SecuriTIC
Latinoamérica

Información de Valor para Integradores de Seguridad Electrónica y Ciberseguridad

Panorama 2023

entre la incertidumbre y los buenos deseos

VIDEOVIGILANCIA

Hikvision reconoce a Distribuidores Oficiales en su primer Hikvision Stores Meeting 2022

LANZAMIENTOS

Dell Technologies presenta su nuevo Dell PowerProtect Data Manager Appliance

Enero 2023 Año 10 Número 115 www.securitic.lat

NUEVO
PRODUCTO

MinMoe
Terminales de Reconocimiento Facial

HIKVISION®

Evoluciona a un control de acceso con **reconocimiento facial e inteligencia artificial**

DS-K1T320 Series

Algoritmo de aprendizaje profundo
Software anti-suplantación de identidad facial y protección de privacidad

Fácil configuración del dispositivo
Admite configuraciones web a través de PC y teléfono móvil

Múltiples métodos de autenticación
Incluyendo Caras, Huellas, Tarjetas, Código PIN

Despliegue flexible
Es compatible con la implementación en la nube y en las instalaciones

Aprende más sobre MinMoe

@HikvisionMx
www.hikvision.com/es-la

Hik-Connect

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. Enero 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.

Panorama 2023

entre la incertidumbre y los buenos deseos

Para muchos la llegada del nuevo año trae un mensaje de esperanza y buenos deseos, principalmente después de haber pasado una de las peores crisis a nivel mundial derivada de la pandemia de covid-19, sin embargo, las noticias no son alentadoras, expertos del Fondo Monetario Internacional como el economista en jefe y director de estudios Pierre-Olivier Gourinchas han anunciado desde hace meses que en 2023 al menos un tercio de los países tienen grandes posibilidades de entrar en recesión.

En América Latina, en el mejor de los casos se vislumbran bajos niveles de crecimiento, aunque también se pronostica que la inflación supere los 11 puntos porcentuales. Entonces la pregunta que nos deberíamos hacer es, qué pasará con los mercados de seguridad electrónica y ciberseguridad.

Afortunadamente, los especialistas que se dedican a este tipo de negocios saben que las oportunidades siguen creciendo. Por ejemplo, a finales de octubre durante el IDX 2022, el mayorista Ingram Micro compartió que hacia 2024 se espera un gasto en soluciones de ciberseguridad y seguridad física a nivel global que ronde los 204 billones de dólares.

MERCADO DE SEGURIDAD ELECTRÓNICA

Para los integradores y distribuidores de soluciones de seguridad electrónica el panorama en 2023 es retador, ya que los jugadores más importantes, llámense fabricantes o mayoristas, no están marcando la pauta a seguir. De alguna manera la estrategia de mantener bajo perfil es una constante que ha marcado la industria en los últimos años.

Sin embargo, es imposible crecer en un ambiente cerrado, a lo largo del tiempo hemos visto cómo se desvanece la imagen o la percepción que se tenía de marcas como Pelco, Panasonic o Bosch, por mencionar algunas.

De los grandes jugadores de antaño solo Axis Communications ha mantenido su estrategia de comunicación, al menos en soluciones para mercados verticales; en el caso de Hanwha Techwin, si bien se alejaron de los reflectores, la marca en otros tiempos supo establecer muy buena relación mediática por lo que esperamos que retomen el camino que los llevó a ser una de los fabricantes más destacados entre los canales; en el mismo caso se encuentra Provision ISR, que bajo la batuta de Martín Calamante crecieron a pasos agigantados y luego se fueron apartando lentamente hacia una estrategia más conservadora en temas de comunicación; el último referente sería Vivotek que empezó con muchas ganas a compartir información y rápidamente se le agotaron las energías.

Tal parece que el empuje que dieron los gigantes asiáticos como Hikvision y Dahua en los últimos años han intimidado a los demás jugadores del mercado.

Pero el 2023 seguro nos traerá nuevas sorpresas, Bolide por ejemplo, una marca que ha tenido varios intentos de posicionarse en el mercado ahora trae el apoyo de Berenice Barrón, especialista de marketing que sabe cómo hacer crecer una marca desde cero.

También tenemos en la mira a Uniview, que lleva ya varios años trabajando arduamente, pero le falta todavía confianza para dar a conocer sus logros. Aunque la marca cuenta con todo el apoyo de Tecnosinergia aún le falta demostrar al canal el alcance

que tienen sus soluciones para hacerse un lugar entre las marcas preferidas para hacer negocio.

En el caso de los mayoristas, Syscom y TVC en Línea siguen siendo la punta de lanza en transacciones, sin embargo, el mercado que todos buscan es el de proyectos y ahí el panorama cambia. En este segmento, esperemos ver nuevamente información por parte de empresas como Tecnosinergia, Adises, Portenntum, MRKTEC, Magocad, Centro de Conectividad, ISTC y Q Digital, por mencionar algunos, es decir, que vuelvan este 2023 a retomar los bríos que tuvieron en épocas anteriores a la pandemia donde tenían una participación mucho más activa en el mercado.

Con mayor empatía por los canales, fabricantes y mayoristas del mercado de seguridad electrónica se darán cuenta que son el ejemplo a seguir en 2023, y que el éxito de sus empresas será consecuencia del crecimiento que tengan los canales. En este caso, conviene más confiar en los buenos deseos, en lo que fluye información que ayude a identificar las oportunidades que depara el año nuevo.

MERCADO DE CIBERSEGURIDAD

En el caso de los especialistas en ciberseguridad, el panorama de oportunidades sí está marcado por fabricantes y mayoristas. En prácticamente cualquier reporte de amenazas se expone que el cibercrimen seguirá su escalada de crecimiento, y por ende, la necesidad de proteger a las empresas.

A diferencia del mercado de seguridad electrónica, el de ciberseguridad no tiene dudas de la importancia de la comunicación, de hecho, cada vez más fabricantes de soluciones han buscado hacerse visibles.

Hace varios años era común leer acerca de lanzamientos o actividades de Cisco, Fortinet, Palo Alto, Check Point Software, WatchGuard, Sophos, SonicWall, Symantec, Kaspersky, ESET, por mencionar algunos; a éstos, ahora se suman nombres nuevos como Stellar Cyber, Lumu Technologies, Netskope, Hillstone Networks, Appgate, Fluid Attacks, Tanium, Akamai, entre muchos otros.

Cada uno desde su trinchera, aporta información de valor que guía a los canales hacia mejores oportunidades, ya sea con planes de capacitación para enfrentar la escasez de especialistas en ciberseguridad hasta estrategias para facilitar su arribo al mundo de los servicios administrados.

En 2023, dicen los expertos, como Juan Alejandro Aguirre, Gerente de Ingeniería en Sophos Latinoamérica, que el Cibercrimen como Servicio permitirá que los ataques sigan su escalada y cada día será más necesario recurrir a un equipo de expertos que se encarguen de la ciberseguridad de las empresas bajo esquemas de suscripción mensuales, que permitan escalar la infraestructura de acuerdo con las necesidades y temporalidad de cada negocio, con tan solo unos clics.

Del lado de los mayoristas, el mercado de ciberseguridad tiene varios jugadores interesados en aprovechar las grandes oportunidades, tenemos el caso de Ingram Micro que a través de su plataforma Xvantage está revolucionado la forma en que los canales adquieren productos y servicios no solo de seguridad sino todas sus unidades de negocio, por lo tanto, en 2023 veremos cómo van a ir reafirmando su liderazgo en la preferencia de los canales.

Otro jugador destacado es Licencias OnLine que está trabajando arduamente en consolidar un portafolio enriquecido en soluciones de ciberseguridad que se adapte a las necesidades que demanda el mercado.

Aunque no son los únicos, seguramente MAPS, Grupo Dice, TD Synnex y Compusoluciones saldrán a relucir con estrategias para garantizar los mejores negocios para sus canales.

De este lado, no solo existen buenos deseos sino bases bien cimentadas de cómo sacar el mejor provecho a una de las más grandes megatendencias a nivel global, la ciberseguridad. Por lo tanto el panorama es muy alentador y se auguran grandes negocios para todos los especialistas que se dedican a resolver este tipo de proyectos. [*]

GENETEC LANZA REPORTE DEL ESTADO DE LA SEGURIDAD ELECTRÓNICA 2022

Genetec compartió los resultados de su Informe del Estado de la Seguridad Electrónica 2022.

Basado en la experiencia de más de 3.700 líderes de seguridad electrónica en todo el mundo (incluidos usuarios finales e integradores/ instaladores/ proveedores de sistemas), el reporte analiza las estrategias de seguridad que las organizaciones están implementando para navegar de manera efectiva las realidades de un ambiente cambiante.

México – Nube: Para proyectos sin implementación en la nube, en México se indicó que el COVID-19 había "activado" su estrategia de nube con más frecuencia que en cualquier otra región (9,8%). Sin embargo, para proyectos donde la nube ya se estaba implementando, solo el 17,4% de los encuestados de México sugirió que el COVID-19 aceleró un poco su estrategia de nube, en comparación con el 30,9% a nivel global. Asimismo, tuvieron la porción más baja de encuestados (29,4%) que indicaron que se aceleró "algo" o "mucho", en comparación con el 46,7% a nivel global.

Las preocupaciones sobre la seguridad cibernética están aumentando: la convergencia de la tecnología de la información (TI) y la seguridad está inspirando nuevos enfoques para implementar y administrar una estrategia sólida de seguridad cibernética. El 64% de los encuestados de TI y el 54% de los encuestados de seguridad indicaron que las herramientas de ciberseguridad han sido uno de los enfoques principales este año.

Uso de la seguridad para las operaciones comerciales: la encuesta mostró que casi dos tercios (63%) de todos los encuestados y 7 de cada 10 organizaciones con más de 10.000 empleados describieron la seguridad electrónica y los datos relacionados como de "misión crítica". En los últimos años, la seguridad electrónica se ha convertido en un activo estratégico para hacer frente a una variedad de desafíos que van más allá de la simple mitigación del riesgo y ahora juega un papel mucho más importante en la transformación digital de las organizaciones.

El futuro de la seguridad es híbrido: el 54% de los usuarios finales encuestados indicaron que la visión objetivo de su organización para la implementación de la seguridad es una combinación de soluciones locales y basadas en la nube. Un enfoque híbrido permite a las organizaciones optimizar sus inversiones locales existentes mientras aprovechan las opciones de la nube para ahorrar costos, aumentar la seguridad y la eficiencia, y permitir el acceso remoto a los sistemas y sensores.

La seguridad se unifica: la mayoría de los encuestados (64%) informaron que utilizan videovigilancia y control de acceso en sus implementaciones de seguridad electrónica. De ellos, el 77% indicó que su organización había implementado la integración entre los sistemas de videovigilancia y control de acceso de diferentes proveedores, o una solución unificada de videovigilancia y control de acceso de un solo fabricante.

