Información) son temas que cada vez se abordan más en las empresas, y se han intensificado en los últimos años, a medida que el mundo comenzó a exigir mucho más a lo digital.

Mirando el escenario actual, algunas tendencias, como la adopción de Zero Trust, el aumento del tráfico de red, la falta de profesionales de TI, la necesidad de controlar la latencia de redes, el uso de la banca digital, y algunos ataques específicos se destacarán en 2023.

"Como cualquier proyección a futuro, estas tendencias pueden ser volátiles. La proyección del mercado se basa en muchos puntos y todo puede cambiar, así como las amenazas, que son cíclicas y evolucionan en sofisticación. Lo importante es que las empresas tengan una guía de lo que probablemente se avecine." señala Hugo Werner, vicepresidente regional de Akamai para LATAM.

Por ello, a continuación se presentan las principales tendencias del mercado de la ciberseguridad para el 2023. Con esto se podrá ayudar a las empresas a definir su estrategia de ciberseguridad, trabajando por etapas para implementarla.

ESCASEZ DE PROFESIONALES DE TI

Muchas empresas están priorizando la tecnología e invirtiendo más en equipos internos de TI. En agosto de este año, Indeed, sitio web de empleo, publicó datos que indican que en México, las vacantes relacionadas con criptografía y finanzas, ciberseguridad y desarrollo de software fueron las más difíciles de cubrir al momento de encontrar al candidato ideal, y esto se debe en parte a la falta de profesionales calificados en el área.

Con los ciberdelincuentes haciendo un uso sofisticado de las herramientas digitales, las vulnerabilidades y el crecimiento del universo digital visto en 2022 demostraron que el mercado carece de profesionales en el área, especialmente en ciberseguridad. Adoptar diferentes estrategias para atender esta necesidad, tales como promover procesos internos de capacitación o alianzas para formar talento externo y soporte calificado para sus demandas más críticas son algunas soluciones que las empresas pueden implementar.

LA ADOPCIÓN DE ZERO TRUST

La adopción de la postura Zero Trust es una necesidad para el futuro de la ciberseguridad y las empresas buscan su implementación. El entorno digital se vuelve cada vez más complejo y diverso, lo cual trae consigo un mayor riesgo. Por tanto, es interesante cambiar la postura ante este entorno: se puede adoptar un comportamiento de desconfianza y mayor seguridad. Siempre es necesario comprobar, validar e incluso revalidar el punto de control para permanecer seguro. Implementar mecanismos de monitoreo y seguimiento constante con evaluación del comportamiento del usuario en base al historial es de suma importancia para que, ante cualquier movimiento inusual, esté alerta y revalide el perfil.

EL AUMENTO DEL TRÁFICO DE RED

A medida que las empresas amplían su conectividad y se intensifica el comportamiento digital, los sistemas exigen respuestas cada vez más instantáneas y precisas, ya que el rendimiento dependerá de la capacidad de procesamiento de ciertas tecnologías para que todo suceda de la forma correcta. Debido

al aumento del tráfico de red, la capacidad de absorción y desempeño en entornos con un alto volumen de datos serán puntos clave para que las organizaciones garanticen la máxima seguridad y estabilidad posible.

Según un estudio de la firma global de consultoría e investigación de telecomunicaciones TeleGeography, el ancho de banda global de Internet aumentó un 28% a lo largo de 2022. Con el número de accesos y el volumen de tráfico creciendo, una red con poca capacidad será un impedimento para el avance de las funciones digitales de la empresa. La cantidad de datos que transportará una red y la seguridad que debe tener es lo que se debe tomar en cuenta a medida que el negocio evoluciona digitalmente.

LA NECESIDAD DE CONTROLAR LA LATENCIA

Con la notoriedad y adopción de Internet de las Cosas (IoT por sus siglas en inglés), el inicio de la integración 5G y la sofisticación en el uso de la Inteligencia Artificial, las posibilidades y entornos para ataques son muchos. Además, las nuevas generaciones de aplicaciones suelen ser muy sensibles a la latencia, y en este sentido es necesario contar con una infraestructura adecuada.

De acuerdo con un estudio sobre el rendimiento del comercio minorista en línea, solo un retraso de 100 milisegundos en el tiempo de carga perjudicó las tasas de conversión hasta en un 7 %, y un retraso de 2,7 segundos en el tiempo de carga generó una tasa de rebote de casi el 29 %. Un alto volumen de visitas o ciberataques puede afectar el rendimiento de las páginas. Cuando el consumidor tiene una mala experiencia, algunos clientes abandonan el sitio web y buscan otra marca, algunos nunca regresan a ese sitio que presentaba problemas, perdiendo al consumidor para siempre.

Otro buen ejemplo para entender el daño que puede causar la latencia es el área de la salud. Una cirugía realizada a distancia, en la cual el médico utilizara un robot como herramienta auxiliar, no puede tener latencia o errores de comunicación. La sensibilidad en estas posibilidades del futuro es muy importante y no puede fallar, cada segundo es importante. Por lo tanto, tratar y resolver los problemas de latencia será relevante para las empresas en 2023.

LA BANCA DIGITAL SEGUIRÁ GANANDO TERRENO ENTRE LOS USUARIOS MEXICANOS

Una encuesta realizada por Akamai por primera vez en México, para conocer las tendencias de la banca digital, reveló datos importantes.

"Con la digitalización de este mercado, podemos observar que la adherencia a los bancos digitales se ha popularizado entre los usuarios. La encuesta reveló que el 50% de los encuestados tiene tanto un banco tradicional como una cuenta bancaria digital. Aun así, el 39% de los usuarios solo utilizan bancos tradicionales, y esta cifra es aún mayor para el grupo de personas mayores de 50 años, siendo del 56%." señala Werner.

