CYBERSECURITY
by itwarelatam.com

Edición - N°17

NOTA DE TAPA

Llegó la inteligencia artificial... ¿y ahora qué sigue?

INFORME ESPECIAL

El rol de la ciberseguridad en el Edge

MÁS TEMAS

NOTA DE TAPA

EDICIÓN N°17

LLEGÓ LA INTELIGENCIA ARTIFICIAL... ¿Y AHORA QUÉ?

04

SUMARIO

Todo lo que nos trae el fin de año

2022 ha sido un año movido en ciberseguridad, pero aún hay cosas que impactan en lo que resta del año, y que tendrán influencia en todo el 2023.

Una de ellas es, sin lugar a dudas, el rol que la Inteligencia Artificial está teniendo en el mundo de la seguridad. Y no sólo desde el lado de las empresas que la utilizan para mejorar y optimizar sus procesos, sino que los cibercriminales también se hacen mano de ella para lograr mejores ataques.

Otro desafío que está en crecimiento es la ampliación del perímetro en las compañías, y cómo esto influye en que puede haber cada vez más brechas y ventanas de oportunidad para que los delincuentes informáticos puedan hacer de las suyas. Como en el caso anterior, un panel de expertos de la industria hablaron con nosotros sobre esta candente temática.

Pero hay más. Relacionado con el último punto, encontrará un interesante informe intitulado "Endpoints, lo que no se ve sí existe", que también habla sobre los desafíos del perímetro.

Asimismo este año que aún transitamos claramente fue reivindicador del rol que tiene el CISO, y cómo este debe seguir evolucionando, así que no se pierdan "2022: la voz del CISO", que también encontrarán en este número.

Por otro lado se requieren cada vez más mejores y más claros informes de seguridad, para que los entiendan y puedan sacarle provecho todas las áreas de una empresa, sea o no tecnológicas, ya que la ciberseguridad debe de ser una responsabilidad de todos.

Sume estrategias en ciberseguridad, los desafíos de las fuerza de trabajo, todo sobre el evento de Ekoparty, y aún tendrá más para seguir leyendo.

¡Disfruten este número, y nos vemos el año que viene!

Matías Perazzo
Director Editorial
mperazzo@mediaware.org

Fernando Juliá
Contenidos
fjulia@mediaware.org

Suscripciones:
info@itwarelatam.com

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

Consultar por suscripción anual

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

Edita, diseña, comercializa y distribuye Mediaware Marketing

CYBERSECURITY by itwarelatam.com
/itwarelatam /ITwareLatam
/ITwareLatam /itwarelatam

LLEGÓ LA INTELIGENCIA ARTIFICIAL... ¿Y AHORA QUÉ?

Por Fernando Juliá

Los ciberataques no sólo han aumentado significativamente, sino que también se han vuelto más sofisticados. Los métodos de seguridad tradicionales no son adecuados para prevenir violaciones de datos en caso de ciberataques.

Los ciberdelincuentes han aprendido a usar nuevas técnicas y herramientas sólidas para piratear, atacar y violar datos. Afortunadamente, las tecnologías de inteligencia artificial (IA) se han introducido en el ciberespacio para construir modelos inteligentes para defender los sistemas de los ataques.

La IA tiene un impacto significativo en la seguridad informática en el mundo. Por un lado, la IA se puede utilizar para construir sistemas defensivos como malware y detección de ataques a la red; por otro lado, la IA podría explotarse para lanzar ataques más efectivos. Los avances en las técnicas criptográficas y de inteligencia artificial (IA) (en particular, el aprendizaje automático y el aprendizaje profundo) se muestran prometedores al permitir que los expertos en seguridad cibernética contrarresten la amenaza en constante evolución que representan los adversarios.

Según un informe de IBM, los principales adoptantes de IA están monitoreando el 95 % de las comunicaciones de la red y reduciendo el tiempo para detectar incidentes en un tercio. También señala que los ejecutivos informan una adopción generalizada de IA para operaciones de seguridad, con un 93 % que ya usa o está considerando implementarla. Y agregan que las empresas de mejor desempeño aumentaron su retorno de la inversión en seguridad (ROSI) en un 40 % o más y redujeron los costos de filtración de datos en al menos un 18 %.

Por su lado, Capgemini asegura que las organizaciones cuentan con la IA para ayudar a los abrumados analistas de ciberseguridad. Casi dos tercios piensan que la IA ayudará a identificar amenazas críticas. El sesenta y nueve por ciento de las organizaciones creen que la IA será necesaria para responder a los ataques cibernéticos. También señalan que tres de cada cuatro ejecutivos dicen que el uso de IA permite que su organización responda más rápido a las infracciones, y que tres de cada cinco empresas dicen que el uso de IA mejora la precisión y la eficiencia de los ciberanalistas.

La inteligencia artificial y su rol en ciberseguridad

"La Inteligencia Artificial (IA) es la combinación de algoritmos planteados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano. En este caso su rol en la ciberseguridad es sumamente importante ya que los ataques cibernéticos evolucionan continuamente a un ritmo cada vez mayor, haciéndose mucho más sofisticados y peligrosos en comparación con algunos años atrás", indica Alejandro Botter, gerente de ingeniería de Check Point para el sur de Latinoamérica.

Botter, de Check Point, suma que las herramientas de seguridad tradicionales utilizan métodos basados en firmas para identificar amenazas, pero este enfoque es defectuoso y puede pasar por alto muchos ataques. Las herramientas de seguridad avanzadas que usan IA/ML (Maching Learning) pueden identificar ataques conocidos y desconocidos, lo que da como resultado tasas de detección cercanas al 100 % y minimiza los falsos positivos. Con AI/ML, no es necesario actualizar las firmas, crear reglas o administrar los esfuerzos de configuración. Sí, puede haber "falsos positivos" ocasionales, pero estudio tras estudio señala que vale la pena evitar la interrupción ocasional causada por un falso positivo para evitar un evento de incumplimiento más impactante.

A su vez, Botter, de Check Point señala un punto importante: "Sumado a esto, la realidad también es que uno de los mayores problemas es que simplemente no hay suficientes profesionales de seguridad para mantenerse al

día con los aumentos de ciberamenazas y todos los problemas relacionados"

Para Arturo Torres, estratega de inteligencia contra amenazas de FortiGuard Labs para Latinoamérica y Caribe, la inteligencia artificial es la tecnología que a través de máquinas o computadoras estudia el comportamiento o patrones de seres vivos o de codificación para después replicarlos, implementarlos e incluso mejorarlos utilizando la información recopilada. El objetivo principal de esta tecnología es procesar una gran cantidad de información para la toma de decisiones utilizando técnicas de predicción o clasificación.

> "Check Point enfrenta el desafío actual de la rápida evolución de amenazas incorporando IA en su arquitectura de seguridad unificada de múltiples capas, proporcionando un sistema inteligente en constante mejora que logra prevenir activamente ataques complejos y sofisticados"

"La IA, especialmente, puede analizar continuamente montañas de datos recopilados de dispositivos en toda la red para identificar amenazas. También puede investigar automáticamente la afluencia de alertas que tradicionalmente han requerido la entrada manual de los equipos de seguridad, lo que les permite tomar decisiones mejor informadas, crear un programa de seguridad más proactivo y eficiente y ser más rentable. Esto libera a los equipos de seguridad para dedicar más tiempo a perfeccionar la estrategia, investigar amenazas avanzadas y cultivar una cultura de conciencia cibernética", agrega Torres, de FortiGuard Labs.

Torres no deja de señalar también que en la ciberseguridad las soluciones impulsadas por AI se han vuelto un componente clave y necesario para las arquitecturas de seguridad ya que, ante la falta de personal con habilidades en este campo, AI ayuda a reducir la carga de trabajo de los equipos de TI, monitoreando, analizando y detectando cualquier actividad anormal dentro de la red, aislándola casi en tiempo real.

"La IA es un poderoso motor para la transformación digital. De acuerdo con el IBM Global AI Adoption Index 2022, casi 7 de cada 10 empresas en la región, aumentó su inversión de IA con la pandemia. Esto evidencia que la IA es un catalizador para acelerar el impacto en el negocio, generar disrupción y desbloquear nuevas oportunidades de mercado", sostiene Pamela Skokanovic, Security Sales Manager, IBM Argentina, Paraguay y Uruguay.

Alejandro Botter
Security Engineering Manager - Región Sur de América Latina de Check Point

Skokanovic, de IBM, indica que a medida que los ciberataques crecen en volumen y complejidad, la IA está ayudando a los analistas de operaciones de seguridad que cuentan con recursos insuficientes a adelantarse a las amenazas. Las tecnologías de IA, como el aprendizaje automático y el procesamiento del lenguaje natural, capturan los insights de inteligencia de

amenazas de millones de artículos de investigación, blogs y noticias, y brindan información rápida a los profesionales de seguridad para eliminar el ruido de las alertas diarias, lo que reduce drásticamente los tiempos de respuesta.