"Toda organización quiere tener en sus manos la última tecnología. Sin embargo, frente a restricciones presupuestarias, escasez de talento y prioridades en constante cambio, los líderes de seguridad deben hacer más con menos", dice Pervez Siddiqui, vicepresidente de Ofertas y Transformación de Genetec. "Una plataforma de seguridad unificada brinda a las organizaciones un camino para modernizar sus sistemas antiguos mientras aprovechan su infraestructura existente. Y pueden hacer esto sin un desarrollo personalizado costoso y complejo".

ANÁLISIS EN LATINOAMÉRICA

La mayoría de las preguntas de la encuesta mostraron pocas diferencias entre los encuestados en distintas regiones. Esto sugiere una visión global consistente de cómo se ha desarrollado la seguridad electrónica durante el último año. Sin embargo, a continuación, se muestran los casos en los que las respuestas de las regiones en Latinoamérica defirieron significativamente del promedio global.

Centroamérica y el Caribe - Unificación y nube: Los sistemas de seguridad unificados son menos comunes en Centroamérica y el Caribe. "Los sistemas de control de acceso y videovigilancia de mi organización no están conectados (son sistemas separados)", fue la segunda respuesta seleccionada más común en esta región. Por el contrario, esta fue la respuesta menos común en las demás regiones.

Los encuestados de esta región también indicaron que utilizan el almacenamiento en la nube pública con más frecuencia que en otras regiones. El 6,9% de los encuestados en esta región seleccionó "Almacenado principalmente con servicios de almacenamiento en la nube pública", en comparación con el 2,6% a nivel global.

Sudamérica - Trabajo remoto y ciberseguridad: El 50,4% de los encuestados de Sudamérica dijeron que sus organizaciones no tienen personal de seguridad electrónica configurado para trabajar de forma remota, en comparación al 33,7% de promedio global. También fueron los menos propensos en identificar una "mejor estrategia de ciberseguridad" como uno de los nuevos procesos que priorizaron este año. Solo el 38% de los encuestados seleccionó esto en comparación con el 49,2% a nivel global. [*]

Dahua reforzará la transformación digital inteligente y las aplicaciones de IA en 2023

2022 ha sido un año lleno de desarrollo e innovación para Dahua.

Como proveedor de servicios y soluciones AIoT centrado en video líder en el mundo, Dahua ha lanzado varias actualizaciones a su cartera de productos existente, así como una artillería de nuevos productos y soluciones que abordan necesidades y problemáticas específicas en la sociedad.

Con tecnologías clave como AIoT, big data y software, las soluciones de Dahua permiten a las familias y las empresas detectar y responder a los riesgos de seguridad y protección con mayor rapidez, precisión y eficacia que nunca. También brindan valor más allá de la seguridad, como permitir que ciudades, empresas y otras organizaciones incorporen los datos visuales capturados por nuestras cámaras como parte de sus soluciones inteligentes para todo, desde aliviar la congestión del tráfico, monitorear parques y vida silvestre, rastrear flujos de desechos, hasta mejorar ventas en tiendas de conveniencia.

Estos son algunos de los aspectos más destacados de la innovación tecnológica de este año:

Dahua Full-color: Con tecnologías como Full-color + TiOC con iluminadores duales inteligentes, disuación actica e IA; Full-color + Panoramic con dispositivos PTZ e IPC de vision panorámica de de 180° con lente dual a todo color; Full-color + ZOOM con capacidad de acercamiento óptico de 5X y función de enfoque automático que proven detalles de color claros incluso después de hacer el acercamiento; Full-color + 4K que adopta un sensor de imagen de 1/1,2" (actualmente el mejor sensor IPC de poca luz de Dahua) que proporciona un aumento del tamaño de píxel del 110 % en comparación con el sensor común de 8 MP.

WizSense: Con tecnología Quick Pick para realizar búsquedas basadas en el color de la ropa o del vehículo, y compararlos con una base de datos; y tecnología AI Scene Self-Adaption (AI SSA) que adopta un algoritmo de aprendizaje profundo que puede identificar varias escenas específicas (p. ej., lluvia, niebla, contraluz, poca luz, parpadeo) y ajusta los parámetros de imagen en consecuencia para garantizar la mejor calidad de imagen.

WizMind: Con Aplicaciones basadas en Humanos que incluye el sistema panorámico Dahua que está diseñado para capturar la conciencia situacional en escenarios que requieren una vista panorámica de 360°, 270° o 180° y Human Metadata 2.0 que está equipada con un algoritmo de aprendizaje profundo que puede ayudar a los operadores a localizar objetivos de manera más eficiente; Aplicaciones basadas en Vehículos con soluciones de estacionamiento en interior y estacionamiento en zona prohibida en exteriores; Aplicaciones de Imágenes Térmicas para el sector industrial que permiten realizar mediciones de temperatura en línea, rápidas y en todo clima.

HDCVI TEN: Con AI para todos que entregó el primer XVR de nivel de entrada con capacidades de inteligencia artificial; IA programada que permite a los usuarios configurar diferentes funciones de IA (disponibles en

la serie XVR5000-4KL-I3) según diferentes períodos de tiempo (hasta 6 períodos de tiempo por día); Iluminadores duales inteligentes con IR y luz cálida; Real 5MP 16:9 que resuelve el problema de distorsión de imagen causado por las cámaras anteriores de 5MP 4:3.

Dahua DeepHub: Pizarra interactiva inteligente que ofrece un enfoque flexible y multimedia para la enseñanza y las conferencias, brindando a los participantes una experiencia inmersiva, interactiva y rica en contenido. Cuenta con proyección inalámbrica, escritura en pizarra, videoconferencia y administración de archivos.

Además de otras innovaciones como un sistema de alarma inalámbrico, cámaras termográficas portátiles, PoE 2.0, y cámaras con transmisión 4G y energicadas con paneles solares.

TENDENCIAS Y SOLUCIONES PROGRAMADAS

La transformación digital inteligente se ha convertido en el tema principal de la industria actual. En el futuro, con la ayuda de la IA, la actualización constante de los productos de monitoreo inteligente se convertirá en el principal punto de crecimiento de la industria de monitoreo de seguridad en las ciudades desarrolladas de todo el mundo.

De hecho, el libro electrónico "2023 Trends in Video Surveillance" de Eagle Eye Networks menciona que las empresas están presupuestando plataformas de videovigilancia que están listas para IA y preparadas para el futuro. Según una encuesta comercial de IA de 2022 realizada por PriceWaterhouseCoopers, más del 50% de las empresas utilizan la IA de alguna manera, y más del 25 % informan una adopción generalizada de la IA dentro de su empresa. La encuesta indica que las empresas que no utilizan IA ya son conscientes de que las tecnologías nuevas y modernas automatizarán sus sistemas y procesos en el futuro; y están presupuestando para esa infraestructura ahora.

En línea con la tendencia mencionada anteriormente, haremos un vistazo rápido a algunos de los planes y programaciones de productos/soluciones de Dahua para el próximo año:

Manténgase al día con las últimas tendencias y acelere la adopción de IA: Dahua se está preparando para presentar la serie WizMind X & S en 2023. Se espera que continúe la exploración de integraciones a todo color el próximo año. También se lanzará el nuevo HDCVI 7.0, junto con actualizaciones de otros productos inteligentes como WizSense y TiOC. Además, el próximo año también se presentarán soluciones térmicas de prevención de incendios en interiores y aplicaciones de tecnología térmica en varios mercados verticales.

Innovar vigorosamente y continuar expandiendo nuevos campos: una serie de productos innovadores de Dahua se exhibirán en 2023, incluidos: dispositivos de visualización y control, incluidos monitores LCD, paredes de video LCD, señalización digital LCD, pantallas LED y pantallas LCD interactivas para establecimientos comerciales, así como Video Management Platform (VMP), decodificadores, controladores de empalme y teclado de red para centros de seguridad; Dahua Memory, una serie de productos flash NAND estables y confiables como SSD, tarjetas de memoria, unidades flash USB y más; Dispositivos de transmisión Dahua que incluyen conmutadores, punto de acceso inalámbrico, enrutador inalámbrico, etc.; pizarra interactiva inteligente Dahua DeepHub; y otros productos/soluciones inteligentes que incluyen un intercomunicador de video híbrido de 2 hilos, una solución de tráfico inteligente, una solución de control de acceso de la serie Insider, entre otros.

Con 2023 a la vuelta de la esquina, Dahua continuará integrando inteligencia artificial, big data e IoT en sus productos y soluciones para promover la innovación digital de las ciudades y la transformación de la inteligencia digital de las empresas, acelerando la innovación de la industria y la inclusión digital en los mercados emergentes en los próximos años. [*]

Generando confianza en las **instituciones financieras**

Para enfrentar los sinnúmeros de ataques violentos y no violentos, las instituciones bancarias de toda Latinoamérica están perfeccionando sus esquemas de seguridad; lo cual se realiza a través de cuatro factores estratégicos:

- Gestión de riesgos
- Óptimos diseños de los sistemas de seguridad
- Evaluaciones de confianza para minimizar el riesgo de fraude ocupacional (insiders)
- Implementación de equipos de respuesta a incidentes de seguridad digital (CSIRT, por sus siglas en inglés) y Centros de Operación de Seguridad (SOC, por sus siglas en inglés), equipos con la responsabilidad de recibir, revisar, analizar y responder a todo aquel reporte y actividad relacionada con problemas de seguridad de la información o seguridad física.

En este sentido, la videovigilancia cuenta con diversas opciones para que las entidades financieras puedan hacer frente a las amenazas de seguridad cambiantes, como hurtos y fraudes. Las soluciones de audio y video en red ofrecen la versatilidad y adaptabilidad necesarias para defenderse de las distintas fuentes de amenazas. La tecnología de seguridad innovadora, incluidas las cámaras de alta definición, se combina con software fiable para habilitar sistemas de vigilancia adaptados a sus necesidades.

Las soluciones de videovigilancia ayudan a proteger a clientes, personal y activos.

Las soluciones de videovigilancia en los bancos ayudan en las investigaciones, ya que con las cámaras de amplio rango dinámico y alta resolución proporcionan una cobertura clara y detallada de todas las zonas.

"La videovigilancia es un factor clave para la eficiencia, pues gracias al análisis y los procesos automatizados, damos un valor agregado, pero sobre todo ofrecemos seguridad a todos los actores de las instituciones bancarias", comenta Carlos Rojas, Business Development.

Esto proporciona una amplia variedad de funciones de seguridad capaces de monitorear diversas sucursales desde una estación de control central. Se puede supervisar las zonas de transacciones para detectar fraudes y robos, controlar la entrada a zonas y salas, configurar alertas automáticas que adviertan de comportamientos sospechosos.