Por otro lado, de los usuarios que no tienen una cuenta digital, el 74% dijo estar dispuesto a abrir una cuenta en un banco digital, mientras que solo el 26% dijo no estar dispuesto a hacerlo. En este sentido, observamos el avance del uso de los bancos digitales en un futuro cercano. El consumidor mexicano busca principalmente el acceso al banco en cualquier momento (66%) y la facilidad de acceso (62%), lo que podría explicar la creciente demanda por el uso de bancos digitales durante los próximos años.

LAS PRINCIPALES AMENAZAS QUE IRÁN EN AUMENTO EN 2023

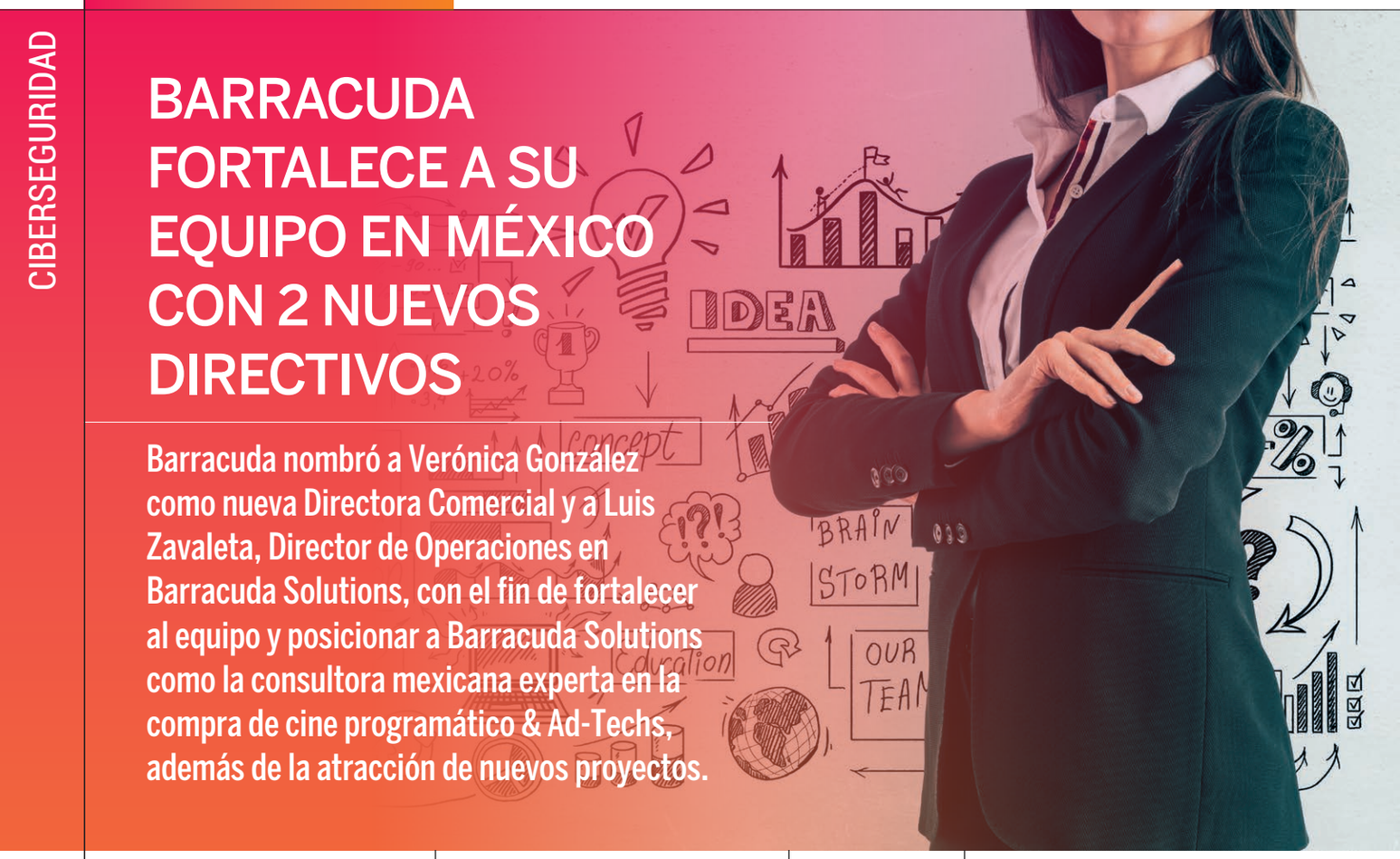
Ransomware: Es probable que los ataques de ransomware continúen aumentando en 2023, ya que brindan un retorno financiero significativo a los atacantes. El Informe global sobre amenazas de ransomware del primer trimestre de 2022 de Akamai reveló que el ransomware se ha vuelto omnipresente en los ataques de ciberseguridad a las organizaciones, lo que ha costado más de mil millones en daños a nivel mundial en 2021. En este tipo de ciberataques se utilizan técnicas para instalar malware dentro de los sistemas de una organización con el objetivo de comprometer, robar y encriptar archivos relevantes, bloqueando el acceso a los mismos. Para descifrar los datos y con la promesa de que no se divulgarán ni venderán, los delincuentes exigen un rescate, que es una gran cantidad de criptomonedas.

DDoS: Estos ataques también son una amenaza cibernética que probablemente aumentará el próximo año, especialmente dada la guerra entre Ucrania y Rusia. Este escenario de tensión geopolítica provoca un aumento de los ataques en Europa, ya que el convulso momento supone una brecha para los hackers empeñados en causar la mayor cantidad de problemas posible en varios países implicados en el conflicto. Al analizar datos del tercer trimestre de 2022, Akamai observó que la cantidad de ataques dirigidos a clientes europeos en Prolexic, la solución DDoS de la compañía, superó la cantidad de ataques en EE. UU. y la cantidad de ataques aumentó en un 1126 % en Europa occidental en comparación con el período previo a la guerra.