"Además, la IA puede aumentar las habilidades de los analistas de seguridad cuando se trata de

Arturo Torres
Estratega de FortiGuard Labs para América Latina & Caribe

tareas para las no están completamente preparados, lo que les permite hacer su trabajo de manera más rápida, precisa y eficiente", agrega Skokanovic, de IBM.

"La inteligencia artificial debe tener la habilidad de aprenderlo todo por sí misma, de adaptarse y de tomar decisiones en situaciones completamente nuevas con una colección incomprensible de información multiformato. Además, debe ser motivada emocionalmente y tener la habilidad de pasar sus progresos intelectuales a sus descendientes", afirma Fabio Assolini, Director del Equipo de Investigación y Análisis para América Latina de Kaspersky, que agrega que "En ciberseguridad, los robots hacen una gran parte del trabajo ya que encuentran e identifican el malware y lo analizan; luego, crean un "repelente", lo prueban, lo distribuyen, y lo incluyen en la protección global. Todo esto sucede (automáticamente) miles de veces al día. Además, los robots siempre están aprendiendo y la detección está corrigiéndose y mejorando constantemente. Solo una pequeña parte del trabajo requiere de un ser humano experto".

Desde Kyndryl, Ariel Dubra, Cybersecurity&Resilience Practice Architect de la empresa, comparte que la Inteligencia Artificial (IA) tiene un rol y una importancia cada vez más preponderante en la ciberseguridad, algo que se replica, a su vez, con el aprendizaje automático (Machine Learning). Estas tecnologías son capaces de analizar rápidamente grandes conjuntos de datos y rastrear una amplia variedad de amenazas, como ser malware, hasta análisis de comportamientos sospechosos que pueden resultar en un ataque mucho más sofisticado.

Para Dubra, de Kyndryl, las principales funciones que se destacan de la Inteligencia Artificial asociada a la ciberseguridad son: "La Detección, debido a la capacidad que tiene la Inteligencia Artificial para identificar el tráfico irregular a través del aprendizaje automático, la Predicción, dado a que ayuda a predecir diferentes tipos de amenazas analizando los datos y haciendo predicciones basadas en el entrenamiento del sistema y la Respuesta, automatizando la creación de un parche o una solución momentánea virtual, para detener una amenaza detectada o desarrollar nuevos mecanismos

> "En Fortinet, sabemos que la información cambia situaciones y somos ese aliado que ayuda a las empresas a mantener a la gente, dispositivos y datos seguros, brindándoles soluciones amplias, integradas y automatizadas que les ayuden a protegerse mejor"

de protección en tiempo real".

Por su parte, Andrés Mendoza, Regional Technical Manager en Zoho Corp y ManageEngine, dice que LLa ciberseguridad es uno de los muchos usos de la inteligencia artificial, las empresas pueden utilizar la IA para evitar tanto pérdidas financieras como de tiempo. IA ofrece información que permite a las empresas comprender las amenazas fácilmente, lo que reduce los tiempos de respuesta y hace que las empresas cumplan con las mejores prácticas de seguridad".
Mendoza, de ManageEngine suma que, por otro lado, el aprendizaje automático (ML) ayuda a reconocer patrones en los datos para que las máquinas puedan aprender de la experiencia. Entonces, al aprovechar la inteligencia de amenazas cibernéticas, el aprendizaje automático y la inteligencia artificial, las empresas pueden responder a los problemas con rapidez y confianza.

¿Ha llegado la Inteligencia Artificial para quedarse?

Para Botter, de Check Point, se ve una adopción de esta tecnología: "En el 2018, el desarrollo global de la IA en el mercado de la seguridad cibernética alcanzó los 7100 millones de dólares, y se proyecta que alcance casi u$s 30.9 mil millones para 2025. Con una evolución y aumento constante de los ciberataques es imprescindible incorporar nuevas tecnologías para poder estar siempre un paso adelante de los atacantes".
Botter, de Check Point, también apunta que es un segmento de mercado que está llegando a los ejecutivos de nivel C (CISO, CIO, etc.). Una encuesta del Instituto CapGemini de 850 altos ejecutivos de seguridad de la información demostró que el 61% de las empresas ya no pueden detectar intentos de incumplimiento sin tecnología de IA. Otro 48 % afirma que tiene en sus planes aumentar los presupuestos de IA en un promedio del 29%. De ejecutivos encuestados, el 75% dice que actualmente está probando casos de uso de seguridad cibernética de IA.
Torres, de FortiGuard Labs también observa un incremento en la adopción de la inteligencia artificial: "De hecho, todas nuestras soluciones están impulsadas por IA y Machine Learning. Ante un panorama cambiante y creciente de ciber amenazas, y la alta demanda de la industria para contar con profesionales de ciberseguridad, la IA se transforma en un recurso vital para enfrentar estos retos, permitiendo a los equipos de TI enfocarse en tareas que no puedan ser resultas con el uso de esta tecnología, para de este modo proteger mejor a la gente, los dispositivos y los datos".
Torres, de FortiGuard Labs agrega que un claro ejemplo es el cómo podemos inspeccionar una gran cantidad de archivos en busca de contenido malicioso, en donde podemos detectar a una nueva variante de malware en un archivo malicioso y clasificarlo como una campaña de malware conocida a través del uso de esta tecnología, así como predecir el comportamiento de un dispositivo infectado.
"Con IA, las empresas pueden armar rápidamente a los equipos de seguridad con la información, contexto e insights que necesitan para tomar decisiones y minimizar el impacto en la experiencia del usuario", suma Skokanovic, de IBM Argentina, "Por ejemplo, de acuerdo con el estudio Cost of Data Breach Report 2022, las organizaciones que desplegaron completamente la automatización y la IA en seguridad incurrieron en un costo promedio menor en filtraciones de datos, y lograron un ahorro de 65.2% frente a las que no, lo cual significó el mayor ahorro de costos observado en el informe. Además, su tiempo de detección y contención es

menor: 2.5 meses más rápido". Desde Kaspersky, Assolini aporta otra mirada y comparte que, en el mercado de la ciberseguridad, se presentan nuevos y "revolucionarios" productos, como por arte de magia, a través de la inteligencia artificial pueden resolver todos los problemas de seguridad y proteger a todos y a todo de cualquier amenaza de un solo golpe: Mientras tanto, en realidad, dentro de estos productos revolucionarios no hay "tecnología reciente". Hay tecnología que data de la época de ¡la máquina de vapor!

"Lo que sí existe es el aprendizaje automático. Y las tecnologías de aprendizaje automático se usan bastante desde hace tiempo. Por ejemplo, en ciberseguridad, los robots hacen una gran parte del trabajo. La burbuja de la IA le quita credibilidad al aprendizaje automático, uno de los subcampos de la ciberseguridad más prometedores", agrega Assolini, de Kaspersky.

"Hemos notado un aumento significativo en la adopción de soluciones de ciberseguridad basadas en Inteligencia Artificial", adiciona Dubra, de Kyndryl, "La tecnología de IA nos permite tener una amplia variedad de casos de uso, tanto sea en ciberseguridad, como en la automatización de procesos de negocio para mejorar el rendimiento de las empresas en el día a día. Si bien sabemos que aún falta bastante para lograr un nivel de madurez en la adopción de estas tecnologías, vamos por un buen camino para los próximos años".

Mendoza, de ManageEngine, argumenta que la pandemia ayudó a que las organizaciones prioricen diferentes proyectos e iniciativas de reforzar la seguridad, ya que muchos procesos o servicios debieron ser expuestos para soportar el trabajo remoto o híbrido. "En ese sentido, varias organizaciones empezaron a implementar herramientas de SIEM o de gestión de privilegios y que éstas ya incluyen funcionalidades soportadas por IA y ML como es el caso de UEBA (User and Entity Behaviour Analytics) que permite identificar comportamientos anómalos y alertar a los administradores de esas desviaciones de actividades en su infraestructura".

El desafío de los CISO

"Sabemos que el mayor problema al que se enfrentan los CISOs es que el personal de seguridad suele estar sobrecargado de trabajo y con la carga de realizar un seguimiento de las amenazas de seguridad diarias. Aún más alarmante, un estudio mostró que el 30% de los equipos de seguridad ignora o no alcanza a investigar la mayoría de las advertencias que reciben. Estas ideas pintan un panorama aterrador", denota Botter, de Check Point.

Botter también explica que los procesos AI/ML pueden automatizar el análisis de incidentes etiquetando automáticamente cada amenaza como "Alta", "Media" o "Baja", y pueden crear un ticket, reunir y analizar los datos apropiados de todas las diversas herramientas. A partir de ahí, el personal de seguridad puede tomar decisiones inmediatas sobre los tickets precargados que merecen la máxima prioridad y actualizar las reglas del firewall de forma rápida y automática. Si bien AI/ML no reemplazará al CISO, también puede desempeñar un papel importante en la automatización de otros procesos, como el análisis de tráfico de red, el análisis de amenazas de correo electrónico y la prevención de amenazas, la protección de endpoints, el código fuente y el análisis del comportamiento del usuario, y la protección del servidor de aplicaciones o bases de datos. Al aplicar inteligencia artificial y aprendizaje automático, el equipo de seguridad puede mejorar la eficiencia y reducir el riesgo.