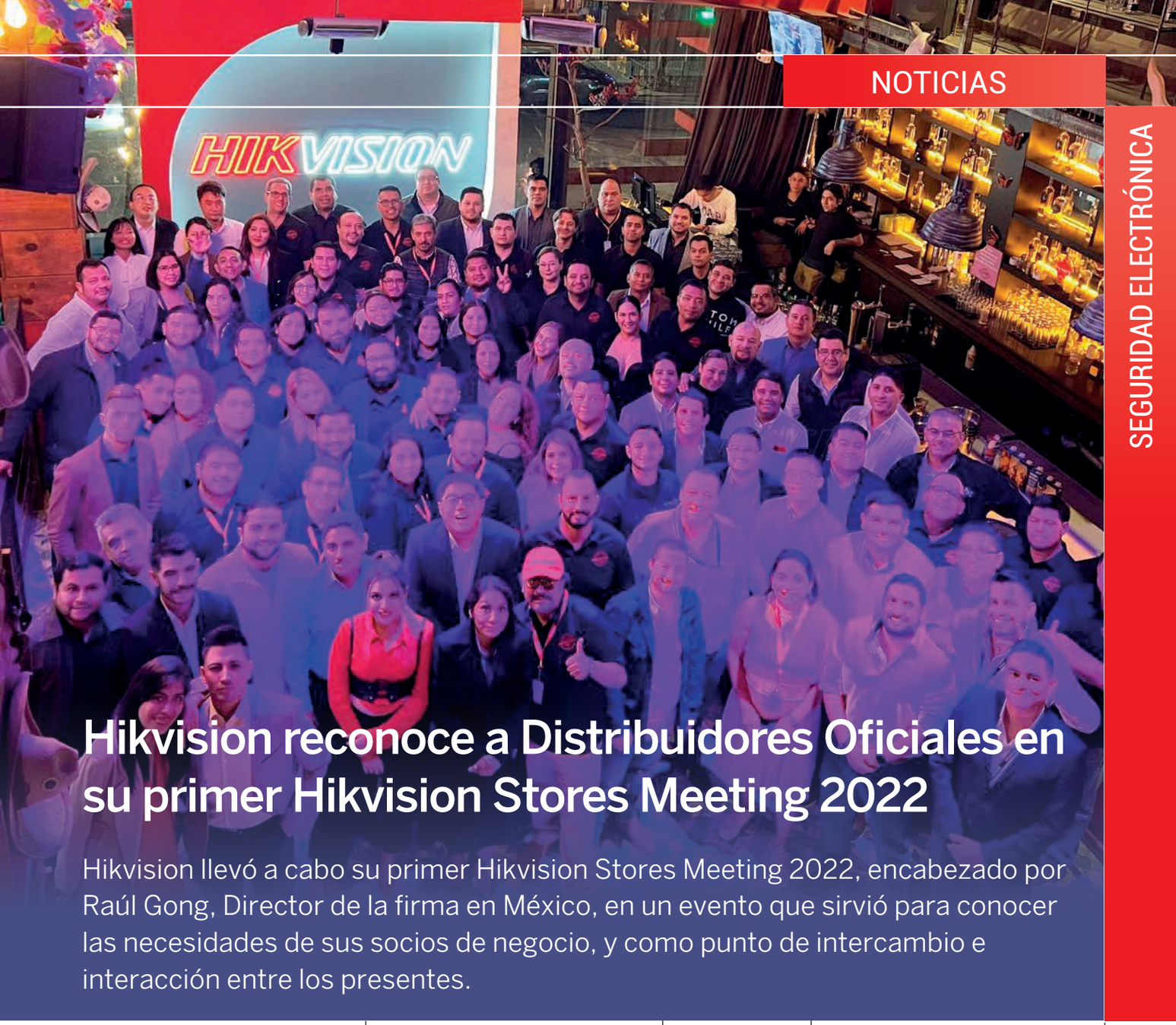
Otra área fundamental en los bancos son los cajeros automáticos, en ellos se debe contar con soluciones de audio y video en red para proteger tanto los cajeros automáticos, como a los clientes que los utilizan.

¿Y LA CIBERSEGURIDAD?

Según la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) de México, de enero a marzo del 2022 se realizaron alrededor de 1,019 millones de pagos con tarjetas en comercios tradicionales y en comercios electrónicos. Además, los pagos en comercios electrónicos representaron el 21.3% del total de pagos, lo que demuestra que dichas transacciones requieren de una atención especial para salvaguardarlas.

De acuerdo con el informe Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe de la Organización de los Estados Americanos (OEA), señala que el 92% de las entidades bancarias identificó algún tipo de evento (ataques exitosos y no exitosos) de seguridad digital. De ellos, el 37% manifestó que dichos ataques fueron exitosos.

Para generar confianza en el consumidor, los bancos deben mostrar que toda su organización es segura y sólida. "Axis permite a las entidades financieras vigilar todas las sucursales desde una ubicación central. Aplicamos las mejores prácticas de ciberseguridad en el diseño de nuestros productos, supervisamos continuamente los nuevos riesgos de seguridad", destacó Carlos Rojas. [*]



Hikvision reconoce a Distribuidores Oficiales en su primer Hikvision Stores Meeting 2022

Hikvision llevó a cabo su primer Hikvision Stores Meeting 2022, encabezado por Raúl Gong, Director de la firma en México, en un evento que sirvió para conocer las necesidades de sus socios de negocio, y como punto de intercambio e interacción entre los presentes.

En 2017 la compañía abrió su primer punto de venta en Ciudad de México. Hoy, con 45 Hikvision Stores ubicadas por todo el país, la firma continúa ampliando su presencia, ofreciendo a los clientes soluciones de seguridad y sistemas de vigilancia en video basados en la inteligencia artificial (IA), tecnología que ha sido determinante para el éxito de la compañía.

Durante la reunión, Raúl Gong agradeció el trabajo y el esfuerzo de todos y cada uno de los distribuidores de sus puntos de venta oficiales autorizados: "Es momento de mejorar y de reinventarnos para retomar el mercado con nuevas ideas y estrategias que permitan el contacto directo con los clientes finales, comprendiendo sus necesidades, gustos y preferencias tecnológicas, con foco en un servicio personalizado y eficiente".

Camilo Muñoz, Sales Director Hikvision México, destaca, por su parte, que en una Era donde el consumidor está más informado, Hikvision busca crear una experiencia memorable de compra y una excelente atención al cliente: "En una Hikvision Store, el cliente visualiza una gama de soluciones tecnológicas en seguridad, que van desde cámaras IP Smart y Análogas en HD, NVR, DVR, Sistemas de control de acceso y alarmas, productos especializados para la grabación de sistemas de videovigilancia, hasta productos para el sector doméstico o pequeño negocio. De esta forma, en una sola ubicación, el usuario tendrá la oportunidad de conocer y apreciar cada uno de los productos antes de llevarlos a casa, y hallar nuevos conceptos e ideas para cualquier proyecto específico".

Uno de los planes del fabricante es continuar el desarrollo de los distribuidores oficiales autorizados de las Hikvision Stores mediante apoyos estratégicos, capacitación técnica y de ventas, materiales de mercadotecnia, descuentos e incentivos, por mencionar algunos.

Finalmente, el ejecutivo adelanta que Hikvision pondrá en marcha un ambicioso plan de expansión de nuevos establecimientos durante el ejercicio 2023. [*]

Palo Alto Networks anuncia la solución de seguridad para el segmento de salud

Los proveedores de atención médica utilizan dispositivos digitales para todo tipo de tareas, como sistemas de diagnóstico y monitoreo, equipos de ambulancia y robots quirúrgicos para mejorar la atención al paciente, por lo que la seguridad de esos es tan importante como su función principal.

Palo Alto Networks anunció Medical IoT (Internet de las Cosas, IdC) Security, la solución de seguridad Zero Trust más completa para dispositivos médicos, la cual permite a las organizaciones de atención médica implementar y administrar nuevas tecnologías conectadas de manera rápida y segura. Zero Trust es un enfoque estratégico de la ciberseguridad que protege a una organización al eliminar la confianza implícita mediante la verificación continua de cada usuario y dispositivo, es decir, confianza cero.

"El aumento de dispositivos médicos conectados en la industria de la salud trae consigo una gran cantidad de beneficios, pero estos a menudo no están bien protegidos. Por ejemplo, de acuerdo con Unit 42, un alarmante 75 % de las bombas de infusión inteligentes examinadas en las redes de hospitales y organizaciones de atención médica tenían brechas de seguridad conocidas", informó Anand Oswal, vicepresidente senior de productos y seguridad de red en Palo Alto Networks. "Esto hace que los dispositivos de seguridad sean un objetivo atractivo para los atacantes cibernéticos, ya que potencialmente exponen los datos de los pacientes y, en última instancia, los ponen en peligro".

Si bien un enfoque Zero Trust es fundamental para ayudar a proteger los dispositivos médicos contra las innovadoras ciberamenazas de la actualidad, puede ser difícil de implementar en la práctica. A través de la detección automatizada de dispositivos, la segmentación contextual, las recomendaciones de políticas de privilegios mínimos y la aplicación de políticas con un solo clic, Medical IoT Security de Palo Alto Networks ofrece un enfoque Zero Trust de una manera simplificada y sin inconvenientes. También proporciona la mejor protección contra amenazas de su clase a través de la perfecta integración con los servicios de seguridad en la nube de Palo Alto Networks, como Advanced Threat Prevention y Advanced URL Filtering.

Medical IoT Security utiliza el aprendizaje automático (Machine Learning, ML) para hacer posible que las organizaciones de atención médica:

- Establezcan procedimientos para los dispositivos con respuestas de seguridad

automatizadas: establezcan fácilmente reglas que supervisen los dispositivos en busca de anomalías de comportamiento y activen automáticamente las respuestas apropiadas. Por ejemplo, si un dispositivo médico que generalmente solo envía pequeñas cantidades de datos comienza a usar una gran cantidad de ancho de banda inesperadamente, el dispositivo puede desconectarse de internet y los equipos de seguridad recibirán una alerta.