A través de estas tendencias, es posible observar que las empresas y los ecosistemas digitales evolucionan y es necesario contar con un socio de ciberseguridad que brinde las protecciones más adecuadas, analizando el entorno específico de cada cliente para atender efectivamente su demanda, protegiendo el sistema en su conjunto. [*]

BARRACUDA FORTALECE A SU EQUIPO EN MÉXICO CON 2 NUEVOS DIRECTIVOS

Barracuda nombró a Verónica González como nueva Directora Comercial y a Luis Zavaleta, Director de Operaciones en Barracuda Solutions, con el fin de fortalecer al equipo y posicionar a Barracuda Solutions como la consultora mexicana experta en la compra de cine programático & Ad-Techs, además de la atracción de nuevos proyectos.



"Hoy damos la bienvenida a Veronica y Luis para continuar innovando y tener la posibilidad de sumar valor en toda la industria. Además de permitir a los mexicanos encontrar en el cine no solo publicidad atractiva sino relevante para su día a día, es decir, lograr un ganar- ganar tanto para los consumidores como para las marcas, frente a un escenario publicitario cada vez más competitivo", dijo Ricardo Izquierdo, Managing Partner en Barracuda Solutions.

El impulso de la digitalización por la pandemia creó una gran oportunidad para Barracuda, ya que es la única consultora de Ad tech en México capaz de ayudar a los anunciantes a poner en marcha sus campañas en las pantallas de los cines y lograr impactar a más de 130 millones de asistentes a través de una tecnología llamada Lumiere de momento en todo el país pero en el último Q se planea la apertura de nuevos mercados.

Verónica cuenta con 12 años de experiencia en planeación de medios, publicidad OOH, branded content y venta de Tv Digital; es Licenciada en Ciencias de la Comunicación y Publicidad y cuenta una Maestría en "Publicidad corporativa, branded content y digital sales program" Por lo que será la encargada de dar solución, diseño, creación de estrategias digitales, atención y ese plus en el servicio al cliente.

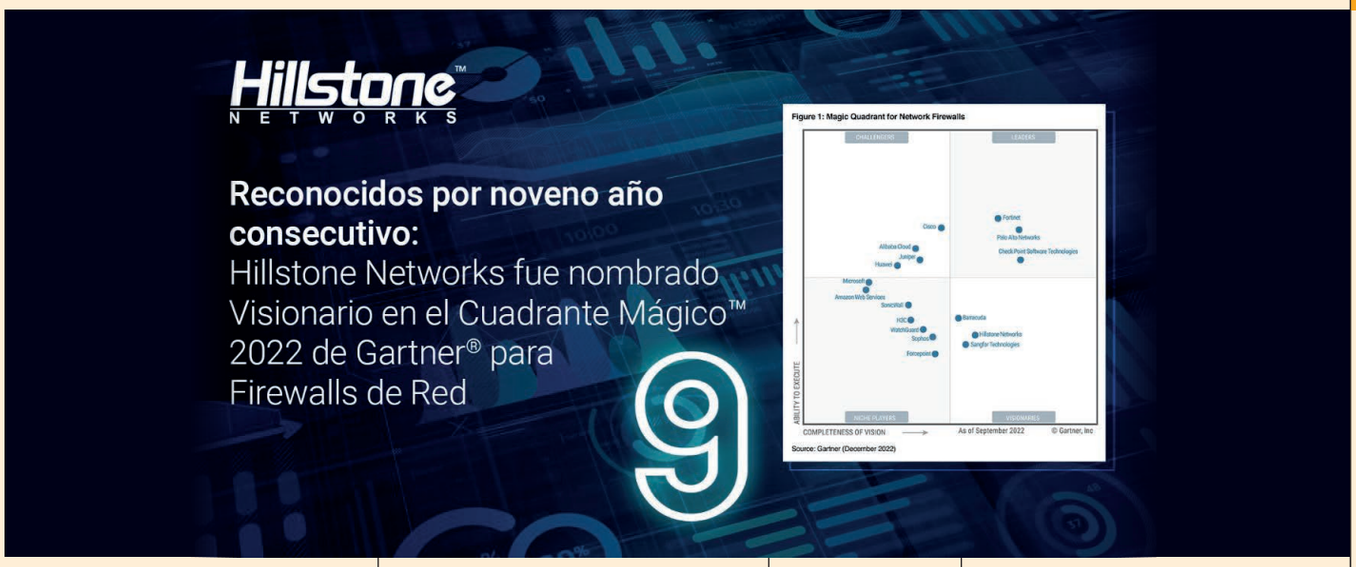
Por otra parte, Luis Zavaleta aprovechará sus conocimientos en search, social, data, performance, ecommerce (incluidos los marketplaces) para impulsar la operación de Lumière Platform y Barracuda. Cuenta con 21 años de experiencia en la industria, 14 de ellos enfocados en el desarrollo digital y conocimiento de marcas y plataformas. Lo que le permitió trabajar en 3 de los conocidos Big6's (Wpp, Publicis, Dentsu, OMG, Havas & IPG), donde logró muchos éxitos en industrias como el sector automotriz, banca, viajes, consumo, retail, entre otras.

"En una era de cambio constante; la capacidad de adaptarse rápidamente y convertir los desafíos en oportunidades es fundamental. Por lo que creemos que con pasión, experiencia, conocimientos y cultura laboral, es posible diferenciarnos en este gran mercado publicitario aprovechando las oportunidades que trae consigo la Industria, el trabajo constante nos permitirá tener una gran cuota de mercado y continuar con nuestras metas de expansión para 2023", reiteró Ricardo Izquierdo.