A su vez, Torres, de FortiGuard

Labs, formula que a medida que los ciberdelincuentes investigan y llevan a cabo métodos automatizados para crear, probar y diseminar malware y otras amenazas, los CISOs y sus equipos, y las soluciones de seguridad heredadas que tienen, pueden verse abrumados por el gran volumen de incidentes y alertas que requieren correlación e investigación. Es imposible defenderse contra ataques automatizados mejorados con dispositivos de seguridad aislados, la correlación manual de datos entre soluciones en silos y respuestas manuales.

> “IBM no es sólo un fabricante de tecnología. Estamos en la primera línea y trasladamos todo ese conocimiento a las soluciones y servicios de seguridad. Hoy más que nunca, las empresas necesitan cambiar el paradigma”

Torres, de FortiGuard Labs también señala que “Tareas como estas en el panorama actual de amenazas han obligado a las organizaciones a adoptar un enfoque en gran medida reactivo de la seguridad porque los equipos de TI luchan por validar y tapar los agujeros de seguridad mientras mantienen las operaciones en funcionamiento. En un esfuerzo por seguir el ritmo de las nuevas amenazas y una huella de red en rápida expansión, los equipos de seguridad cibernética a menudo implementan productos puntuales inconexos. Esto ha aumentado la complejidad de la seguridad, especialmente cuando la información debe coordinarse en una arquitectura de seguridad desagregada. Como resultado, muchos equipos de seguridad se están quedando atrás a medida que sus propias redes se vuelven cada vez más complejas, la cantidad de bordes que deben protegerse continúa expandiéndose y el panorama de amenazas cibernéticas se acelera”.

Para Skokanovic, de IBM Argentina, ”A medida que los ciberataques crecen tanto en volumen como en sofisticación, las herramientas necesarias para combatirlos también se complejizan y encontrar a personas con las habilidades adecuadas resulta en un desafío para los líderes. La demanda de talento de seguridad se ha disparado en los últimos años, pero la oferta no se mantiene al ritmo de la demanda. De acuerdo con un estudio del 2019 de IBM Resilient & Ponemon, el 75% de los encuestados está enfrentando una dificultad en la contratación y retención de personal especializado en ciberseguridad”.

Skokanovic agrega que frente a esta situación es fundamental que se de atención y prioridad a la formación de talento para cerrar la brecha de habilidades. Es esencial invertir en soporte y capacitación para el personal de operaciones de TI, así como para garantizar que los equipos de defensa tengan un conocimiento adecuado. A la par de la formación de las personas, otro factor a tener en cuenta es salir de los procesos de selección tradicionales. Distintas personas pueden tener el tipo adecuado de habilidades, aptitudes y la

Pamela Skokanovic
IBM Argentina
Security Sales Manager

experiencia amplia y necesaria para ocupar diversos roles clave en el ecosistema de seguridad, así no tengan un título de cuatro años.

Dubra, de Kyndryl, explica que "el crecimiento de la Inteligencia Artificial muchas veces lo vemos como un arma de doble filo para los CISOs, ya que las compañías se enfrentan a una cantidad enorme de ciberataques automatizados, que

Fabio Assolini
Director del Equipo de Investigación y Análisis de Kaspersky

aumentan exponencialmente en velocidad, variedad y complejidad. Sin embargo, es esa misma tecnología la que está colaborando con los equipos de ciberseguridad en la detección y respuesta a amenazas, cambiando fundamentalmente los paradigmas de defensa de las organizaciones".

Pero Dubra, de Kyndryl, sostiene que, a la hora de considerar adquirir una solución de ciberseguridad, su recomendación es realizar algunas preguntas iniciales para comprender la profundidad de la solución y cómo aplica el modelo de Inteligencia Artificial que ayudará a la organización. A modo de ejemplos, menciona los siguientes interrogantes: ¿Se pueden obtener métricas de rendimiento?, ¿Podríamos obtener una demostración práctica donde se evidencie la mejor solución ante una situación de un ataque?, ¿Quién posee los datos y metadatos que estará procesando la solución? Esto último pensando en el tipo de tratamiento y las diferentes normativas o leyes vigentes dependiendo el país.

A su vez Mendoza, de ManageEngine adiciona que la mayoría de los administradores u organizaciones asume que implementar IA es realizar el despliegue de un chatbot de auto-servicio, que es una sola de las varias aplicaciones que tenemos en el mercado, y ese concepto es erróneo. "Por el lado de la ciberseguridad, no es necesario desarrollar o armar algoritmos desde cero para aprovechar las ventajas que esta tecnología nos brinda. Es por eso que nos atrevemos a decir que los desafíos en cuanto a despliegue o implementación son mínimos, lo importante es tener la aceptación de la dirección y top management para invertir en ciberseguridad como un pilar base de todas sus operaciones y arrancar con los proyectos".

> "La inteligencia artificial debe tener la habilidad de aprenderlo todo por sí misma, de adaptarse y de tomar decisiones en situaciones completamente nuevas con una colección incomprensible de información multiformato. Además, debe ser motivada emocionalmente y tener la habilidad de pasar sus progresos intelectuales a sus descendientes"

Cómo enfrentar este desafío y qué deberían hacer las empresas

"Sin duda los cibercriminales también evolucionan en sus ataques e incorporan la IA para hacerlos más sofisticados. Es una competencia sin fin. Lo importante es intentar estar siempre un paso adelante para prevenir

posibles amenazas. El ciclo de seguridad de una empresa debe basarse en 4 etapas: predecir, prevenir, detectar y responder. Al integrar IA en este ciclo los tiempos de respuesta se acortan y mejora la seguridad", señala Botter, de Check Point.

Torres, de FortiGuard Labs comenta que los CISOs ahora se encuentran en constante búsqueda de nuevas herramientas para agregar a su arsenal, a menudo solo para descubrir que los ciberdelincuentes han desarrollado una forma aún más avanzada de atacar y eludir los controles de seguridad existentes. "Los enfoques y soluciones de seguridad tradicionales deben complementarse con modelos alternativos, como IA y automatización. Estas ventajas permiten les permiten no solo mitigar el riesgo provocado por los ataques cibernéticos automatizados con tiempos de respuesta más rápidos, visibilidad más amplia y administración de red simplificada, sino también adelantarse a sus adversarios cibernéticos", comenta, y agrega que al aprovechar las soluciones que incorporan IA y automatización, los CISOs pueden abordar de manera proactiva los ataques cibernéticos automatizados de hoy y mantenerse un paso por delante de los ciberdelincuentes.

Asimismo, Torres, de FortiGuard Labs, menciona que la asistencia de ciberseguridad automatizada no es una propuesta de todo o nada, se pueden ir agregando nuevas capacidades poco a poco, empezado por ejemplo creando escenarios "que pasaría si", utilizando herramientas como SEIM o SOAR, y después agregar capacidades más sofisticadas. "Otro aspecto clave es incorporar expertos a nuestro equipo con experiencia en AI, o en su defecto capacitarlos, esto ayudará además a mantenerlos motivados ya que puede venir acompañado de una prospección de crecimiento dentro de su plan de carrera, lo que se traduce en retención de talento que como hemos comentado ya, es hoy más importante que nunca".

Y Torres, de FortiGuard Labs no deja de sumar que "por último tomar en cuenta cada espacio de la superficie de ataque, enfocando en soluciones de punto de acceso y sandboxing, para poder preparar a nuestras arquitecturas ante cualquier intento de ataque".

"Como parte la transformación constante del mundo del cibercrimen, diariamente hay vectores de ataque nuevos y en expansión, los atacantes están cambiando a amenazas adaptables y de múltiples variantes, y demás, están implementando IA y Automatización para impulsar sus ataques. Los profesionales de ciberseguridad deben mantenerse actualizados y aprovechar estas tecnologías para tener información al día sobre las amenazas cada vez más sofisticadas que surgen y evolucionan a diario. Además, los apoyarán en la detección de actividades maliciosas y frenar a los ciberdelincuentes de forma más rápida", señala Skokanovic, de IBM Argentina.

Skokanovic también menciona que esto ayuda a tener un plan de seguridad estratégico robusto con un enfoque de seguridad evolucionado basado en la Confianza Cero, es decir, operar bajo el supuesto de que una identidad autenticada, o la propia red, ya están comprometidas y, por lo tanto, valida todo continuamente. Este enfoque requiere que las empresas unifiquen sus datos de seguridad para abarcar en forma envolvente el contexto de seguridad alrededor de cada usuario, dispositivo e interacción. Para esta unificación y acción constante, la tecnología de IA es una herramienta clave a la hora de automatizar procesos y recabar datos pertinentes para garantizar la toma de decisiones informada.