- Automaticen las recomendaciones y la aplicación de políticas Zero Trust: hagan cumplir las políticas de acceso con privilegios mínimos recomendadas para dispositivos médicos con un solo clic utilizando los firewalls de próxima generación de Palo Alto Networks o las tecnologías de aplicación de redes compatibles. Esto elimina la creación manual de políticas, la cual es propensa a errores y requiere mucho tiempo, y se escala fácilmente a través de un conjunto de dispositivos con el mismo perfil.
- Comprendan las vulnerabilidades de los dispositivos y la situación de riesgo: accedan a la lista de materiales de software (Software Bill of Materials, SBOM) de cada dispositivo médico y mapee las exposiciones de vulnerabilidades comunes (Common Vulnerability Exposures, CVEs). Este mapeo ayuda a identificar las bibliotecas de software utilizadas en los dispositivos médicos y cualquier vulnerabilidad asociada, así como obtener información inmediata sobre la capacidad de riesgo de cada dispositivo, incluido el estado de su vida útil, la notificación de recuperación, alerta de contraseña predeterminada y la comunicación de sitios web externos no autorizados.
- Mejoren el cumplimiento: comprendan fácilmente las vulnerabilidades de los dispositivos médicos, el estado de los parches y la configuración de seguridad, y luego obtengan recomendaciones para que los dispositivos cumplan con las reglas, pautas, leyes y reglamentos médicos.
- Verifiquen la segmentación de la red: visualicen el mapa completo de dispositivos conectados y se aseguren de que cada uno esté ubicado en su segmento de red designado. La segmentación adecuada de la red puede garantizar que un dispositivo solo se comunique con sistemas autorizados.
- Simplifiquen las operaciones: dos tableros distintos permiten que los equipos de ingeniería biomédica y de TI vean la información crítica para sus funciones. La integración con los sistemas de gestión de información sanitaria existentes, como AIMS y Epic Systems, ayudan a automatizar los flujos de trabajo.

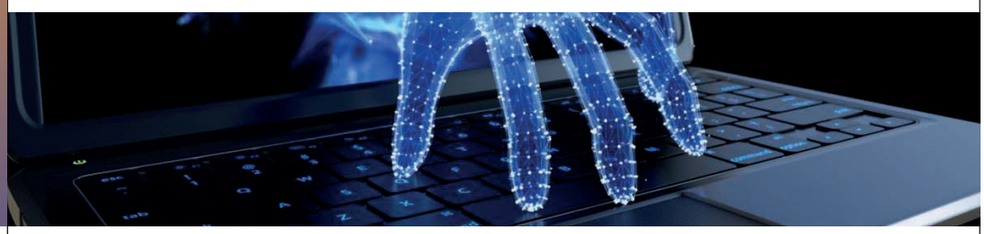
Las organizaciones de atención médica están utilizando productos de Palo Alto Networks para proteger los dispositivos que brindan atención de vanguardia a millones de pacientes en todo el mundo.

"Establecer y mantener conciencia de la situación del entorno del Internet de las Cosas Médicas es fundamental para establecer un programa de ciberseguridad empresarial eficaz. La capacidad de detectar, identificar y responder con precisión a las amenazas cibernéticas es fundamental para garantizar un impacto operativo mínimo en los procedimientos clínicos durante un evento cibernético", dijo Tony Lakin, CISO, Moffitt Cancer Center.

La solución de Palo Alto Networks se integra a la perfección con nuestros procesos de monitoreo continuo y operaciones de búsqueda de amenazas. La plataforma brinda constantemente a mis equipos información procesable que les permite administrar proactivamente la superficie de amenazas de nuestro portafolio de dispositivos médicos". [*]

Appgate comparte su panorama de ciberseguridad en 2023

Appgate analiza cómo será el panorama de riesgos, amenazas y estrategias para proteger la seguridad tecnológica en las empresas de cara al próximo año.



David López Agudelo, vicepresidente de ventas para Latinoamérica de Appgate, comenta que: "En el próximo año, esperamos que el número de incidentes reportados siga su tendencia en aumento, ya que las superficies de ataque son cada vez mayores y con más usuarios, aumentando las puertas de acceso de los delincuentes a las redes empresariales. Esto ha sido demostrado con el incremento del phishing que, por su masividad y efectividad, no solo se ha convertido en una de las principales amenazas del 2022, sino que seguirá creciendo y será el ataque más usado por los cibercriminales en 2023".

La ciberseguridad ha tomado un papel protagónico en los procesos digitales y de adopción tecnológica en las empresas. Su importancia para proteger a las organizaciones en entornos de alto riesgo seguirá siendo la prioridad, y se buscará responder efectivamente a las escaladas estratégicas de los cibercriminales. Junto a este panorama, la industria de ciberseguridad espera los siguientes comportamientos para el próximo año que Appgate ha resumido en estos siete puntos:

1. Incremento de ataques en redes sociales: Se cree que con un incremento del 50% en el número de incidentes relacionados con las redes sociales, estas sigan siendo uno de los vectores de ataque más empleados por los cibercriminales. Aquellas como: Instagram, Facebook y Twitter tendrán el protagonismo, al ser las más usadas en Latinoamérica.

2. Apps y Dispositivos móviles en riesgo: El desarrollo de nuevas apps y el uso masivo de smartphones, tablets y hasta relojes inteligentes, trae consigo un aumento en los incidentes relacionados con dispositivos móviles, ya que suelen tener menos controles de seguridad y son objetivo de aplicaciones móviles maliciosas, Smishing y Vishing.

3. Sectores más impactados: Aunque la adopción de tecnología para el desarrollo de distintas actividades empresariales e industriales pone en riesgo a todo tipo de sectores, se prevé que aquellos con mayor número de incidentes serán: el financiero y plataformas de pagos electrónicos, e-Commerce, comercios retail, wallets, portales de criptomonedas, entre otros.

4. Ransomware: Esta modalidad seguirá afectando a las organizaciones, especialmente a empresas cercanas a procesos industriales de manufactura, construcción, transporte, gobierno, educación y salud. Su evolución a una versión 2.0 tendrá gran impacto en las infraestructuras críticas y representará doble cobro, tanto por la liberación de los sistemas, como por la NO publicación de información interna de las empresas.

5. Mayor número de incidentes: En el 2022, el Centro de Operaciones de Seguridad (SOC) de Appgate, reportó un 60% más de casos catalogados como "información revelada". Este tipo de incidentes aumentarán en 2023 y estarán acompañados de aquellos como: explotación de vulnerabilidades (Cyber Threat), brechas de datos (Data Leak), fraude electrónico, suplantación de identidad (Impersonation), entre otros.

6. Conciencia y capacitación: Los cibercriminales han detectado que uno de los puntos más débiles en la seguridad informática, son las personas mismas, ya que por medio de ingeniería social, son engañados para revelar datos y comprometer credenciales. En el 2023, la concientización de los equipos de trabajo y su capacitación para tener hábitos seguros en la protección de los dispositivos y la información que manejan, será una de las prioridades para minimizar efectos de ataques como el phishing y el robo de credenciales.

7. Autenticaciones alternativas: La renovación de los mecanismos para verificar el acceso a los sistemas, más allá de las credenciales tradicionales, estará dirigida a la autenticación basada en el riesgo (RBA), la cual estará acompañada de una mayor capacidad de hardwares para soportar tecnologías que requieren reconocimientos biométricos y faciales, códigos QR, Tokens, Push, entre otros. Estos han demostrado tener una efectividad mucho mayor y mejorar la experiencia de los usuarios.

"Para el 2023, no será suficiente mantenerse al día en los avances de detección y mitigación del fraude, cada vez será más necesario contar con la implementación de soluciones preventivas de múltiples capas, que analicen las amenazas de manera integral e ir un paso adelante de los ciberdelincuentes. Además, nuestra recomendación principal para las empresas, es la articulación de un plan de seguridad con un enfoque de Zero Trust, en el cual se cubran las amenazas desde dentro y fuera del perímetro de una empresa, considerando a cualquier dispositivo, usuario o conexión como una potencial amenaza dentro de los sistemas y creando un entorno seguro alrededor de las personas", concluye David López Agudelo, vicepresidente de ventas para Latinoamérica de Appgate. [*]

SonicWall gana terreno en América Latina unificando esfuerzos con sus canales

SonicWall señaló que 2022 fue un año de crecimiento para la empresa y sus socios de negocio, alcanzando un récord de ventas interno en soluciones de firewalls de Generación 7, SD-WAN y WiFi 6.

"Hoy en día hemos visto cómo las empresas son más conscientes de los retos de ciberseguridad que enfrentan y han entendido que no es un tema aparte. Temas en expansión como trabajo híbrido y 5G serán algunos de los principales retos el siguiente año, y las empresas sin importar su tamaño deberán estar preparadas", señaló Arley Brogiato, líder de Ventas para SonicWall en América Latina".

De acuerdo con el ejecutivo, las ventas de soluciones de seguridad en este año superaron las expectativas de la compañía a nivel global, logrando un crecimiento superior al prospectado y un aumento de doble dígito en las cuotas de mercado de SonicWall.

Arley Brogiato, líder de Ventas para SonicWall en América Latina.

Al respecto, Eustolio Villalobos, Country Manager para México, Centroamérica y El Caribe de SonicWall, destacó que estos avances se deben a que la marca unificó esfuerzos con sus canales, ayudando a desarrollar proyectos y particularmente apoyándolos a incrementar el ticket promedio, dando como resultado un aumento en sus ganancias globales. "Una vez que los partners identificaron que en conjunto podíamos hacer más, las oportunidades de negocio empezaron a crecer y logramos entrar a nuevos mercados. Lo cual nos llevó a alcanzar niveles de crecimiento de triple dígito tanto en la parte de ventas de soluciones como en la cantidad de proyectos realizados."

FORTALECIMIENTO DE LA CADENA DE SUMINISTRO

En la parte de logística, SonicWall logró desarrollar una estrategia en todas las regiones del mundo, que le permitió contar con excelentes tiempos de entrega, y de esta manera marcar un diferenciador respecto al resto de los jugadores de ciberseguridad que han tenido dificultades con este tema.

De acuerdo con Arley Brogiato, un punto fundamental del éxito de la compañía es la parte de comunicación en tiempo real respecto a la disponibilidad del producto, ya que en el negocio de ciberseguridad es imprescindible tener la certeza de contar con el producto, porque de nada sirve hacer una gran labor comercial si no se puede entregar. "Mantener buenos niveles de inventario no solo beneficia al canal en reputación, también le genera ganancias adicionales. Este ha sido uno de los años en que más cheques hemos entregado por concepto de rebates, con lo cual nuestros canales están sumamente contentos pues este es un beneficio adicional que trae el trabajar con SonicWall. Además de ayudarlos a cerrar negocio, premiamos sus ventas de manera trimestral", destacó el directivo.

MÁS NEGOCIO EN EL SURESTE MEXICANO

Con el impulso que tomaron las ventas en la región, SonicWall aprovechará la oportunidad para ganar terreno en la zona del sureste del país. En este aspecto, Eustolio Villalobos explicó que ya se tuvo acercamiento con una de las principales asociaciones de distribuidores a nivel nacional, con lo cual se pronostica que poco a poco vaya fluyendo más negocio en esta región.

Asimismo, SonicWall está tomando acciones para que los ejecutivos enfocados en la región sureste del país pongan foco en los proyectos que se han ido detectando en estados como Puebla, Veracruz, Yucatán, Quintana Roo, Chiapas y Oaxaca.