Por su parte en esta fase de crecimiento, venimos construyendo un proyecto sobre educación llamado Barracuda University donde se busca impulsar el conocimiento sobre tecnología, marketing digital, soluciones emergentes, entre otros temas, de la mano de expertos y al mismo tiempo fortalecer a su equipo e impulsar y aprovechar el talento de todo el equipo, explicó Izquierdo. [*]

GARTNER UBICA COMO VISIONARIO A HILLSTONE NETWORKS EN SU CUADRANTE DE FIREWALLS DE RED

Hillstone Networks ha anunciado que nuevamente ha sido reconocido en el Cuadrante Mágico de Gartner 2022 en Network Firewalls por noveno año consecutivo y nombrado Visionario por segunda vez.



Las soluciones de Hillstone Networks han evolucionado desde una plataforma de seguridad de red a una sólida cartera de ciberseguridad que ofrece ciberresiliencia, desde el edge hasta el cloud, y todo lo que esté entre ellos. Desde las PYMES hasta los requisitos de red más exigentes de red los carriers-class, así como en todos los principales sectores verticales a nivel mundial. La cartera actual aprovecha el Next Generation Firewall (NGFW) fundacional para incluir las siguientes soluciones:

- Solución Hillstone Secure SD-WAN para empresas distribuidas.
- Solución Hillstone ZTNA, que permite el acceso Zero Trust desde cualquier dispositivo, en cualquier lugar.
- Hillstone CloudArmour, protección de cargas de trabajo en la nube.
- Hillstone CloudHive solución de microsegmentación para centros de datos virtualizados.
- Hillstone sBDS, protección de servidores integrada con la solución de detección y respuesta de red (NDR) contra amenazas multietapa y multicapa dirigidas a servidores y hosts críticos.
- Hillstone iSource, una plataforma de detección y respuesta ampliada (XDR) impulsada por IA que incluye funciones NDR y aportaciones de plataformas de terceros.

"Estamos encantados de volver por noveno año consecutivo al reconocimiento de nuestra visión completa y capacidad de ejecución", afirma Tim Liu, CTO y cofundador de Hillstone Networks. "En el mundo híbrido multicloud de hoy en día, nuestra estrategia cloud-first resuena con clientes y socios por igual. Seguimos aprovechando la galardonada plataforma NGFW, líder en el sector, e integramos funciones avanzadas para desbloquear las capacidades SD-WAN y ZTNA y ofrecer soluciones adicionales que cubran las carencias del mercado, así como las necesidades de nuestra creciente base de clientes."

Un enfoque cloud-first es un mandato para ofrecer soluciones ciber-resistentes eficaces que protejan los activos críticos de la empresa y la infraestructura. Más allá de los entornos locales, privados y de nube híbrida, el portafolio de soluciones de Hillstone Networks incluye seguridad IoT que ayuda a detectar, proteger y gestionar los riesgos de forma proactiva en todos los dispositivos IoT.

Gartner, Cuadrante mágico de Gartner para Network Firewalls, Rajpreet Kaur, Adam Hils, Thomas Lintemuth, 19 de diciembre de 2022. [*]

MAYORISTAS

Carlos Soto

INGRAM MICRO DESARROLLA NUEVO CENTRO DE DISTRIBUCIÓN PARA ATENDER LAS CRECIENTES NECESIDADES DEL MERCADO DE RETAIL Y MOVILIDAD

El viernes pasado Ingram Micro México inauguró oficialmente su Centro de Distribución Cuautitlán, el cual se encuentra ubicado en la colonia Axotlán en el municipio de Cuautitlán, Izcalli en el Estado de México.

Con una superficie de casi 5mil metros cuadrados, el nuevo CEDIC, albergará principalmente productos enfocados en el segmento de retail y movilidad. Este centro de distribución tiene la capacidad de procesas más de 400 mil unidades por mes.

Al respecto, Luis Férez, SVP y presidente de Latinoamérica en Ingram Micro, comentó que el desarrollo de este nuevo centro de distribución es una muestra de cómo Ingram hace frente a las necesidades del mercado.

Desde el CEDIC atenderemos primordialmente las necesidades de los centros de distribución de los retailers, de carriers y prácticamente cualquier punto de venta que se encuentre en territorio nacional", comentó Férez.

Al interior del recinto también se encuentra un área de oficinas, donde predomina el concepto de las oficinas corporativas, es decir, cualquier colaborador puede hacer uso libremente de un espacio para trabajar. En el área de almacén destaca el orden con que se llevan a cabo las actividades y particularmente se percibe una tendencia de concientización ecológica, ya que el mayorista ha implementado una máquina que hace cajas a medida, la cual además de hacer más eficiente el embalaje de los productos también reduce el desperdicio de cartón, tema sumamente importante y que no debe pasar desapercibido por otros mayoristas. [*]

TANIUM REVELA QUE LOS ATAQUES DIRIGIDOS A LOS EMPLEADOS SON LA CAUSA PRINCIPAL DE LOS INCIDENTES DE CIBERSEGURIDAD EVITABLES