Finalmente, Skokanovic com-

parte que “Es clave que las empresas definan un plan de seguridad estratégico, robusto, capaz de reflejarse en la arquitectura general, como tecnologías y herramientas, profesionales involucrados, procesos y modelos de gobernanza. La IA es una aliada para abordar diferentes desafíos. Sin embargo, las organizaciones y proveedores que emplean la IA tienen la responsabilidad fundamental de construir sistemas confiables y garantizar que la tecnología se diseña y utiliza de forma responsable, en todas las instancias del ciclo de vida de la IA. Para IBM, tecnologías poderosas como IA deben ser transparentes, explicables y mitigar prejuicios dañinos e inapropiados”.
“Si bien se está volviendo evidente que la Inteligencia Artificial en ciberseguridad será completamente necesaria, la implementación de la tecnología también puede convertirse en un nuevo vector de ataque. Esto se produce debido a que los ciberdelincuentes aprenden, construyen y lanzan sus propios esquemas de contraataque de Inteligencia Artificial como respuesta. De hecho, los actores malintencionados utilizarán sus propias creaciones de software de IA para intentar infiltrarse en nuestros datos más valiosos”, comparte Dubra, de Kyndryl.

Ahora, ¿esto significa que vamos a dejar de innovar o renunciar a la lucha constante contra la ciberdelincuencia?, se pregunta Dubra, de Kyndryl, que responde que la respuesta es un rotundo no, ya que siempre habrá una oportunidad de ser más astutos que las entidades que buscan dañarnos para su propio beneficio, y para eso es importante mantenerse actualizados sobre las últimas amenazas, para poder estar prevenidos, además de innovar en soluciones y herramientas, entre las cuales la IA tiene un rol preponderante, para poder utilizarlas a nuestro favor.

Dubra, de Kyndryl, a su vez señala que es importante destacar que una empresa necesita integrar todas las herramientas para asegurar la existencia de estructuras capaces de protegerse desde una perspectiva de negocio. En este contexto, es crucial asegurar la resiliencia, es decir, la capacidad de las empresas y sus sistemas para seguir operando, incluso en caso de ataque, definitivamente deben considerar la Inteligencia Artificial dentro de la estrategia de la compañía, porque su adopción es clave para estar un paso delante de las potenciales amenazas, pero no hay una formula específica para seguir a la hora de implementar el mejor modelo como un estándar general.
“Entonces, siempre se deben considerar tres factores. En primer lugar, “los objetivos y los riesgos”, aceptando riesgos que son tanto conocidos como desconocidos, porque la IA ofrece un poderoso potencial para obtener información predictiva. También debemos comprender “el elemento humano”, ya que la IA complementa el esfuerzo de los equipos al ayudar a los analistas a reducir errores, acelerar el análisis y automatizar tareas que requieren mucha mano de obra. Y, por último, es importante “centrarse en los casos de uso” que necesita la compañía, para que las organizaciones se esfuercen en implementar dichos casos, basados en Inteligencia Artificial, como primer paso en cualquier iniciativa de adopción de IA más amplia”, concluye Dubra, de Kyndryl.

– Kyndryl: “La IA permite establecer potentes colaboraciones entre profesionales y tecnología que amplían nuestros conocimientos, enriquecen nuestras vidas e impulsan la ciberseguridad de una forma que parece ser mayor que la suma de sus partes”
“Así como la tecnología y estas nuevas funcionalidades pueden

aprovecharse para defenderse de los ataques y nuevos métodos de intrusión, los mismos atacantes están buscando alternativas para que esa misma tecnología pueda usarse para crear malware más robusto, capaz de burlar controles estáticos o reglas manuales de firewall, IDS, IPS, entre otros. Es por eso, que es mandatorio contar con la IA/ML para defendernos y mantenernos a la vanguardia de la seguridad", explica Mendoza, de ManageEngine.

> "La IA permite establecer potentes colaboraciones entre profesionales y tecnología que amplían nuestros conocimientos, enriquecen nuestras vidas e impulsan la ciberseguridad de una forma que parece ser mayor que la suma de sus partes"

Por otro lado Mendoza, de ManageEngine, aporta que "Antes de implementar tecnología nueva es muy importante empezar por entender lo que tenemos y hacemos, con ese relevamiento se puede priorizar dónde esté la información sensible y qué estamos haciendo para protegerla, entender quién, cómo, desde dónde consume dicha información o accesos para claramente definir el nuevo perímetro de lo que está permitido y con esa base empezar a restringir o activar alarmas y notificaciones de lo que esta fuera de ese rango, incluso lograr remediación automática si es posible. En ese momento podemos elegir entre herramientas de SIEM, SOAR, PAM, UBA, UEBA o incluso armar una estrategia basada en Zero Trust para reforzar la seguridad y tener control de todo lo que ocurre en la red".

El aporte de los proveedores de soluciones

Check Point

Desde Check Point Software estamos continuamente desarrollando y optimizando las protecciones para reconocer y prevenir las nuevas formas de ataques.
Check Point utiliza varios modelos de IA para mejorar la predicción de ataques, que están integrados en todos los productos:
- Harmony (protección para usuarios y acceso)
- Quantum (protección para Red)
- CloudGuard (protección para infraestructura en la nube)
- Horizon (gestión unificada y operaciones de seguridad)
- ThreatCloud (inteligencia de amenazas)

Por ejemplo, Behavioral Guard es uno de los motores de predicción de Harmony Endpoint y aprovecha Harmony Endpoint Forensics para identificar de manera efectiva y única el comportamiento de malware nuevo y desconocido y permitir una clasificación precisa de las familias de malware. El motor combina firmas de comportamiento creadas por investigadores de Check Point con un modelo de IA que analiza patrones de comportamiento para detectar e identificar malware. Esta combinación única de firmas genéricas y validación del modelo

Ariel Dubra
Cybersecurity&Resilience Practice Architect - Kyndryl

de IA permite la activación de firmas que no se pudieron activar anteriormente debido a las altas tasas de falsos positivos. Al incorporar la validación de IA, la tecnología de Check Point ignora el 99 % de los comportamientos sospechosos y previene con precisión sólo los ataques genuinos.

Hace muy poco lanzamos nuestro nuevo producto Check Point

Andrés Mendoza
Regional Technical Manager
ManageEngine

Quantum Titan, una nueva versión de la plataforma de ciberseguridad Check Point Quantum. El lanzamiento de Quantum Titan presenta tres nuevos módulos de software que aprovechan la inteligencia artificial (IA) y el Deep Learning para ofrecer una prevención avanzada de amenazas contra explotaciones avanzadas del sistema de nombres de dominio (DNS) y phishing, así como seguridad IoT autónoma. Check Point Quantum Titan es ahora una de las únicas plataformas de la industria que puede proporcionar detección de dispositivos IoT y aplicar automáticamente perfiles de prevención de amenazas de Zero Trust para proteger los dispositivos IoT.

FortiGuard Labs

Retomando un poco las primeras preguntas, AI se ha convertido en la clave para poder combatir el esquema cambiante y creciente de ciber amenazas, y por ende las soluciones impulsadas por IA son parte ya del ADN de nuestros productos. Esto a través de estos pilares:

IA en FortiGuard Labs: Durante una década, nuest ros investigadores de amenazas globales han estado aplicando el aprendizaje automático, las redes neuronales artificiales y otros análisis avanzados para generar inteligencia global frente a amenazas que potencie nuestros productos de prevención de amenazas

IA implementada en línea: Fortinet utiliza aprendizaje automático en particular, construido directamente dentro de nuestros Firewalls de Siguiente Generación, Web Application Firewall, Network Detection & Response (NDR) y plataforma de protección de endpoint (EPP) para brindar una prevención basada en el comportamiento como complemento de las técnicas tradicionales.

IA para detección de amenazas avanzadas: En combinación con sensores distribuidos con análisis centralizado de Big Data,

> “Antes de implementar tecnología nueva es muy importante empezar por entender lo que tenemos y hacemos, con ese relevamiento se puede priorizar dónde está la información sensible y qué estamos haciendo para protegerla”

Fortinet permite que las organizaciones apliquen aprendizaje automático, redes neuronales artificiales y otros análisis con el fin de detectar las ciber amenazas de las que son objeto.

IA para acelerar la respuesta: Para garantizar una respuesta oportuna a las amenazas, a pesar de una abundancia de productos de seguridad y

escasez de profesionales de ciberseguridad, Fortinet ofrece un panel único de visibilidad, análisis y automatización a lo largo de Security Fabric, entornos de múltiples proveedores y procesos de seguridad bien definidos.

IBM

IBM no es sólo un fabricante de tecnología. Estamos en la primera línea y trasladamos todo ese conocimiento a las soluciones y servicios de seguridad. Hoy más que nunca, las empresas necesitan cambiar el paradigma y fortalecer su sistema inmunológico digital. La esperanza, no es una estrategia de seguridad. Lo único que uno puede controlar es la preparación y fallar en la preparación, es prepararse para fallar en un mundo donde todo es digital.