2023: EL NEGOCIO ESTARÁ EN LA ENTREGA DE SERVICIOS

Una de las grandes apuestas para el 2023, es la entrega de servicios administrados de ciberseguridad. En este caso SonicWall adelanta un ajuste en el modelo de negocio para el año que viene, se trata de la posibilidad de ofrecer servicios de seguridad por contratos mensuales.

La figura del MSSP en la región de América Latina está tomando cada vez más importancia, actualmente el modelo de venta de servicios se hacía por contratos de 12 meses, sin embargo, analizando las necesidades del mercado latino, se identificó que la flexibilidad es un tema primordial que garantiza una mayor cantidad de negocio. "Ahora se abre la opción de atender a todas aquellas empresas que necesiten protección por periodos de tiempo cortos, a partir de un mes, tal cual como se hacen hoy en día con las plataformas de streaming, donde se paga mensualmente y el cliente decide en qué momento ya no requiere el servicio", destacó Brogiato.

Con esta estrategia se espera mantener los niveles de crecimiento de este año, incluso superarlos en la medida en que más MSSPs de la región se vayan sumando a las filas de SonicWall. [*]

¿Sabes por qué las empresas necesitan protección en la nube?: Hillstone Networks

En la dinámica actual de las empresas, donde es vital mantenerse innovando y avanzando a la par de los requerimientos del mercado, la tecnología de computación en la nube ofrece beneficios de almacenamiento, intercambio de datos y una gran variedad de servicios digitales.

De esta forma, las organizaciones pueden concentrarse en las actividades medulares para hacer crecer sus negocios, en lugar de desplegar, gestionar y mantener el software que necesitan para asegurar la continuidad de sus operaciones.

En este sentido, Hillstone Networks, proveedor líder de soluciones de seguridad de red y gestión de riesgos, explica que utilizar servicios e infraestructura en la nube requiere ineludiblemente contar con sistemas de ciberseguridad lo suficientemente robustos para mantener protegida la información que ahí radica. Y que la seguridad en estos casos es una responsabilidad compartida, por lo tanto, ya sea una persona, pyme o un gran compañía, deben de conocer qué implica la seguridad en la nube y qué importancia tiene para la empresa.

¿QUÉ ES LA SEGURIDAD EN LA NUBE?

Este concepto hace referencia al conjunto de medidas de seguridad que se diseñan para resguardar tanto la infraestructura, como las aplicaciones y los datos basados en la nube. Este tipo de medidas permiten garantizar la protección de la privacidad de los datos, así como el control de acceso a datos y recursos, y la autenticación de usuarios y dispositivos.

En la práctica, la seguridad informática en la nube, como también se le conoce, garantiza la seguridad y la integridad de todos los sistemas informáticos en la nube, ante el riesgo de un ataque cibernético o filtraciones de datos. Por eso, es importante confirmar que el proveedor de servicios en la nube garantice niveles de seguridad adecuados.

¿CUÁL ES EL ALCANCE DE LA SEGURIDAD EN LA NUBE?

La seguridad en la nube está diseñada para brindar un

nivel de protección de amplio alcance, incluyendo:

- Aplicaciones (servicios de correo electrónico, soluciones de productividad, etc.)
- Sistemas operativos
- Servidores de datos (hardware y software de la red central)
- Redes físicas (energía eléctrica, enrutadores, cableado, etc.)
- Datos (toda la información a la que se accede se modifica o se almacena)
- Middleware (para administrar la interfaz de programación de aplicaciones o API)
- Almacenamiento de datos (discos duros y otros dispositivos)
- Plataformas de virtualización de computadoras (software de máquinas virtuales, anfitrionas e invitadas)
- Hardware de usuarios finales (computadoras, dispositivos móviles, dispositivos IoT, etc.)

IMPORTANCIA DE LA SEGURIDAD EN LA NUBE

La seguridad en la nube puede ayudar a las empresas de muchas formas, por ejemplo:

Garantiza seguridad centralizada. Con la computación en la nube se pueden tener todos los datos y aplicaciones en una ubicación centralizada, lo que facilita su administración, así como la de todos los dispositivos conectados. De esa forma, es posible garantizar que todo esté protegido.

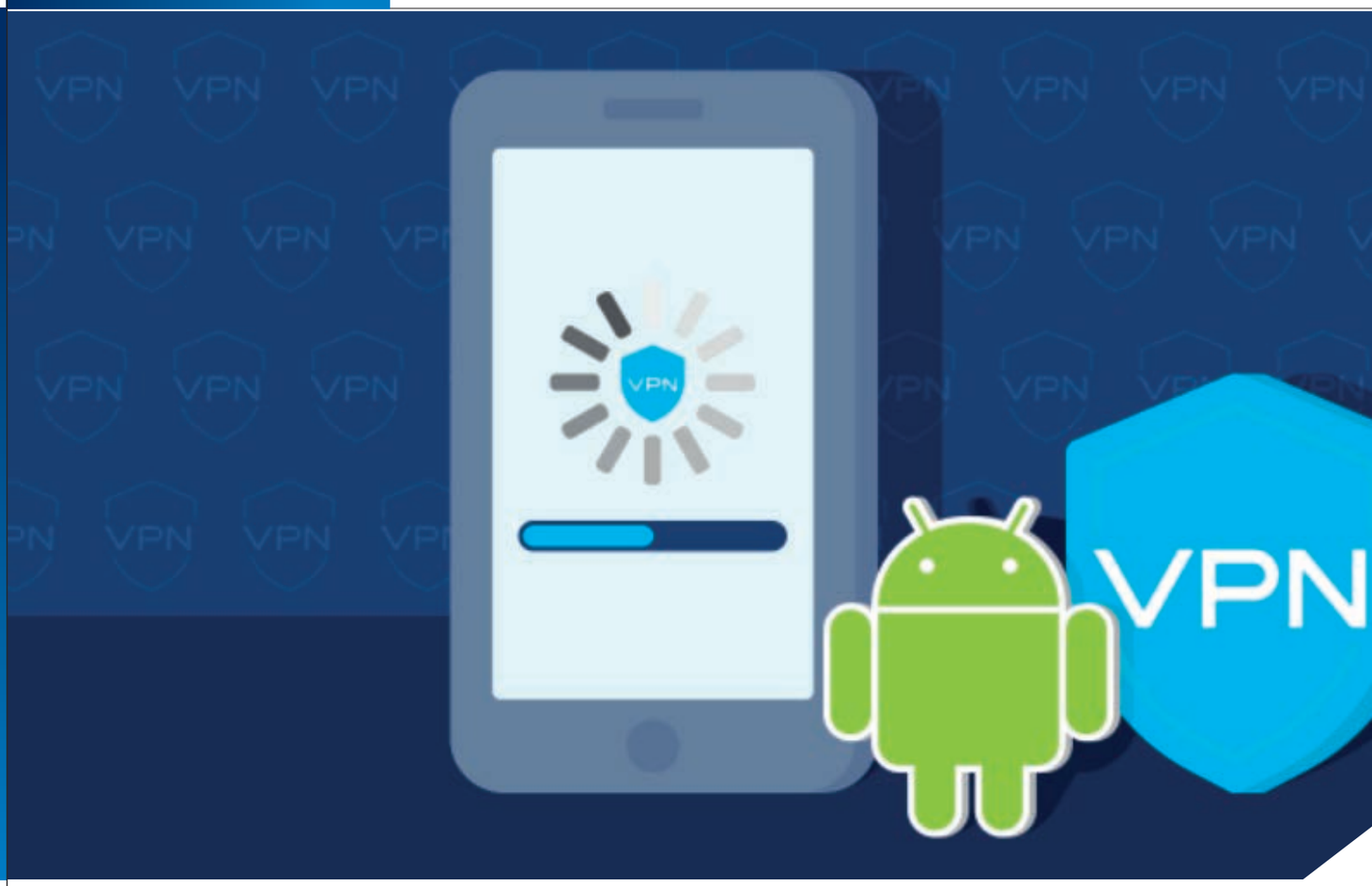
Además, una ubicación centralizada permite a las empresas de seguridad en la nube realizar tareas con mayor facilidad, por ejemplo, optimizar el monitoreo de eventos de red, mejorar el filtrado web o implementar planes de recuperación de desastres.

Ofrece costos iniciales más bajos. Al contratar un servicio de computación en la nube, no se tiene que pagar por un hardware dedicado, por lo tanto, se puede ahorrar una cantidad significativa de dinero y, al mismo tiempo, se mejora la seguridad informática.

Del mismo modo, los proveedores de soluciones en la nube (CSP) garantizan un manejo proactivo de la seguridad, desde el mismo momento en que se contrata el servicio. De esa forma, es posible ahorrar costos y reducir los riesgos relacionados con contratar un equipo de seguridad interno para proteger un hardware dedicado.

Permite escalar con mayor facilidad la seguridad informática. Frente a nuevas demandas de servicios, la seguridad en la nube ofrece más aplicaciones y almacenamiento de datos, en el momento en que el cliente lo necesite. Eso significa que cuando las necesidades cambian, la naturaleza centralizada de la seguridad en la nube permite integrar fácilmente nuevas aplicaciones y funciones, sin afectar la seguridad de los datos. También, la seguridad en la nube puede escalar en momentos puntuales en que se incrementa el tráfico, por ejemplo, y recuperar su estado inicial en lo que disminuye el tráfico.

Ayuda a gestionar mejor el trabajo remoto. Con el almacenamiento de datos en la nube, es posible tener acceso a ellos desde cualquier parte del mundo sin ningún problema. Sin embargo, esto expone mucho más la información de la empresa a riesgos de seguridad, haciéndola susceptible a ataques de phishing o malware. En ese sentido, la seguridad en la nube garantiza que los datos de la empresa se manejen de forma adecuada y estén siempre protegidos contra amenazas digitales, incluso cuando los empleados cometan errores como, por ejemplo, no cumplir con los estándares requeridos al usar el internet público. [*]



CIBERCRIMINALES APUNTAN A USUARIOS DE ANDROID CON FALSAS APPS DE VPN: ESET

ESET identificó una campaña en curso dirigida a los usuarios de Android y que lleva adelante el grupo de APT Bahamut.

Esta campaña ha estado activa desde enero de 2022 distribuyendo aplicaciones maliciosas a través de un sitio web falso de SecureVPN que ofrece descargas apps de Android. Aunque el malware empleado a lo largo de esta campaña utiliza el nombre SecureVPN, no tiene asociación alguna con el servicio y el software multiplataforma legítimo SecureVPN.