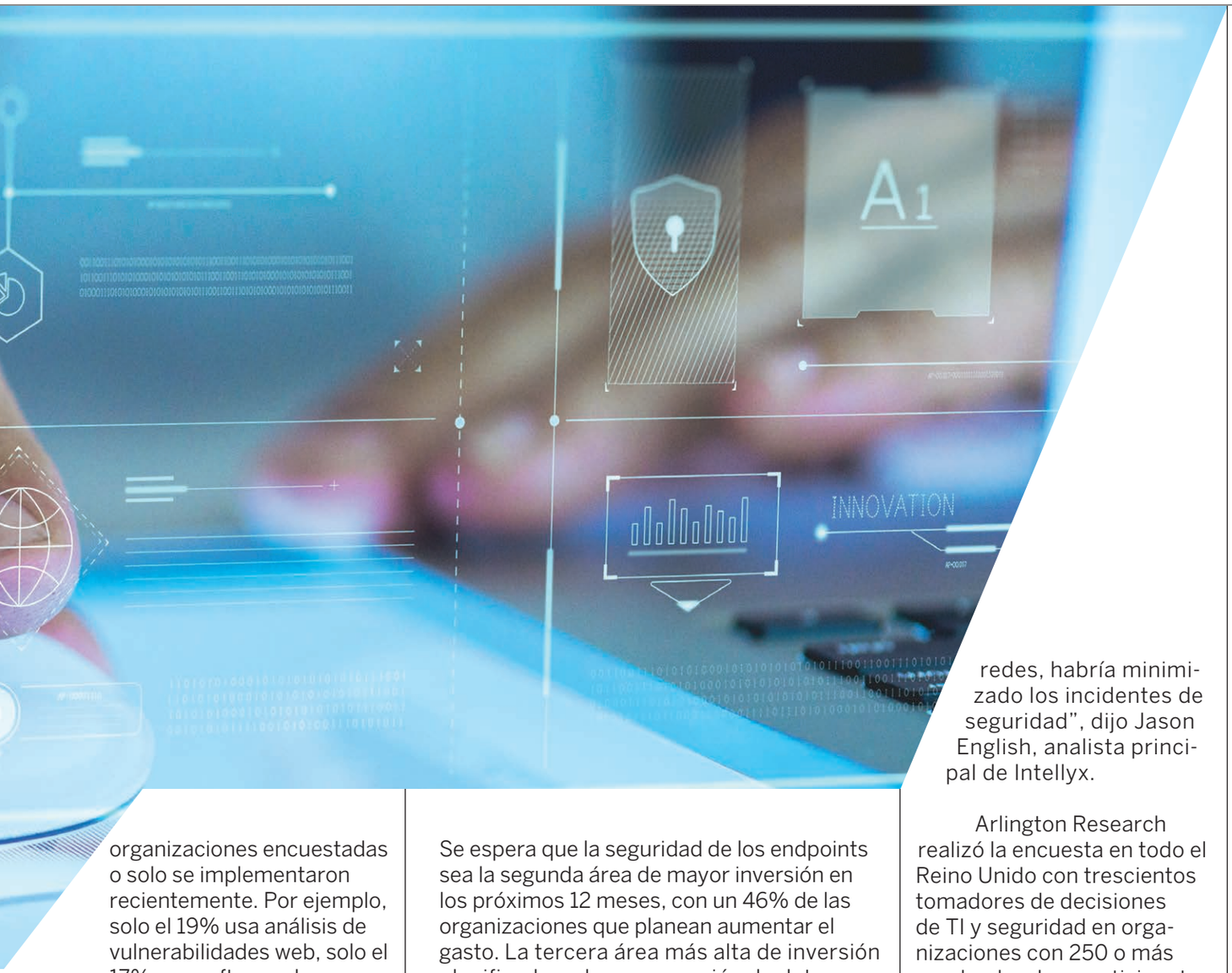
Tanium publicó una investigación que revela que los ataques dirigidos a los empleados son la causa principal de los incidentes de ciberseguridad evitables.

El estudio, "Seguridad cibernética: más vale prevenir que remediar", revela la cantidad de tiempo y recursos que las organizaciones gastan en medidas de ciberseguridad reactivas en comparación con las preventivas y la razón detrás de sus decisiones. El informe encuestó a los tomadores de decisiones de TI del Reino Unido en una variedad de industrias, incluido el sector público, los servicios financieros, la atención médica y el comercio minorista. Los resultados muestran que el 54% de los encuestados mencionaron que el personal hace clic en enlaces de phishing como el problema más común que puede facilitar un ataque cibernético exitoso. El informe también revela problemas de ciberseguridad que se han visto exacerbados por el cambio al trabajo híbrido, ya que el 71% de los propietarios de empresas y socios encuentran más difícil defenderse de las amenazas hoy que antes de la pandemia.

"Está claro a partir de nuestra investigación que muchas organizaciones están luchando para protegerse contra las amenazas cibernéticas en el entorno de trabajo híbrido", "Durante la pandemia, las organizaciones tuvieron que implementar nuevas tecnologías de la noche a la mañana para garantizar la continuidad del negocio. El mosaico de soluciones que se armó apresuradamente dejó importantes brechas de seguridad. Estas brechas aún existen y deben corregirse, lo cual es una de las razones por las que a los tomadores de decisiones de TI les resulta más difícil proteger sus entornos; y esto se reproduce en todo el mundo", señaló Miguel Llerena, vicepresidente para Latinoamérica de Tanium.

LOS HALLAZGOS CLAVE INCLUYEN:

- El phishing y las configuraciones incorrectas de seguridad son las principales preocupaciones de los líderes de TI. El 64% de los encuestados del sector público encontró incidentes de seguridad evitables causados por empleados que hacen clic en un enlace de phishing. El segundo incidente evitable más alto, citado por el 50% de los encuestados, son las configuraciones incorrectas de seguridad, como que los empleados no protejan con contraseña los datos confidenciales. Esta tasa se eleva al 57% entre las organizaciones con 250-500 empleados.
- Las organizaciones no cuentan con la tecnología adecuada para proteger los activos de TI. El tercer incidente evitable más común es la falta de software para prevenir ataques cibernéticos, citado por el 47% de los encuestados. De hecho, algunas de las principales herramientas de ciberseguridad no son utilizadas por las



organizaciones encuestadas o solo se implementaron recientemente. Por ejemplo, solo el 19% usa análisis de vulnerabilidades web, solo el 17% usa software de pruebas de penetración y solo el 11% ha usado rastreadores de paquetes durante cinco años o más.

- Áreas donde se gastarán las próximas inversiones en ciberseguridad. Al 61% de los propietarios de empresas y socios les resulta más difícil defenderse de las amenazas que antes de la pandemia. Esto los ha llevado a realizar nuevas inversiones en ciberseguridad, siendo la detección de amenazas y la seguridad de puntos finales las dos principales áreas destinadas a un mayor gasto. Casi la mitad de los encuestados (49%) espera invertir más en la detección de amenazas en 2023; las organizaciones que sufrieron un ciberataque o una filtración de datos en los últimos seis meses también son más propensas a invertir en esta área (56%).