Es clave que las empresas implementen un enfoque transversal y holístico de seguridad, bajo una visión híbrida, abierta y colaborativa. De esa manera, van a aumentar su ciberresiliencia, haciendo frente a los diferentes tipos de ciberamenazas. Es fundamental que entiendan que tener una seguridad exitosa es un trabajo constante, una estrategia en curso. Es un compromiso con la organización, sus empleados, clientes, socios y un verdadero cambio cultural.

Por otra parte, IBM está haciendo varias cosas para promover la colaboración de la industria de la seguridad con el fin de combatir esta nueva era de ciberdelito. Por ejemplo, para acelerar la colaboración, se lanzó la Open Cybersecurity Alliance (OCA) en 2019, una iniciativa de seguridad de código abierto encabezada por IBM y McAfee, a la que recientemente han ingresado otros 16 actores importantes entre los que se encuentran VMware, F5, entre otras. El objetivo de OCA es hacer que la tecnología de seguridad sea más interoperable entre las categorías de productos y los proveedores, mediante los estándares abiertos.

Kaspersky

A diferencia de las empresas emergentes, nosotros protegemos a los usuarios con una gigantesca infraestructura en la nube, la cual es capaz de resolver rápida y efectivamente tareas mucho más complejas. Y sí, es por ello que utilizamos tantos modelos diferentes de aprendizaje automático.

Kyndryl

La ciberseguridad es un tema complejo por sí mismo, pero la Inteligencia Artificial puede ser una poderosa herramienta para ayudar a protegerse de los ataques. La IA permite establecer potentes colaboraciones entre profesionales y tecnología que amplían nuestros conocimientos, enriquecen nuestras vidas e impulsan la ciberseguridad de una forma que parece ser mayor que la suma de sus partes.

Con tecnología y análisis de última generación, los servicios de respuesta y operaciones de ciberseguridad de Kyndryl están diseñados para ayudar a las organizaciones a detectar, clasificar, investigar y responder con confianza a amenazas de seguridad avanzadas. Nuestra solución integral de administración de amenazas integra pruebas ofensivas, servicios de seguridad administrados, Inteligencia Artificial y respuesta a incidentes para un enfoque integral de la administración de amenazas.

ManageEngine

Desde ManageEngine contamos con varias herramientas que pueden ser identificadas en esta página especial relacionada a la ciberseguridad: https://www.manageengine.com/latam/soluciones-de-ciberseguridad-ti.html además de una guía que permite a los administradores conocer los principales desafíos y cómo podemos ayudarlos a tener visibilidad, control y remediación.

Inteligencia Artificial y Machine Learning: una respuesta óptima frente a los nuevos retos en seguridad

Alain Karioty

Por Alain Karioty, Vicepresidente para Latam de Netskope

La rápida adopción de servicios en la nube como SaaS/IaaS/PaaS en la empresa ha suscitado una importante migración de los datos, desde los confines de los centros de datos corporativos a los localizados en la nube, los cuales, además, escapan al control empresarial. Esta evolución, unida al crecimiento del trabajo remoto e híbrido y a la imparable digitalización obliga a una transformación de la seguridad, desde las tradicionales pilas de dispositivos de seguridad ubicados en las instalaciones hasta la seguridad entregada desde la nube.

Security Service Edge (servicio de seguridad en el borde o SSE), término acuñado por Gartner, representa una nueva plataforma donde los servicios de seguridad, como la puerta de enlace de seguridad web, el agente de seguridad de acceso a la nube, el acceso a la red basado en confianza cero o el firewall, se entregan desde la nube para permitir a los usuarios realizar su trabajo de forma segura y reducir el riesgo de verse comprometidos o pierdan sus datos.

Entre las características de SSE destaca el acceso a los datos basado en confianza cero, ya que estas soluciones aplican políticas de seguridad fundamentadas en el contexto, cuya información se convierte en el distintivo virtual que permite, deniega o recomienda el acceso de un usuario a los activos digitales corporativos; y la detección de amenazas internas y externas, para garantizar que los usuarios internos no filtren datos sensibles de forma inadvertida o maliciosa, y las empresas cuenten con una capa de defensa añadida para proteger sus datos frente a amenazas del exterior.

El papel de la IA/ML en las soluciones SSE

El rol fundamental de la IA y ML en ciberseguridad es de suma importancia, no solo para simplificar procesos y para el cumplimiento de regulaciones y privacidad, sino también para la detección de actividades de manera más precisa, lo que mejora la fiabilidad y veracidad, aspectos vitales en industrias con recursos limitados. Una solución SSE eficaz debe tener la capacidad de extraer información contextual muy rica al procesar el tráfico de red y aplicar las políticas de confianza cero en el acceso a los datos. Para tomar la decisión de acceder a los datos se tienen en cuenta tanto la sensibilidad que presentan los que salen de la empresa como los indicadores de amenaza que presentan los que proceden del exterior. Y en estas dos áreas, la inteligencia artificial (IA) y el aprendizaje automático (ML) han demostrado ser excelentes para brindar la oportunidad de pasar rápidamente de la identificación y la respuesta manual, a la mitigación automatizada.

Así, y frente a las soluciones tradi-

cionales de seguridad de datos que utilizan una combinación de expresiones regulares, palabras clave y diccionarios para identificar los datos sensibles, la clasificación de datos basada en el aprendizaje automático reduce los errores y el exceso de falsos positivos, al ofrecer decisiones de clasificación de alta veracidad. Dichas decisiones se apoyan también en algoritmos de procesamiento de lenguaje natural (NLP), muy adecuados para resolver este problema.

Netskope ha desarrollado modelos de NLP para clasificar documentos comunes para el negocio como formularios de impuestos, nóminas, contratos comerciales, o acuerdos de confidencialidad. Al utilizar estos modelos preconfigurados, los administradores de seguridad no necesitan recurrir a expresiones regulares u a otros patrones dificultosos o que lleven a error a la hora de identificar aquellos documentos con información sensible a proteger.

Las imágenes son otro elemento a proteger. De hecho, en Netskope Security Cloud, el 20% de los documentos que se escanean son imágenes, como archivos JPG y PNG. Aunque hasta ahora la forma más habitual de clasificarlas ha sido a través de un motor de reconocimiento óptico de caracteres (OCR), la ineficacia demostrada por este tipo de soluciones con las imágenes actuales exige un cambio. La clasificación de imágenes mediante el aprendizaje automático proporciona una forma rápida y eficaz de identificación y ayuda a las empresas a proteger aquellas que contienen datos personales. Las empresas pueden cumplir así con las regulaciones sobre privacidad (CCPA, RGPD/GDPR, LGPD, etc.)

Detección de amenazas

Las amenazas internas, perpetradas por empleados malintencionados o descontentos que roban datos y los comparten en el exterior, siguen siendo uno de los mayores problemas a los que se enfrentan las empresas. Netskope Intelligent SSE mantiene un registro de todas las actividades de los usuarios y aplica algoritmos de IA/ML para detectar comportamientos anómalos. Además, la solución realiza una puntuación de riesgo para cada usuario, que posteriormente se introduce en las políticas de confianza cero de acceso a los datos. Así, por ejemplo, un usuario con una mala puntuación se le podrá negar el acceso a datos sensibles.

Una forma muy común de detectar amenazas como el malware y el ransomware es mediante el uso de firmas de vulnerabilidades y exploits. Los indicadores de compromiso, como los hashes defectuosos de archivos y las URL maliciosas, son también otras técnicas utilizadas para detectar amenazas. Sin embargo, cuando se trata de vulnerabilidades desconocidas o amenazas de día cero, hace falta algo más. Netskope ha desarrollado con éxito modelos de IA/ML para detectar amenazas en archivos ejecutables (denominados archivos PE), así como en formatos de documentos comunes como PDF y documentos de Microsoft Office. En Netskope Next Gen Secure Web Gateway (gateway de seguridad web de nueva generación o NGSWG), los modelos de IA/ML se utilizan para clasificar las URLs, así como el contenido web perteneciente a los sitios de phishing que tienden a robar las credenciales de los usuarios. La IA/ML también se utiliza para clasificar los sitios web y bloquear contenido inapropiado para los usuarios de la empresa.

Sin duda, los algoritmos de IA/ML pueden ayudar a resolver una variedad de problemas que se ven comúnmente en las empresas. Sin embargo, y cuando se trata de soluciones SSE, hay que tener en cuenta que estos algoritmos de IA/ML tienen que estar optimizados para ejecutarse y devolver una decisión en tiempo real para ser eficaces. Con el tiempo, va a haber muchos más casos de uso desafiantes donde la IA/ML puede ser utilizada para resolverlos de manera efectiva.

Netskope, seguirá a la vanguardia tecnológica abordando presentes y futuros desafíos y ayudar a las organizaciones a resolver cualquier problema de seguridad en la nube.

emBlue

Hacemos que la **omnicanalidad sea simple**

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

EL ROL DE LA CIBERSEGURIDAD EN EL EDGE

Por Fernando Juliá

Un entorno de TI de borde, como los que se encuentran en las fábricas industriales, puede tener una gran cantidad de puntos finales distribuidos que proporcionan una gran superficie de ataque para los ciberdelincuentes y los piratas informáticos.