HALLAZGOS CLAVE DE ESET:

- El objetivo principal de las modificaciones realizadas a la aplicación es extraer datos confidenciales de la víctima y espiar activamente las aplicaciones de mensajería que utiliza.
- Se cree que los objetivos apuntados por los actores maliciosos son elegidos cuidadosamente, ya que una vez que se inicia el spyware Bahamut, solicita una clave de activación antes de que se pueda habilitar la funcionalidad de VPN y spyware. Es probable que tanto la clave de activación como el enlace del sitio web se envíen a usuarios específicos.
- Se desconoce el vector de distribución inicial (correo electrónico, redes sociales, aplicaciones de mensajería, SMS, etc.).
- La aplicación utilizada son versiones troyanizadas de dos apps de VPN legítimas, SoftVPN u OpenVPN, que se volvieron a empaquetar con el código del spyware Bahamut, el cual fue utilizado en el pasado por el grupo Bahamut.
- ESET identificó al menos ocho versiones de estas aplicaciones parcheadas maliciosamente con cambios de código y actualizaciones disponibles a través del sitio web de distribución, lo que podría significar que la campaña recibe mantenimiento.

El equipo de investigación de ESET descubrió al menos ocho versiones del spyware Bahamut. El malware se distribuye a través de un sitio web falso de SecureVPN bajo la forma de versiones troyanizadas de dos aplicaciones legítimas: SoftVPN y

OpenVPN. Estas aplicaciones maliciosas nunca estuvieron disponibles para descargar desde Google Play.

El malware tiene la capacidad de exfiltrar datos confidenciales del equipo de la víctima, como la lista de contactos, mensajes SMS, registros de llamadas, ubicación del dispositivo y llamadas telefónicas grabadas. También es capaz de espiar activamente los mensajes de chat intercambiados a través de aplicaciones de mensajería muy populares, como Signal, Viber, WhatsApp, Telegram y Facebook Messenger. La exfiltración de datos se realiza a través de la funcionalidad de keylogging del malware, que hace un uso malintencionado de los servicios de accesibilidad.

El grupo de APT Bahamut generalmente apunta a entidades e individuos ubicados en Medio Oriente y en el sur de Asia a utilizando como vector de ataque mensajes de phishing y aplicaciones falsas. Bahamut se especializa en ciberespionaje, y el equipo de ESET cree que su objetivo es robar información sensible de sus víctimas. Bahamut también se conoce como un grupo de mercenarios que ofrece servicios de piratería a sueldo a una amplia gama de clientes.

La aplicación maliciosa para Android que fue utilizada en esta campaña se distribuyó a través del sitio web thesecurevpn[.]com, que utiliza el nombre, pero no el contenido ni el estilo del servicio SecureVPN legítimo (en el dominio securevpn.com).

Este falso sitio web que se hace pasar por SecureVPN se creó en base a una plantilla web gratuita, que probablemente fue utilizada por el actor de amenazas como inspiración, ya que solo requirió pequeños cambios y parece confiable.

Thesecurevpn[.]com se registró el 27 de enero de 2022; sin embargo, se desconoce el momento de la distribución inicial de la falsa versión de la aplicación de SecureVPN. La aplicación maliciosa se proporciona directamente desde el sitio web y no ha estado disponible en la tienda Google Play.

"La campaña dirigida a dispositivos móviles operada por el grupo de APT Bahamut sigue en curso y utiliza el mismo método para distribuir sus aplicaciones de spyware para Android: a través de sitios web que se hacen pasar por servicios legítimos, como se ha visto en el pasado. Además, el código del spyware y, por lo tanto, su funcionalidad, es la misma que en campañas anteriores, incluida la capacidad de recopilar datos para exfiltrarlos en una base de datos local antes de enviarlos al servidor de los atacantes, una táctica que rara vez se ve en las aplicaciones móviles para ciberespionaje", comenta Camilo Gutiérrez Amaya, Jefe del Laboratorio de Investigación de ESET Latinoamérica.

Si el spyware Bahamut es habilitado, los operadores de Bahamut pueden controlarlo de forma remota y exfiltrar varios datos confidenciales del dispositivo, como:

- contactos,
- mensajes SMS,
- registros de llamadas,
- una lista de aplicaciones instaladas,
- ubicación del dispositivo,
- cuentas de dispositivo,
- información del dispositivo (tipo de conexión a Internet, IMEI, IP, número de serie de SIM),
- llamadas telefónicas grabadas y
- una lista de los archivos en el almacenamiento externo.

Al abusar del servicio de accesibilidad, el malware puede robar notas de la aplicación SafeNotes y espiar activamente los mensajes de chat e información sobre llamadas en aplicaciones de mensajería muy populares, como:

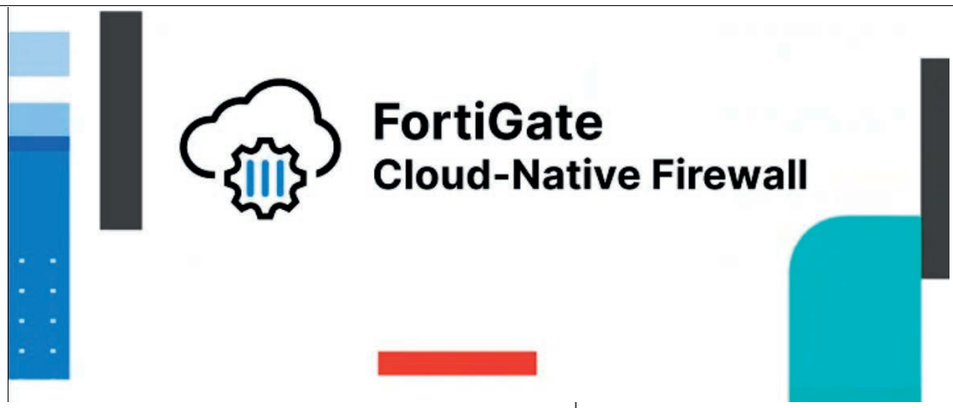
- imo-International Calls & Chat,
- Facebook Messenger,
- Viber,
- Signal Private Messenger,
- WhatsApp,
- Telegram,
- WeChat, y
- Conion.

Todos los datos extraídos se almacenan en una base de datos local y luego se envían al servidor de C&C del atacante. La funcionalidad del spyware Bahamut incluye la capacidad de actualizar la aplicación mediante un enlace con una nueva versión del servidor C&C.

"Parece que esta campaña ha mantenido un perfil bajo, ya que no vemos instancias en nuestros datos de telemetría. Esto probablemente se logra a través de una distribución altamente dirigida, donde junto con un enlace al spyware Bahamut, la potencial víctima recibe una clave de activación, que es necesaria para habilitar la capacidad de espionaje del malware.", concluye el investigador de ESET. [*]

FORTINET LANZA SERVICIO ADMINISTRADO DE FIREWALL NATIVO EN LA NUBE

Fortinet anunció el lanzamiento del firewall de próxima generación FortiGate nativo en la nube (FortiGate CNF) en Amazon Web Services (AWS), un servicio de firewall de próxima generación de nivel empresarial diseñado específicamente para ambientes AWS.



FortiGate CNF incorpora los servicios de seguridad impulsados por inteligencia artificial (IA) de FortiGuard para detección en tiempo real y protección en contra de amenazas internas y externas, y apuntalada por FortiOS para una experiencia integral a través de AWS y ambientes en las instalaciones.

Al migrar el manejo de la infraestructura de seguridad de red de Fortinet utilizando FortiGate CNF, los clientes pueden enfocarse más en sus competencias básicas, desplegando políticas de seguridad efectivas para proteger las aplicaciones y los datos críticos para su negocio. Compatible de forma nativa con AWS y disponible ahora en AWS Marketplace, FortiGate CNF brinda a los clientes acceso inmediato a los servicios de seguridad impulsados por IA de FortiGuard para una protección de nivel empresarial, incluido el filtrado de URL, filtrado de DNS, IPS, control de aplicaciones y otros servicios de seguridad de FortiGuard en los que confían las organizaciones.

FortiGate CNF otorga a los clientes los siguientes beneficios:

Protección integral para la red a costos optimizados: FortiGate CNF está diseñado para agregar seguridad, zonas de disponibilidad y nubes privadas virtuales (VPCs) en el entorno de nube de un modo sencillo. También soporta AWS para ayudar a optimizar la inversión de seguridad en la nube, utilizando AWS Gravitation para proveer mejor costo por rendimiento que otras ofertas.

Operaciones en red simplificadas con integraciones nativas en la nube: FortiGate CNF provee una interface de usuario intuitiva (UI) y simple que minimiza la necesidad de experiencia en ciberseguridad y hace que sea más fácil definir y desplegar políticas de seguridad robustas, incluyendo políticas en AWS basadas en meta-datos dinámicos. Este soporte de AWS ayuda a los equipos de seguridad a moverse a la velocidad y escala de las aplicaciones, mientras que el soporte de AWS Gateway Load Balancer elimina la automatización de bricolaje y ayuda a proteger los entornos de Amazon Virtual Private Cloud (Amazon VPC) mientras mejora la alta disponibilidad y la escala. Además, la compatibilidad con AWS Firewall Manager simplifica la administración de la seguridad y automatiza la implementación de la seguridad.

Mayor cumplimiento con seguridad de grado empresarial integral a través de despliegues en las instalaciones y en la nube: De acuerdo a una encuesta reciente realizada a más de 800 profesionales en ciberseguridad, el 78% indicó que una plataforma de seguridad en la nube centralizada en un solo punto de control podría ayudarlos a proteger mejor los datos en su huella en la nube y fortalecer su postura de seguridad. FortiGate CNF proporciona un panel intuitivo para administrar fácilmente las políticas de seguridad en las implementaciones de AWS de los clientes. Como parte de la plataforma Fortinet Security Fabric, también ofrece un panel único a través de FortiManager para centralizar la administración de políticas, aumentar la visibilidad y automatizar la aplicación de políticas en AWS. Esta capacidad ayuda a los equipos a aplicar controles de seguridad de manera eficaz en áreas on premise y de nube híbrida.

Impulsado por inteligencia de amenazas global basada en IA: FortiGate CNF incluye un conjunto de servicios de seguridad confiables impulsados por la inteligencia artificial de FortiGuard, desarrollados y mejorados continuamente. Usando modelos de aprendizaje automático/IA (ML), FortiGate CNF con los servicios de seguridad de FortiGuard permite una postura de seguridad proactiva y la remediación de amenazas conocidas y desconocidas basadas en inteligencia de amenazas en tiempo real, detección basada en el comportamiento y prevención automatizada.

FORTINET Y AWS: MEJOR JUNTOS

FortiGate CNF es el ejemplo más reciente del compromiso de Fortinet por brindar servicios nativos en la nube para ayudar a nuestros clientes. El trabajo de Fortinet con AWS garantiza que las cargas de trabajo de la nube pública de los clientes estén protegidas por las mejores soluciones de seguridad de su clase con tecnología de inteligencia integral sobre amenazas. La compatibilidad de Fortinet con los servicios clave de AWS simplifica la administración de la seguridad, lo que facilita la visibilidad completa en todos los entornos y brinda una amplia protección en todas las cargas de trabajo y aplicaciones. A lo largo de cualquier etapa de la migración de un cliente a la nube, la plataforma de malla de ciberseguridad Fortinet Security Fabric, de mayor rendimiento de la industria, ofrece redes basadas en seguridad y protección adaptativa en la nube para la máxima flexibilidad y control necesarios para construir en la nube.