Se espera que la seguridad de los endpoints sea la segunda área de mayor inversión en los próximos 12 meses, con un 46% de las organizaciones que planean aumentar el gasto. La tercera área más alta de inversión planificada es la recuperación de datos y las herramientas de copia de seguridad, con un 45% de todas las organizaciones dispuestas a aumentar su gasto en estas tecnologías. un número que se eleva al 58% para aquellos que han sufrido un ciberataque o una filtración de datos en los últimos seis meses. La cuarta y quinta áreas más importantes de inversión potencial son la capacitación para la concientización de los empleados (43%) y los nuevos dispositivos finales (42%), respectivamente.

"Las organizaciones luchan por enfrentarse a vulnerabilidades conocidas y desconocidas en una superficie de ataque cada vez mayor de puntos endpoints, y los resultados de esta encuesta confirman esta realidad. Los equipos de seguridad con poco personal y equipamiento buscan un enfoque de seguridad cibernética más proactivo, pero a menudo no invierten en contramedidas hasta que ocurre un incidente. El estudio encontró que el 86% de las organizaciones comprometidas por una brecha en los últimos seis meses creen que una mayor inversión en medidas preventivas, como capacitación del personal o herramientas que brinden una mayor visibilidad de las redes, habría minimizado los incidentes de seguridad", dijo Jason English, analista principal de Intellyx.

Arlington Research realizó la encuesta en todo el Reino Unido con trescientos tomadores de decisiones de TI y seguridad en organizaciones con 250 o más empleados. Los participantes procedían del sector público, la banca y los servicios financieros, la tecnología, manufactura, comercio minorista, telecomunicaciones, atención sanitaria y la educación.

"La gran cantidad de encuestados que mencionan la seguridad de los endpoints como una inversión futura prioritaria subraya los desafíos que enfrentan las empresas de todo el Reino Unido y el mundo. Es difícil, si no imposible, proteger los datos y los dispositivos de los que las organizaciones no tienen visibilidad, por lo que no es sorprendente ver cómo destinan recursos para cubrir sus puntos ciegos. Al realizar estas inversiones, cambiar de herramientas puntuales a una solución de plataforma puede ayudar a reducir el costo y la complejidad en los estados de TI", finalizó Llerena. [*]

QUÉ TAN VULNERABLES SON LAS REDES SOCIALES AL ROBO DE IDENTIDAD

En México, el número de usuarios en las redes sociales va en aumento, ya que se han vuelto un medio imprescindible para interactuar a diario. Se estima que la cifra llegue a más de 90 millones en el 2023, según el informe El uso de redes sociales en México, elaborado por Statista.

La tasa de penetración de las redes sociales entre la población del país es del 78% y el rango de edad con el mayor porcentaje de usuarios que ocupan plataformas digitales como Facebook, Twitter, WhatsApp, entre otras, oscila entre los 25 y 24 años.

A la par de este crecimiento, los ciberataques también aumentaron. Para el robo de identidad de perfiles en redes sociales, los delincuentes emplean algunas tácticas como la suplantación, el hackeo a la base de datos del sitio web, el phishing de mensajes directos, entre otros métodos.

"Cuando un usuario se registra en una red social generalmente se le pide un nombre, un correo electrónico y una fecha de nacimiento para confirmar que es mayor de edad, pero, no existe una garantía de que esta información sea real, por ello, la validación de identidad o KYC (Know Your Customer) en redes sociales se convierten en una herramienta imprescindible para que las plataformas cumplan con criterios de regulaciones y al mismo tiempo brinden certeza a sus usuarios", indica, Ricardo Robledo, director general y fundador de Tu Identidad, plataforma especializada en validación de identidad de empresas y usuarios.

Explica que aquellas redes sociales que carecen de registros de validación de identidad se encuentran en una desventaja que podría poner en riesgo no sólo la seguridad y datos de sus usuarios, sino también de la empresa detrás de esa plataforma.

"La validación de identidad para personas y empresas o KYB (Know Your Business) en redes sociales es un tema clave, ya que se han dado casos de perfiles apócrifos que pueden poner el riesgo la reputación o carrera de una persona. Mientras que uno de estos perfiles empresariales, tiene un potencial mucho mayor de que a través de él se comentan otros delitos como fraude, ante eso la magnitud del riesgo se potencializa y queda de por medio el prestigio de la empresa, incluso puede verse implicada en temas legales o fiscales", añade Robledo.