La gestión de este riesgo requiere la implementación adecuada de la segmentación de la red y varios dispositivos de seguridad. Edge Computing implica conectar dispositivos y sistemas de punto final a una red.

Estas conexiones ofrecen posibles vías de ataque para los piratas informáticos. Mitigar estos riesgos de ciberseguridad requiere soluciones que abarquen las mejores prácticas de seguridad para dispositivos, redes y aplicaciones. Esto también requiere acciones por parte del usuario para mantener su nivel requerido de ciberseguridad.

Los incidentes de ciberataques contra las redes de TI se han ido intensificando a nivel mundial. Esto, combinado con la creciente adopción de dispositivos IoT, la convergencia de las redes de TI y OT (tecnología de operaciones), y el uso de sistemas analíticos y de administración basados en la nube, ha llevado a que la ciberseguridad sea una preocupación urgente para los propietarios y operadores de TI perimetrales. Los riesgos de ataques cibernéticos están empeorando debido a la naturaleza cada vez más distribuida de TI.

La tendencia de la computación perimetral está colocando cada vez más dispositivos terminales en la periferia de las redes informáticas, lejos de los centros de datos centralizados y más seguros. Esto ha aumentado drásticamente la superficie de ataque disponible para los ciberdelincuentes y los piratas informáticos.

Por dónde vienen los ataques

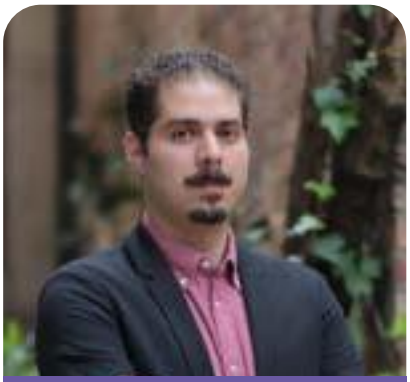
"Mientras mayor sea la cantidad de dispositivos finales (endpoints) se amplía la superficie de ataque, porque estos dispositivos necesitan conectarse a diferentes redes y aplicaciones, haciendo difícil la segmentación necesaria para evitar que los atacantes aprovechen esas conexiones. Entonces la naturaleza distribuida de estos ambientes Edge, aumenta también el riesgo de vectores de ataque comunes como: malware, vulnerabilidades sin parchar, credenciales comprometidas, phishing a los administradores o configuraciones débiles en los dispositivos", expone Francisco Lugo, Ingeniero de Soluciones LATAM para BeyondTrust.

Lugo, de BeyondTrust agrega que "Incluso dispositivos muy simples como UPS (Uninterruptible Power Supply), cámaras de seguridad, sensores ambientales y otros, al requerir conectarse al Edge o a Internet, constituyen potencialmente un eslabón débil en aspectos de seguridad. Un atacante podría obtener acceso no autorizado a alguno de estos dispositivos, y si la segregación de la red no es la adecuada, le permitirá explorar otras redes y moverse lateralmente".

Por su lado, Vladimir Villa, CEO de Fluid Attacks, sostiene que "Edge computing y la producción de dispositivos IoT avanzan de manera cada vez más acelerada, aumentando la cantidad de sistemas que guardan y manejan datos y, consecuentemente, la superficie de ataque. Por eso, el riesgo de sufrir fuga de datos y ataques de denegación de servicio es más alto. El punto de entrada de un ciberdelincuente puede ser u n sistema con configuraciones no apropiadas, un mecanismo de autenticación inseguro o controles de acceso inapropiados, y a partir de este primer acceso, o al explotar componentes vulnerables del software, puede llegar a comprometer otros dispositivos conectados a la red, datos y la disponibilidad de servicios. En Fluid Attacks, el 75% de

los sistemas que evaluamos este año utilizaban componentes de software vulnerables y, además, entre los cinco problemas más riesgosos para la infraestructura encontramos la configuración inapropiada de servicios y mecanismos de autenticación inseguros".

"Entre los vectores que generan mayor falta de seguridad en Edge Computing hay dos que se destacan y están



Francisco Lugo
Ingeniero de Soluciones LATAM para BeyondTrust

relacionados con la falta de criptografía y la autenticación", comenta Luiza Dias, Directora Presidente de GlobalSign Brasil, que agrega "En el primer caso se trata de los datos enviados sin cifrar en las redes compartidas o abiertas, lo que genera vulnerabilidad en la información enviada. Por otra parte, los dispositivos que no tienen autenticación robusta en sus puertas físicas y virtuales abiertas debido a descuidos en sus diseños, lo que también representa un riesgo de violación".

Según Germán Patiño, Vicepresidente de Ventas para Latinoamérica en Lumu Technologies, el trabajo remoto amplía la superficie de ataque ya que los dispositivos corporativos se conectan a diferentes tipos de redes. "Esto dificulta que las organizaciones puedan tener visibilidad de activos comprometidos. El incremento de dispositivos IoT en la red. Ya que usualmente no es fácil instalar soluciones de antivirus en estos dispositivos, y esto hace que sean altamente vulnerables", comenta Patiño, de Lumu, que sostiene que la mayor capacidad de procesamiento en la red hace que los atacantes quieran sacar ventaja para infectar los activos con malware dedicado a criptominería.

Al ser una arquitectura distribuida, Edge Computing se enfrenta a nuevos riesgos tanto físicos como lógicos. Sobre los primeros hay que reseñar que, en un escenario centralizado, el control del acceso físico a los servidores se ofrecía por las capacidades de las políticas de acceso al centro de datos principal, mientras que ahora se debe tener ese control en cada sucursal asegurando que solo el personal autorizado tenga acceso físico, indica Hugo Riveros, Solutions Engineering Manager de Netskope LATAM.

"En lo que respecta al punto de vista lógico, podemos ci-

> "Un ambiente Edge puede tener una variedad muy amplia de dispositivos finales, aumentando y haciendo más compleja la superficie de ataque. Controlar los flujos de tráfico de red y administrar las sesiones privilegiadas en redes industriales, es también administrar la seguridad de sensores y otros dispositivos"

tar dos riesgos principales: la exposición directa a Internet o a la red WAN, y el acceso no autorizado a los recursos de Edge Computing mediante diferentes interfaces posibles", agrega Riveros de Netskope, y suma que "Al encontrarse en un ambiente distribuido, ya no

toma ventaja de la protección de los elementos centrales de seguridad, como IPS, IDS, Firewall entre otros. Por lo anterior, es de vital importancia que el acceso a la intranet, extranet o Internet esté protegido desde la misma oficina remota con una solución igualmente distribuida con funcionalidades de seguridad y de separación

Vladimir Villa
CEO de Fluid Attacks

de instancias para topologías específicas en la WAN. En este frente, tiene vital importancia soluciones de WAN inteligentes conocidas como SD-WAN (Software defined WAN)".

Riverso, de Netskope, no deja de puntualizar que, por otro lado, existen diferentes interfaces para brindar acceso, por ejemplo, a ethernet, WIFI, BLE, WIFI y 4G, entre otras. Es importante tener control de las interfaces de acceso disponibles y además garantizar que los dispositivos o usuarios que deben tener acceso únicamente son los autorizados. Para esto es de suma importancia contar con soluciones de microsegmentación y de análisis del comportamiento del usuario, de tal forma que, por ejemplo, un sensor de temperatura que usa Edge Computing, solo acceda al recurso indicado y no pueda acceder a otros sistemas, como el servidor de videovigilancia.

"Tanto el acceso físico como lógico no autorizado siempre son cuestiones relevantes para considerar. Por un lado, los dispositivos de procesamiento perimetrales deberían seguir principios de seguridad al igual que lo hacen los sistemas alojados en la Nube o en Data Centers tradicionales. Por ejemplo, es muy relevante el principio de seguridad que propone el "Zero Trust", en el que cada pedido de acceso a un equipo o a cargas de procesamiento pasa por un escrutinio granular que asegura el acceso solo a identidades o procesos autorizados", sostiene Diego Taich, socio de PwC Argentina de la práctica de consultoría en ciberseguridad & IT.

Taich, de PwC Argentina, agrega que en el caso del "Edge Computing", dado que la capacidad de procesamiento puede estar contenida en hardware o dispositivos ubicados en zonas al aire libre, de tránsito intenso de personas o alejadas de los sistemas de monitoreo visual, se debe considerar al

> "En una época en que las organizaciones y sus clientes necesitan disponer de sus datos en la nube en mayor cantidad y de manera más rápida, deben hacerse pruebas de seguridad continuas de la infraestructura que los soporta, para así evitar que estos sean comprometidos a causa de ciberataques"

acceso físico como un riesgo relevante.