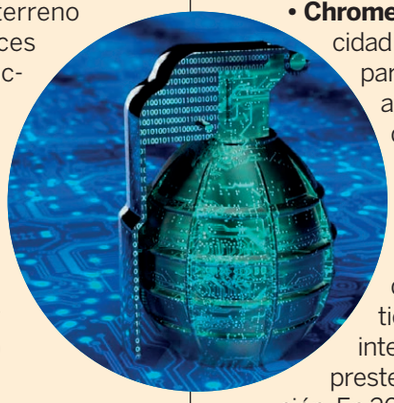
"Sabemos que las organizaciones buscan simplificar y modernizar aún más la seguridad en la nube, por lo que estamos trabajando con Fortinet para ofrecer soluciones de seguridad adaptativas en la nube. Con FortiGate CNF, los clientes pueden construir con confianza, aumentar la agilidad y aprovechar todo lo que AWS tiene para ofrecer. Como un servicio nativo de la nube completamente administrado, FortiGate CNF proporciona servicios de firewall de nivel empresarial y seguridad de red que ayudan a reducir el riesgo y mejorar el cumplimiento, al tiempo que optimiza las inversiones de seguridad de los clientes. Esperamos continuar nuestro trabajo con Fortinet para ayudar a nuestros clientes mutuos a acelerar sus objetivos de seguridad en la nube". - Dave Ward, gerente general de Redes y Aplicaciones de AWS. [*]

McAfee hace su pronóstico de amenazas informáticas para el 2023

El 2022 está por terminar y nunca está de más prepararnos para ver que nos deparará el año nuevo en cuanto a estafas digitales y hacer nuestro entorno online más seguro.

Es por eso que el equipo de McAfee Threat Labs ha hecho algunas predicciones sobre el panorama de amenazas informáticas del próximo año y así mantenernos alerta ante estas situaciones.

Este pronóstico prepara el terreno para un 2023 que promete avances no solo en la forma en que interactuamos con la tecnología, sino también en la forma en que ciertos delincuentes pueden explotarla, y perjudicarnos.



A continuación, te presentamos las situaciones a las que debes estar atento para no caer en ellas y mantenerte protegido mientras navegas en línea:

- **Aplicaciones de Inteligencia Artificial:** En los últimos meses, varias aplicaciones de IA se han puesto a disposición del público, ahora cualquiera que tenga un teléfono celular o una computadora puede aprovechar esta tecnología. Esto significa que los avances proporcionaron beneficios a los delincuentes, al permitir una mejor falsificación y una manipulación más realista de las imágenes, datos, etc.
- **Estafas financieras:** El panorama financiero del 2023 será difícil para la mayoría de las personas, esto puede generar vulnerabilidad ante los mensajes de las redes sociales y a los anuncios en línea que ofrecen inversiones y préstamos falsos que pueden llevarlos a perder todo. Tan solo en el primer semestre del 2022, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) recibió 3.5 millones de reclamaciones relacionadas con fraudes financieros, por lo que los usuarios deben estar alerta de las páginas y enlaces que consultan.
- **Criptomonedas:** Este año vimos varias estafas en línea que usaban contenidos existentes para hacer más creíbles las estafas de criptomonedas. Esperamos que esta práctica siga evolucionando en 2023 y que haga uso de videos falsos profundos, así como audio, para engañar a las víctimas para que les entreguen su dinero ganado con esfuerzo.
- **Metaverso:** Los llamados "metaversos" como Horizon de Facebook permiten que usuarios exploren mundos en línea que antes eran inimaginables. Cuando se lanzan estas plataformas y están en una fase inicial, los malhechores suelen intentar explotar la falta de conocimiento de su funcionamiento y aprovecharse para estafar a la gente.
- **ChromeOS:** La capacidad de ChromeOS para ejecutar aplicaciones de Android, combinada con su amplia adopción, crea el clima para que quienes tienen malas intenciones le presten más atención. En 2023 se prevé que los usuarios de Chromebook estén entre los millones de víctimas desprevenidas que descargan y ejecutan contenido peligroso, ya sea de aplicaciones Android maliciosas, de aplicaciones multiplataforma o de extensiones de la Chrome Web Store.
- **Web3:** Los servicios descentralizados de Internet como las NFT, Blockchain y Bitcoin ahora son muy populares, pero a medida que incremente la conciencia sobre este tema, los consumidores comenzarán a explorar estas ofertas de la Web3 sin entender completamente lo que significan o los peligros que deben conocer, dejándoles expuestos a las estafas mientras invierten tiempo y dinero en las cripto o en la creación de sus propias NFTs.

Ahora que se conocen cuáles son algunas de las estafas que estarán rondando durante el 2023, no hay que olvidar mantener las conexiones seguras, no dar clic a enlaces sospechosos y tener una conexión VPN segura. [*]

Dell Technologies presenta su nuevo Dell PowerProtect Data Manager Appliance

Dell Technologies fortalece su portafolio de protección de datos y seguridad multicloud con nuevos sistemas, software y servicios para ayudar a los clientes a proteger su información en instalaciones, nubes públicas y el Edge.

Dell PowerProtect Data Manager Appliance, APEX Data Storage Services Backup Target y Dell PowerProtect Cyber Recovery for Google Cloud son las nuevas ofertas diseñadas con para ser simples y fáciles de utilizar, permitiendo a las organizaciones permite a las organizaciones acelerar su proceso de adopción arquitectura Zero Trust y protegerse en contra de la pérdida de datos, y la amenaza creciente de ataques de tipo ransomware.

Las nuevas soluciones ayudan a abordar los crecientes desafíos de protección de datos a los que se enfrentan las organizaciones. De acuerdo con el Índice Global de Protección de Datos (GDPI) 2022, realizado por Vanson Bourne para Dell, las organizaciones a nivel global han experimentado mayores niveles de desastres naturales y modernos que en años anteriores, lo que ha provocado una mayor pérdida de datos, tiempos de inactividad y costos de recuperación. En el último año, los ciberataques fueron la causa principal de esta interrupción (48%, en comparación con el 37% de 2021). La encuesta reveló que un 85% de las organizaciones globales que utilizan múltiples proveedores de protección de datos ven un beneficio en la reducción de su número de proveedores. Además, reveló que las organizaciones que utilizan un único proveedor de protección de datos gastaron un 34% menos de costos para recuperarse de ciberataques u otros incidentes cibernéticos que quienes utilizaron varios proveedores.

La encuesta del Índice Global de Protección de Datos (GDPI) de Dell en 2022 encontró que el 18% de las organizaciones en América conocen y actúan sobre una arquitectura de Zero Trust - un modelo de ciberseguridad que cambia la forma en que organizaciones abordan la seguridad, pasando de depender únicamente de las defensas perimetrales a una estrategia proactiva que permite únicamente la actividad buena y conocida por medio de ecosistemas y conductos de datos. Sin embargo, un 6% aún no comprende en totalidad los beneficios de la arquitectura Zero Trust, mientras que un 20% está en proceso de evaluación de las implicaciones que esta tecnología puede tener en el negocio; un 19% está comprometido en implementar las prácticas de esta solución; un 27% está aplicando activamente un modelo de Zero Trust y el 18% lo ha implementado completamente. El enfoque holístico de Dell, con funciones de seguridad integradas, diseñadas en el hardware, el firmware y puntos de control de seguridad ayuda a las organizaciones a lograr resultados de Zero Trust para fortalecer la resistencia cibernética y reducir la complejidad de la seguridad.

PROTECCIÓN MODERNA DE DATOS INTEGRADA PARA UNA MAYOR FACILIDAD DE USO

El software mejorado Dell PowerProtect Data Manager admite los principios de

Zero Trust con capacidades de seguridad operativa integradas, como la autenticación multifactor, la autorización dual y controles de acceso basados en roles. El software incluye funciones de supervisión, Inteligencia Artificial y análisis basadas en la nube que permiten a los clientes tomar medidas proactivas y acelerar las resoluciones. La última versión disponible en las instalaciones y a través de AWS, Microsoft Azure y Google Cloud incluye una experiencia de usuario mejorada, que facilita orquestar las capacidades de protección de datos en todo el entorno de copia de seguridad.

Basado en esta arquitectura definida por software, el nuevo Dell PowerProtect Data Manager Appliance ofrece una forma aún más sencilla de implementar el software de protección de datos de Dell. A través de una experiencia de usuario unificada, las organizaciones pueden supervisar fácilmente la integridad de los datos, impulsar el análisis y la elaboración de informes y realizar operaciones de copia de seguridad y restauración de autoservicio para reforzar la resiliencia cibernética. El sistema de debut es ideal para casos de uso pequeños y medianos con un soporte que escala de 12 a 96 terabytes de datos.

DELL AMPLÍA LA CIBER RECUPERACIÓN PARA QUE LAS BÓVEDAS DE LA NUBE PÚBLICA SEAN RÁPIDAS Y FÁCILES DE DESPLEGAR.

PowerProtect Cyber Recovery for Google Cloud permite a los clientes implementar una bóveda cibernética aislada en Google Cloud para proteger y separar datos de forma más segura de un ataque de ransomware. A diferencia de las soluciones de copia de seguridad estándar basadas en la nube, el acceso a las interfaces de administración está bloqueado por los controles de red y puede requerir credenciales de seguridad independientes y autenticación de múltiples factores para el acceso.

Las organizaciones pueden utilizar su suscripción actual a Google Cloud para adquirir PowerProtect Cyber Recovery por medio de Google Cloud Marketplace, y el servicio puede adquirirse directamente con Dell y sus socios de canal.

Esta oferta marca la última expansión de las capacidades de recuperación cibernética de Dell para nubes públicas, tras la introducción este año de Dell PowerProtect para Microsoft Azure y CyberSense para Dell PowerProtect Cyber Recovery para AWS.

DELL APEX SIMPLIFICA EL ALMACENAMIENTO DE COPIAS DE SEGURIDAD CON OPCIÓN DE CONSUMO FLEXIBLE

Los servicios de almacenamiento de datos de Dell APEX se han ampliado para ofrecer una opción de Backup Target para proporcionar un almacenamiento de copias de seguridad seguro en un modelo de consumo flexible y de pago por uso. La oferta de servicio Backup Target es fácil de adoptar para los clientes y agiliza el proceso tanto de compra, implementación y mantenimiento del almacenamiento de backup. Basándose en el liderazgo de Dell en dispositivos de datos y protección de datos, Backup Target reduce el espacio de almacenamiento del cliente y aumenta la disponibilidad de los datos.