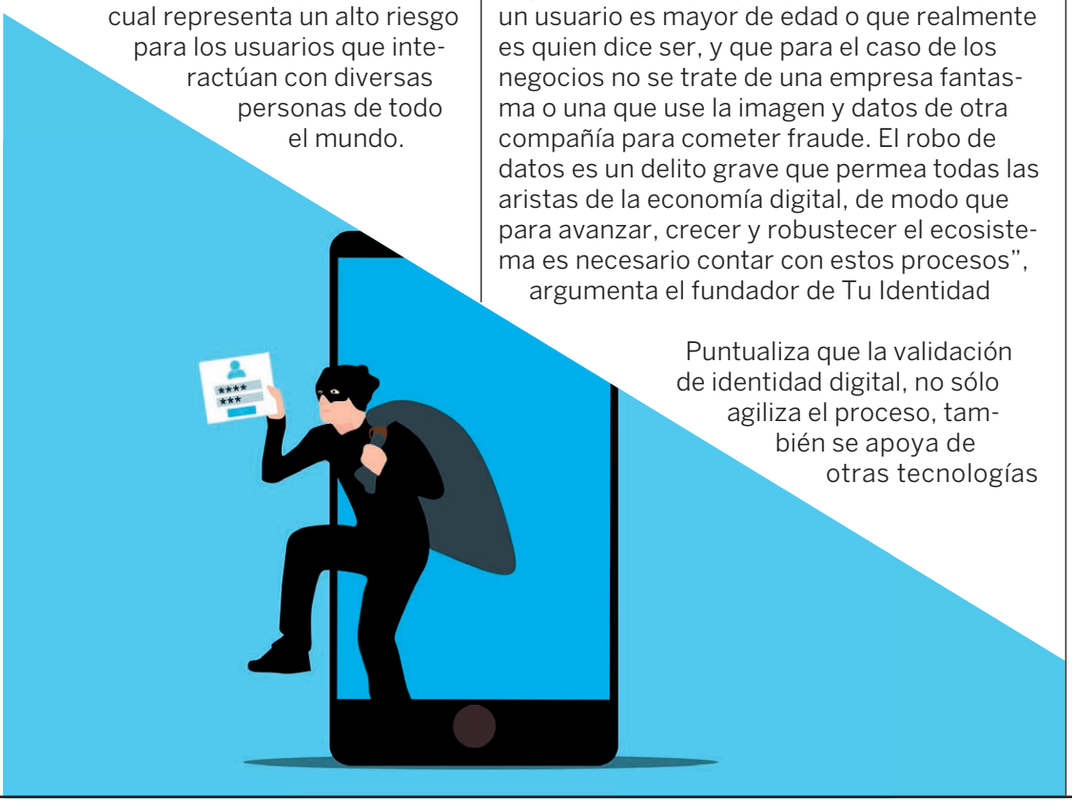
UN ECOSISTEMA MÁS ROBUSTO

No hay una cifra precisa acerca del número de cuentas falsas o bots que existen en las redes sociales, pero se estima que por lo menos el

5% de los perfiles activos, de grandes plataformas como Facebook, son apócrifos, lo cual representa un alto riesgo para los usuarios que interactúan con diversas personas de todo el mundo.

"En este contexto, los procesos KYC y KYB pueden ayudar a brindar una mayor seguridad, por ejemplo, para confirmar que un usuario es mayor de edad o que realmente es quien dice ser, y que para el caso de los negocios no se trate de una empresa fantasma o una que use la imagen y datos de otra compañía para cometer fraude. El robo de datos es un delito grave que permea todas las aristas de la economía digital, de modo que para avanzar, crecer y robustecer el ecosistema es necesario contar con estos procesos", argumenta el fundador de Tu Identidad

Puntualiza que la validación de identidad digital, no sólo agiliza el proceso, también se apoya de otras tecnologías como biometría o incluso Inteligencia Artificial, lo cual, además de ágil, la hace confiable y permite a las empresas reducir hasta un 60% del costo.



REDES SOCIALES COMO CANALES DE VENTA Y EXPOSICIÓN PARA LAS EMPRESAS

Por otro lado, para muchas empresas (sobre todo las que están en etapa de desarrollo), las redes sociales representan un canal importante, tanto de ventas, como de leads o de exposición de la marca. El Estudio de Venta Online 2022 de la Asociación Mexicana de Venta Online (AMVO) señala que el 27% de los consumidores digitales sigue a sus marcas favoritas en redes sociales, 17% utiliza las redes como canales de comunicación frecuente con sus marcas favoritas y 11% las utiliza como una línea de apoyo para poder concluir sus compras.

"Para el caso de las empresas los datos hablan de que las redes son un espacio de comunicación y atención al usuario, en el cual los consumidores externar sus dudas y buscan un mayor acercamiento con la empresa. Pero cuando caen en un perfil falso pueden exponer sus datos personales e incluso información bancaria, de modo que el grado de vulnerabilidad es sumamente alto. Este tipo de fraudes se han visto con empresas de todo tipo desde retail, banca, transporte, etc.", afirma Ricardo Robledo.

El especialista de Tu Identidad concluye que si bien, los procesos de KYC y KYB en las redes sociales no inhiben por completo los fraudes o las suplantaciones de identidad, pueden contribuir para detectar y responsabilizar a las personas que hacen mal uso de estas plataformas. [*]

ESET INDICA QUE EN 2022 SE ALCANZÓ UN RÉCORD HISTÓRICO DE VULNERABILIDADES REPORTADAS

El equipo de investigación de ESET analizó el panorama de las vulnerabilidades durante 2022 para comprender cuáles son los tipos más reportados y su impacto, qué tipo de aplicaciones concentran la mayor cantidad de vulnerabilidades reportadas y cuáles son los productos en los qué se reportaron más vulnerabilidades.

Los datos destacados por ESET son:

- En 2022 se alcanzó un pico histórico de vulnerabilidades reportadas con un aumento de más del 26% con respecto a 2021.
- Entre las cinco aplicaciones con más vulnerabilidades reportadas aparecen cuatro navegadores web.
- Las vulnerabilidades de ejecución remota de código fueron las más reportadas en 2022.

"Esta información nos aporta valor para comprender nuestro nivel de exposición a las amenazas informáticas, tanto a nivel usuario como de empresa, y tener un mejor panorama de cómo actúan los actores maliciosos", comenta Mario Micucci, Investigador de Seguridad Informática de ESET Latinoamérica.

En 2022 se alcanzó un pico histórico con 25226 vulnerabilidades reportadas en distintos productos y fabricantes. Esta cifra representa un crecimiento de 26,5% en el número de vulnerabilidades reportadas en comparación con 2021 y equivale a unas 70 vulnerabilidades por día, situación que demuestra que si el promedio diario se mantiene y se puede proveer un aumento de detecciones para el 2023 respecto a 2022.

De las vulnerabilidades reportas, solo el 3,4% son de carácter crítico. Esto representa una caída con respecto a 2021 donde el porcentaje de vulnerabilidades criticas reportadas fue del 5,81%. Por lo tanto, si bien durante 2022 se descubrieron más vulnerabilidades que otros años, la severidad de las mismas fue menor.