En el caso de SonicWall, Edilson Cantadore, Director, Solutions Engineering LATAM de la empresa, comparte que el primer punto a entender en la implicación de usar Edge Computing es la expansión del perímetro de seguridad. A medida que acercamos los

recursos informáticos a los usuarios, es decir, los sacamos de los perímetros de control tradicionales, ya sea en una nube privada, híbrida o en un Data Center convencional, ampliamos intensamente nuestros puntos de exposición que, por supuesto, necesitan seguridad al igual que otros recursos alojados en silos de infraestructura de TI tradicionales.
"A la hora de decidir acercar los recursos informáticos y,

> "Es necesario contar con seguridad para los dispositivos más cercanos"

en consecuencia, los datos al usuario, se multiplican los puntos de exposición a los más variados vectores de ataque y explotación de vulnerabilidades. Aumenta en gran medida la exposición de los datos recopilados, manipulados y almacenados localmente, y también se debe evaluar seriamente la preocupación por la fuga de información (DLP)", agrega Cantadore, de SonicWall.

Javier Bernardo, Head of Strikers de Strike, suma que hoy en día volvemos a tener una creciente necesidad de que el procesamiento de datos esté ubicado cerca de los usuarios en dispositivos del tipo "Edge Computing" principalmente para reducir la latencia y acelerar el análisis de los datos, sensores, etc. Esto significa que los datos se procesan y almacenan cada vez más en dispositivos IoT o equipos industriales en ubicaciones remotas geográficamente distribuidos cerca del usuario.
"Los modelos convencionales de ciberseguridad no son adecuados para esta redistribución. A medida que la tecnología vuelve a avanzar hacia el borde <Edge>, estos modelos corren el riesgo de exponer los activos de datos corporativos y retrasar la transformación digital. Las arquitecturas clásicas normalmente se benefician de los enfoques de 'defense in depth', donde los controles de seguridad de varias capas protegen los datos ocultos en el back-end", agrega Bernardo, de Strike.
Bernardo, de Strike, señala a su vez que los vectores comunes de amenazas a la ciberseguridad para la infraestructura crítica incluyen organizaciones criminales y ataques sponsoreados por estados, supply chain attacks, sistemas de control obsoletos (el firmware de un dispositivo de Edge computing es fundamental para su seguridad) la manipulación del firmware podría permitir que un atacante utilice un dispositivo para transmitir datos "falsos o corruptos" a los sistemas de control. Otros

Luiza Dias
Directora Presidente de GlobalSign Brasil

vectores son la falta de segmentación de redes y tecnología operativa, dependencias de soluciones "Air Gapped", vulnerabilidades sin parches, explotación de servicios no utilizados, ransomware, falta de alertas, logins inadecuados, falta de topologías de red y amenazas internas.
Adiciona su opinión el Chief de estrategia de seguridad en

Tenable, Nathan Wenzler, que comenta que la propia naturaleza de las arquitecturas de Edge Computing hace que los tipos de sistemas y dispositivos utilizados sean increíblemente susceptibles a sufrir ciberataques. El hecho de acercar la potencia de procesamiento y los datos a los usuarios finales para aumentar la velocidad y reducir la latencia creó una situación en la que los dispositivos eficientes, construidos específicamente, se convierten en puntos de acceso.

"Centrarse más en la eficiencia significa que hay menos opciones sólidas para construir controles y configuraciones de seguridad fuertes en esos dispositivos para protegerlos de la explotación. Y es debido a la falta de opciones de seguridad sólidas en ellos que estos dispositivos son más susceptibles a las técnicas de ataques más comunes, dando un punto de acceso fácil para realizar un mayor número de ataques contra el resto del entorno", sostiene Wenzler, de Tenable.
Asimismo, Claudio Muñoz-Vivas, TELECOM DC POWER & OSP, Sales Application Engineer Team Leader en Vertiv, dice que algunos de los vectores más frecuentes son: versiones de firmware obsoletas en dispositivos de TI con vulnerabilidades de seguridad conocidas, tecnología heredada que no cumple con los protocolos de seguridad y estándares de encriptación modernos, certificados de seguridad autofirmados o caducados en dispositivos de gestión; usuarios con privilegios de acceso excesivos que los ciberdelincuentes podrían explotar; falta de visibilidad de las actividades de los usuarios que podrían afectar negativamente a la infraestructura de IT, falta de actualización de listas de usuarios y/o administradores que mantienen acceso y poca o ninguna gestión de configuración estandarizada.

Qué medidas básicas debe de tomar una empresa

"Al igual que en otros ambientes, es muy importante cumplir con mejores prácticas de seguridad informática como tener un programa de mitigación de vulnerabilidades, aplicar medidas típicas como controles de tráfico de red, anti-malware, accesos administrativos, segregación de privilegios, y finalmente disponer de un equipo de profesionales para monitoreo y respuesta a incidentes", sostiene Lugo, de BeyondTrust.
Lugo, de BeyondTrust explica que en ambientes de Edge Computing se destacan dos requerimientos de seguridad: buscar que los dispositivos finales soporten protocolos de comunicación segura (por ejemplo, mediante TLS - Transport Layer Security), y dispositivos que permitan control de acceso basado en roles. Esto no siempre es factible, pero es preferible porque disminuye los riesgos de un atacante tomando el control remoto de estos dispositivos, y aumenta las propiedades de confiabilidad y disponibilidad, que son tan relevantes en estos ambientes.
Villa, de Fluid Attacks, opina que un primer paso para las empresas que desarrollan tecnología es definir que se sigan requisitos de seguridad del desarrollo del software para así ofrecer sistemas e infraestructura seguros para sus usuarios. En edge computing, esto significa, entre otras cosas, asegurar que los servicios se mantengan disponibles y que los sistemas tengan mecanismos de protección contra modificaciones y accesos no autorizados, permitiendo salvaguardar la información confidencial.
"La política de la organización debe considerar educar sobre la responsabilidad compartida de la seguridad en la nube,

hacer pruebas integrales de seguridad del software continuamente, remediar las vulnerabilidades que se detecten, divulgar los hallazgos y las mejoras realizadas, entre otros procesos. Además, un apoyo para legitimar los procesos, políticas y responsabilidades es que las organizaciones hagan de la ciberseguridad un tema a tratar en la agenda de la junta directiva", agrega Villa, de Fluid Attacks.

> "Mayor capacidad de procesamiento en la red y una superficie de ataque más amplia representa un atractivo perfecto para los adversarios"

"Cuando se considera una política activa de seguridad para Edge Computing es necesario pensar desde la concepción del dispositivo. Se debe considerar que una vez instalado, es muy difícil intervenir un dispositivo. Por ese motivo, al momento de diseñarlo, de proyectarlo, ya se esté pensando en la seguridad que requerirá. A partir de esta planeación se evita uno de los principales inconvenientes que afronta la industria, que es la dificultad al momento de implementar seguridad en un dispositivo ya producido", comparte Dias, de GlobalSign Brasil.

Dias, de GlobalSign agrega que cuando se desarrolla IoT se debe considerar que la intervención manual suele ser costosa o difícil una vez que se ha implementado un dispositivo en el campo. Por ese motivo se debe tener en cuenta la caducidad de un certificado, ya que de fallar generaría fallas también en el dispositivo. De allí que los mecanismos de renovación deben ser sólidos.

Sobre esto, Patiño, de Lumu Technologies, manifiesta que "En el pasado, las estrategias de seguridad se diseñaban sobre la idea de que los atacantes estaban fuera de la red. Una estrategia moderna de ciberseguridad, que esté a la altura de los desafíos que plantea el Edge Computing, se construye sobre la hipótesis de que ya la red está comprometida y se debe probar lo contrario".

Por su parte, Riveros, de Netskope, asevera que, para tener una política activa de seguridad, se deben tener en cuenta una serie de medidas transcendentales. Así pues, antes de adquirir una solución de Edge Computing es importante validar sus capacidades de seguridad y las buenas prácticas para realizar el endurecimiento del equipo, teniendo en cuenta las recomendaciones de firmware, protección de interfaces y de su almacenamiento local.

"También, es recomendable

Germán Patiño
Vicepresidente de Ventas para Latinoamérica, Lumu Technologies

garantizar la disponibilidad de mecanismos de seguridad física para acceso al equipo; seguir las recomendaciones del fabricante, creando una política de actualización periódica de software, con su debido proceso de gestión de cambios; y asegurar las comunicaciones, usando protocolos de red como TLS, desde y hacia

el dispositivo", explica Riveros, de Netskope, que agrega que "Por último, es esencial que, a nivel de red, únicamente los dispositivos asignados tengan acceso al servidor, mientras que, en una sucursal remota, además de contar con funcionalidades de seguridad en la conexión hacia Internet y la WAN, idealmente con soluciones SDWAN (Software defined WAN) y SSE (Secure service Edge)".

Hugo Riveros
Solutions Engineering Manager de Netskope LATAM

"Una de las cuestiones fundamentales es entender cómo las nuevas arquitecturas híbridas, que incluyen Data Centers tradicionales, Edge Computing, Cloud, y personas y dispositivos IoT interactuando, son acompañadas por niveles de seguridad acordes. Como primer paso, contar con un entendimiento integral de los riesgos asociados al Edge Computing es importante para poder establecer medidas de seguridad apropiadas", adiciona Diego Taich, de PwC Argentina.