La nueva oferta de Dell APEX Backup Target respalda la creciente dependencia de las ofertas as-a-Service para ayudar a superar los desafíos de la protección de datos. Casi todos los encuestados del GDPI 99% a nivel global identificaron al menos una oferta como servicio como una alta prioridad para ayudar a superar los desafíos de protección de datos para su organización. El almacenamiento como servicio 44%, la recuperación cibernética como servicio 41% y la copia de seguridad como servicio 40% fueron las tres principales prioridades de protección de datos como servicio.

DELL AMPLÍA SU PROGRAMA FUTURE-PROOF CON UNA NUEVA GARANTÍA DE CIBER RECUPERACIÓN

Con el aumento de las amenazas cibernéticas y que los datos son cada vez más valiosos, Dell está introduciendo una nueva garantía de recuperación cibernética para proporcionar seguridad a los clientes de que estarán protegidos financieramente por hasta 10 millones de dólares en caso de un ciberataque. El compromiso está diseñado para aumentar la comodidad y confianza de los clientes a la hora de elegir las soluciones de protección de datos de Dell, ya sea para los datos en producción o, de forma más segura, en una ciber bóveda. Esta nueva garantía de ciber recuperación amplía el Programa Future-Proof de Dell Technologies, que ya incluye la Garantía de Deduplicación de Protección de Datos. [*]

ATACAN A USUARIOS CON **400,000 NUEVOS ARCHIVOS** MALICIOSOS DIARIAMENTE: **KASPERSKY**

Durante los últimos 10 meses, los sistemas de detección de Kaspersky descubrieron un promedio de 400,000 nuevos archivos maliciosos diariamente.

En comparación, se detectaron alrededor de 380,000 de estos archivos por día en 2021, lo que representa un incremento anual del 5%. En total, los sistemas de Kaspersky detectaron aproximadamente 122 millones de archivos maliciosos en 2022, seis millones más que el año pasado.

La cantidad de ciertos tipos de amenazas también aumentó: por ejemplo, se descubrió un aumento del 181% en la proporción de ransomware detectado diariamente en comparación con 2021, alcanzando así los 9,500 archivos cifrados por día. Estas y otras conclusiones son parte del Kaspersky Security Bulletin (KSB), una serie anual de predicciones e informes analíticos sobre cambios clave en el mundo de la ciberseguridad.

En cuanto a otras amenazas, las soluciones de seguridad de Kaspersky también detectaron un crecimiento del 142% en la proporción de Downloaders (Descargadores), programas maliciosos que instalan en los dispositivos infectados nuevas versiones de malware o aplicaciones no deseadas. Windows continuó siendo el objetivo principal de los ataques entre todas las plataformas donde se propagaron las familias de amenazas.

En 2022, los expertos de Kaspersky descubrieron un promedio de casi 320,000 archivos maliciosos que atacaban a dispositivos Windows. De todos los archivos maliciosos que se propagaron, el 85% de ellos estaba dirigido a este sistema operativo, sin embargo, no es la única plataforma popular para los atacantes ya que, en este año, también se descubrió que la proporción de archivos maliciosos en formatos de Microsoft Office distribuidos diariamente se duplicó (con un 236% de crecimiento).

En este año, los expertos también identificaron un aumento del 10% en la proporción de archivos maliciosos dirigidos cada día a la plataforma Android. Por tanto, además de los archivos de Windows y Office, los usuarios de Android se han convertido en uno de los objetivos favoritos de los estafadores. Las campañas de Harly y Triada Trojan, que emboscaron a miles de usuarios de Android en todo el mundo, son excelentes ejemplos de esta tendencia.

"Teniendo en cuenta la rapidez con la que el panorama de las amenazas está expandiendo sus límites y la cantidad de nuevos dispositivos que aparecen en la vida diaria de los usuarios, es muy posible que el próximo año no detectemos 400,000 archivos maliciosos por día, isino

medio millón! Aún más peligroso es que, con el desarrollo de Malware-as-a-Service, cualquier estafador novato ahora puede atacar dispositivos sin ningún conocimiento técnico en programación. Convertirse en un ciberdelincuente nunca ha sido tan fácil. Es esencial no solo para las grandes organizaciones, sino también para todos los usuarios comunes emplear soluciones de seguridad en las que pueda confiar, para así evitar ser víctima de los ciberdelincuentes. Los expertos de Kaspersky, por su parte, harán todo lo posible para proteger contra estas amenazas y evitar a los usuarios las pérdidas para que su experiencia diaria en línea sea completamente segura", comenta Vladimir Kuskov, jefe de investigación antimalware de Kaspersky.

Para mantenerse protegido, Kaspersky también recomienda a los usuarios lo siguiente:

- No descargar o instalar aplicaciones de fuentes no confiables.
- No hacer clic en ningún enlace de fuentes desconocidas o anuncios en línea sospechosos.
- Crear contraseñas seguras y únicas, que incluyan una combinación de letras minúsculas y mayúsculas, números y signos de puntuación, además de activar la autenticación bifactorial.
- Mantener las actualizaciones. Algunas de ellas pueden contener correcciones de problemas de seguridad críticos.
- No hacer caso a los mensajes que solicitan desactivar los sistemas de seguridad para la oficina o el software de ciberseguridad.
- Usar una solución de seguridad sólida y adecuada para su tipo de sistema y dispositivos, como son Kaspersky Internet Security o Kaspersky Security Cloud. Le dirán qué sitios no deben estar abiertos y lo protegerán contra el malware.

PARA QUE LAS EMPRESAS SE MANTENGAN SEGURAS, KASPERSKY RECOMIENDA A LAS ORGANIZACIONES:

- Actualizar siempre el software en todos los dispositivos que utilizan para evitar que los atacantes se infiltren en su red aprovechando las vulnerabilidades.
- Establecer contraseñas seguras para acceder a los servicios corporativos. Utilicen la autenticación multifactorial para acceder a servicios a distancia.
- Seleccionar una solución comprobada de seguridad para endpoints, como Kaspersky Endpoint Security para negocios, que está equipada con capacidades de control de anomalías y detección basada en el comportamiento para lograr una protección eficaz contra las amenazas conocidas y desconocidas.
- Utilizar un conjunto dedicado para la protección eficaz de endpoints, la detección de amenazas y los productos de respuesta para detectar y remediar oportunamente incluso amenazas nuevas y evasivas. Kaspersky Optimum Security es el conjunto esencial de protección de endpoints potenciado con EDR y MDR.
- Consultar la información más reciente sobre Threat Intelligence para estar al tanto de los TTPs reales utilizados por los agentes de amenazas. [*]

UTILIZAN **VIPERSOFTX** PARA ROBAR MÁS DE 130 MIL DÓLARES EN **CRIPTOMONEDAS**

Los investigadores de Avast publicaron un análisis a profundidad de ViperSoftX.

Se trata de un ladrón de información utilizado principalmente para robar criptomonedas, el cual suele instalar una extensión del navegador que los investigadores de Avast llamaron VenomSoftX, para obtener acceso completo a los navegadores Chromium. ViperSoftX se propaga principalmente a través de versiones de software crackeadas de Adobe Illustrator, Corel Video Studio y Microsoft Office que se distribuyen habitualmente a través de torrents. Avast ha bloqueado más de 93 mil intentos de infección de ViperSoftX en todo el mundo desde enero de 2022. Los tres principales países en los que Avast hizo bloqueos son India, Estados Unidos e Italia, Avast también protegió a más de mil clientes en México.

"Se estima que los ciberdelincuentes detrás de ViperSoftX robaron más de 130 mil dólares en criptomonedas Bitcoins, Ethereum, Dogecoins, Bitcoin Cach, Cosmos (ATOM), Tezos y Dash", dijo Jan Rubin, investigador de malware en Avast. "Cuando la gente descarga versiones crackeadas de programas, tienen la intención de ahorrar dinero, pero a menudo terminan perdiéndolo. Frecuentemente vemos malware disfrazado de software descifrado, recomendamos a las personas que tengan cuidado con esto y utilicen las versiones oficiales del software. En este caso, en lugar de descargar el software deseado, las personas descargan un archivo ejecutable llamado 'Activator.exe' o 'Patch.exe' y luego de la ejecución, sus computadoras se infectan con el ladrón de información".

CAPACIDADES DE ROBO DE VIPERSOFTX

ViperSoftX puede robar información relacionada con el dispositivo infectado, incluido el nombre de la computadora, el nombre de usuario, detalles sobre el sistema operativo y la arquitectura y si el dispositivo está ejecutando un software antivirus activo. Además, roba criptomonedas almacenadas localmente en el dispositivo infectado en software de criptomonedas y extensiones de navegador y monitorea el portapapeles en busca de direcciones de billeteras de criptomonedas para realizar el cambio de portapapeles.

Asimismo, el ladrón de información registra criptomonedas y otras aplicaciones financieras.

ViperSoftX verifica el contenido del portapapeles para detectar direcciones de billetera. Si encuentra una dirección de billetera, el malware reemplaza el contenido del portapapeles con la dirección del atacante y envía el dinero directamente a la cuenta del ciberdelincuente. Las criptomonedas que roba el ladrón de información incluyen: BTC, BCH, BNB, ETH, XMR, XRP, DOGE y DASH.

Además, el ladrón tiene la funcionalidad de troyano de acceso remoto (RAT) y, por lo tanto, puede ejecutar comandos arbitrarios desde la línea de comandos, descargar cargas útiles adicionales proporcionadas por el servidor C&C y eliminarse del sistema infectado.

CAPACIDADES DE ROBO DE LA EXTENSIÓN DEL NAVEGADOR VENOMSOFTX

VenomSoftX, que ViperSoftX instala de manera silenciosa, brinda a los ciberdelincuentes acceso completo a los navegadores de las víctimas, como Chrome, Edge, Brave y Opera. La extensión maliciosa se disfraza de extensiones de navegador conocidas como Google Sheets y atrae solicitudes de API en algunos de los intercambios de cifrado más populares como Blockchain.com, Binance, Coinbase, Gate.io y Kucoin. Cuando se llama a una API para enviar o retirar criptomonedas, VenomSoftX falsifica la solicitud para redirigir todas las criptomonedas de la cuenta de la víctima a la cuenta del atacante, este método funciona a un nivel más bajo que el intercambio de portapapeles común, por lo que es muy difícil de detectar. También es capaz de robar contraseñas de intercambio de criptomonedas. [*]

CEMPRO

COMUNICACIÓN EN MOVIMIENTO

AGENCIA DE RELACIONES PÚBLICAS

Una buena estrategia de comunicación hará que te olvides de la competencia.

https://www.facebook.com/ComunicacionEnMov