APLICACIONES CON MAYOR NÚMERO DE VULNERABILIDADES REPORTADAS EN 2022

Se detallan las 10 aplicaciones sobre las cuales se reportó un mayor número de vulnerabilidades el último año. Desde ESET recomienda prestar atención a las nuevas vulnerabilidades que se detectan sobre un determinado software o aplicación web para actualizar e instalar a tiempo los parches de seguridad y no ser víctimas de ataques que busquen explotar estos fallos.

Dentro del Top 10 de aplicaciones con más fallos reportados aparecen varios navegadores web. El primero en la lista es de hecho el navegador Google Chrome, el cual es utilizado por millones de usuarios. El segundo lugar lo ocupa el navegador Firefox, que también es de uso masivo. En tercer puesto aparece el gestor de bases de datos Mysql, que también es muy utilizado tanto en infraestructuras de tecnología como por usuarios finales.

"Si pensamos en términos de rédito, para los ciberatacantes las aplicaciones más utilizadas siempre serán las

más propensas a ser explotadas, ya que generalmente los actores maliciosos buscan llegar a la mayor cantidad de personas/víctimas posibles. En 2022 solamente Google lanzó varias actualizaciones de Chrome en las que reparó nueve vulnerabilidades zero-day que afectaban al navegador y la propia compañía aseguró estar al tanto de reportes que indican que estaban siendo explotadas por actores maliciosos al momento de su hallazgo", agrega Micucci de ESET.

SISTEMAS OPERATIVOS CON MAYOR NÚMERO DE VULNERABILIDADES

Si bien Debian Linux se presenta como el sistema operativo con mayor número de fallos de seguridad reportados en el histórico hasta 2022, es importante aclarar que no necesariamente hablamos vulnerabilidades críticas.

Teniendo esto claro, en el caso de Debian Linux el histórico de vulnerabilidades reportadas desde 1999 hasta 2022 es de 7489. En 2022 se reportaron 720 vulnerabilidades, siendo 2018 el año en que se registró el mayor número con 1407. Con respecto a la severidad, de los 720 fallos reportados en 2022 solo 14 eran críticos y 109 permitían la ejecución de código.

Para el sistema Android se llegó a un récord histórico en 2022 con 899 vulnerabilidades reportadas, superando a 2020, que hasta ahora era el año en el que más vulnerabilidades se habían reportado con 859. De las vulnerabilidades reportadas en 2022, 43 de ellas fueron consideradas de alta criticidad y 102 permitían ejecutar código. En el acumulado desde 2009 a 2022 se reportaron un total de 4902 vulnerabilidades en Android.

En el caso de Fedora es el tercer sistema operativo con más vulnerabilidades reportadas desde 2007 a 2022 con un total de 4108. En 2022 se reportaron un total de 906 vulnerabilidades de las cuales 84 son de ejecución de código.

FABRICANTES CON MÁS VULNERABILIDADES REPORTADAS EN SUS PRODUCTOS

Con respecto a las compañías tecnológicas que desarrollan los software y aplicaciones dirigidas a usuarios y empresas en el primer puesto está Microsoft como el fabricante que acumula mayor número de vulnerabilidades reportadas desde sus inicios. Pero, desde ESET aclaran que para sacar mejores conclusiones es importante considerar otras variables, como la evolución histórica, la cantidad de productos en los que se han reportado fallos y la criticidad de los mismos. Solo así es posible tener un panorama más completo sobre los riesgos a los que se exponen las personas y organizaciones según los productos que utilizan. Microsoft, por ejemplo, registra el mayor número de vulnerabilidades, pero sobre una base de 719 productos, mientras que Fedora, por ejemplo, es sobre la base de 22 productos, lo que da un promedio de 190 vulnerabilidades por producto.

TIPO DE VULNERABILIDADES MÁS REPORTADAS EN 2022

Con respecto al tipo de amenazas detectadas desde ESET indican que el escenario es variado, pero se destacan las vulnerabilidades que permiten la ejecución de código con el 22% de las vulnerabilidades reportadas. Es importante mencionar que este tipo de vulnerabilidad es de alta criticidad y riesgo.

VULNERABILIDADES MÁS UTILIZADAS POR CIBERCRIMINALES DURANTE 2022 EN LA REGIÓN:

Entre las cinco vulnerabilidades más utilizadas por cibercriminales durante 2022 en América Latina hay dos que fueron descubiertas hace 10 años y afectan a servicios de uso masivo. Una de ellas es la CVE-2012-0143 cuyo exploit asociado aprovecha de una vulnerabilidad de Microsoft Windows que permite la ejecución remota de código arbitrario, y la segunda es la CVE-2012-0159 cuyo exploit abusa de una vulnerabilidad en Microsoft Windows que también permite acceder remotamente y sin necesidad de autenticación a un sistema vulnerable. En relación a esto, Micucci de ESET, advierte: "La vigencia de estas vulnerabilidades sin dudas habla de que aún existe una falta concientización por parte de los usuarios y debería despertar las alarmas para que aboguen por implementar buenas prácticas de seguridad que contemplen la instalación de actualizaciones y parches de seguridad a fin de evitar posibles incidentes".

Además, desde ESET agregan que las aplicaciones de uso masivo siempre estarán en la mira de los atacantes para buscar vulnerabilidades y no es casual que las aplicaciones de uso masivo siempre tengan más vulnerabilidades asociadas que el resto para las que los cibercriminales se esfuerzan en desarrollar exploits y desplegar sus ataques. Por lo que recomiendan estar al tanto de las nuevas vulnerabilidades, siempre mantener los sistemas actualizados y contar con una solución de seguridad instalada en todos los dispositivos. [*]

Síguenos en las Redes Sociales

facebook.com/SecuriTICmx

twitter.com/securiticmx

linkedin.com/company/securitic