Por su lado, Cantadore, de SonicWall, remarca que, en primer lugar, evalúe la madurez de los usuarios y los sistemas alojados de forma remota, e identifique posibles fallos sistémicos. Edge Computing implica procesar datos lo más cerca posible del origen de esos datos y, por lo tanto, las preocupaciones de seguridad también deben trasladarse a este "edge".

"En segundo lugar, estimar los riesgos e implicaciones de estas vulnerabilidades y qué pasos y tecnologías se necesitan para garantizar una operación segura y, luego, modelar las herramientas de protección y comunicación para que sean viables desde el punto de vista del negocio. La visión de seguridad en silos ya no es fácilmente modelada en este escenario donde el "edge" se mueve junto con los usuarios y/o sistemas involucrados", adiciona Cantadore, de SonicWall.

En el caso de Strike, Bernardo enumera cuatro mejores prácticas para abordar la ciberseguridad en Edge Computing de forma coherente y reducir drásticamente el riesgo de incidentes:

1. Criterios de selección de dispositivos: Seleccionar dispositivos que se pueda verificar que hayan sido desarrollados por proveedores que siguen un proceso de ciclo de vida de desarrollo seguro (SDL) bien implementado. O, si hablamos de dispositivos ICS, se debe seguir el estándar IEC 62443.
2. Diseño de red segura: No solo debe elegir dispositivos de red desarrollados y optimizados para la seguridad y la privacidad de los datos, sino que la red misma, por supuesto, también debe diseñarse, implementarse y administrarse con la seguridad como principal preocupación, con conceptos básicos como el uso de una red privada virtual (VPN) que emplea túneles encriptados, implementa firewalls y usa sistemas de control de acceso.

> "En una estrategia Multicloud, son los clientes los responsables de mantener una postura integral de seguridad"

Más allá de esas herramientas, la red debe implementarse utilizando un esquema de "defensa en profundidad" (Defense in Depth). Otra práctica recomendada es el uso de dispositivos de sistema de detección de intrusos (IDS).
3. Instalación/configuración del dispositivo: Antes de usar un dispositivo de Edge computing, se debe realizar un análisis adecuado para comprender cómo se comunica y cómo se comporta el dispositivo en el caso de uso que el cliente necesita operar. Esto implica usar y aplicar un hardening provisto por el proveedor, realizar escaneos de puertos y garantizar que se apliquen todas las actualizaciones y parches de firmware, entre otras cosas.
4. Operación y mantenimiento: Si bien existen aplicaciones específicas pueden tener tácticas únicas y específicas para garantizar la seguridad, existen ciertas prácticas que se aplican a todas las aplicaciones de Edge computing. Entre ellos se incluyen la gestión de parches, análisis de vulnerabilidades y las pruebas de penetración. Y finalmente, también es importante considerar la seguridad física como parte de la estrategia general de ciberseguridad.

> "Los dispositivos conectados a Internet están cambiando los paradigmas de computación, y por ende la ciberseguridad debe seguir evolucionando y acompañando las nuevas arquitecturas de redes y procesamiento, incluyendo la protección de los dispositivos de Edge Computing y el IoT en su paraguas"

Wenzler, de Tenable, asevera que no hay una única respuesta correcta a esta pregunta. "El Edge Computing es un concepto de arquitectura, y puede ser implementado de muchas maneras diferentes, utilizando muchos tipos diferentes de tecnologías y dispositivos como puntos de acceso", dice.
"Sin embargo, tener una comprensión completa de estos puntos en su entorno de Edge Computing es el primer paso crítico para determinar cuáles serán los mejores controles de seguridad para su organización. Sin visibilidad, terminará con puntos ciegos de dispositivos fácilmente comprometedores, lo que dará a los atacantes una gran ventaja para entrar en su entorno sin ser notados. Por lo tanto, se debe comenzar con tener visibilidad y luego debe decidir qué medidas serán las mejores para mitigar el riesgo que presenta su entorno de Edge Computing", agrega Wenzler, de Tenable.

Diego Taich
Socio de PwC Argentina de la práctica de consultoría en ciberseguridad & IT

Asimismo, Muñoz-Vivas, de Vertiv, indica que cuando se trata de establecer estándares de seguridad, los líderes de TI deben garantizar el uso de los últimos protocolos de seguridad y algoritmos de cifrado mientras aplican perfiles de seguridad estrictos para bloquear el acceso a su solución OOB.

"Abordar las vulnerabilidades de seguridad conocidas también significa garantizar que los dispositivos de IT se actualicen con el firmware más reciente, que se cambien todas las credenciales predeterminadas en los sistemas de IT y que solo se utilicen los certificados firmados por las autoridades. Todos los certificados deben rotarse con frecuencia", suma Muñoz-Vivas, de Vertiv.

Las mejores prácticas para implementar ciberseguridad en el Edge

"La serie de estándares ISA/IEC 62443 (International Society of Automation/International Electrotechnical Commission) presenta los requerimientos que deben cumplir las partes involucradas en estos sistemas de automatización, para aumentar la integridad, confiabilidad y seguridad de los sistemas de control industriales, incluyendo Edge Computing", sostiene Lugo, de BeyondTrust, que agrega "Entre las principales, están la administración activa y el mantenimiento correcto de los dispositivos que consumirán los servicios del Edge, e implementar un diseño seguro de la red, que permita crecer pero que esté correctamente segmentado".

Para Villa, de Fluid Attacks, las compañías que desarrollan tecnología deben pensar en la seguridad de su software, para lo cual recomiendan realizar pruebas de seguridad continuas desde el comienzo del ciclo de vida del desarrollo. Estas deben combinar el uso de herramientas automáticas, que escanean el software en búsqueda vulnerabilidades, y pruebas manuales por expertos, ya que estos últimos pueden encontrar las fallas más complejas, como lo son la configuración inapropiada de los servicios de la nube y de controles de acceso, mecanismos inseguros de autenticación y secretos en el código, entre otras.

"Además, las vulnerabilidades detectadas deben ser remediadas tan pronto como sea posible, priorizando aquellas que representen el mayor riesgo para la disponibilidad de los sistemas y la integridad de los datos. En Fluid Attacks, descubrimos que quienes monitorean y evitan desplegar versiones inseguras de su software toman 30% menos tiempo en su remediación", comparte Villa, de Fluid Attacks.

"Entre las mejores prácticas a considerar en ciberseguridad se destaca el análisis de riesgo a cada paso. Es decir, en el proceso completo del dispositivo, desde la concepción y desarrollo de un dispositivo hasta su implementación", asevera Dias, de GlobalSign Brasil.

En el caso de Lumu Technologies, Patiño afirma que las organizaciones deberían asegurarse de que sus proveedores, terceros y cadena de suministro no representen un riesgo para la seguridad de su red. Adicionalmente, todas organizaciones que incluyan soluciones tipo SaaS para su operación deberían asegurarse de que dichas soluciones cuenten con certificaciones tipo SOC2, Privacy Shield, entre otras que evidencien las buenas prácticas sobre las que están construidas y soportadas.

"Entre las recomendaciones para mantener una estrategia de ciberseguridad acertada pasan, implantar el control de acceso y la vigilancia para mejorar la seguridad física en el borde, controlar la configuración y el funcionamiento del borde desde las operaciones centrales de TI (Secure Access Service Edge SASE) y establecer procedimientos de auditoría para controlar los cambios de alojamiento de datos y aplicaciones en el borde",

agrega desde su conocimiento Riveros, de Netskope.

Asimismo, hay que aplicar el mayor nivel de seguridad de red posible entre los dispositivos/usuarios y las instalaciones de borde. (Descubrimiento de dispositivos, perfilamiento, análisis de comportamiento, granularidad del contexto y microsegmentación) así como supervisar y registrar toda la

> “Libérese con la ciberseguridad sin límites de sonicwall, cuando las amenazas son ilimitadas, sus defensas deben ser ilimitadas”

actividad del borde, en particular la relacionada con las operaciones y la configuración, agrega Riveros, de Netskope.
Entre las mejores prácticas que Diego Taich, de PwC Argentina enumera, se encuentran:
1- Zero Trust: las arquitecturas basadas en este deben ser consideradas para asegurar datos, servicios, y activos de la red en general.
2- Protección de los endpoints: agregar capacidades de análisis de comportamiento y aprendizaje de máquina para poder detectar amenazas como las que hoy plantean los ransomware.
3- Monitoreo activo 7x24 de eventos de seguridad: con el objetivo de poder identificar y detener un ataque en sus fases más tempranas, y que no llegue a convertirse en un incidente severo.
4- Identificación periódica de vulnerabilidades; para poder remediar rápidamente aquellas cuestiones que pueden ser explotadas por los ciber atacantes.
5- Seguridad Física, por ejemplo, en los equipos de borde que procesen datos provenientes de dispositivos IoT, se deberían considerar medidas de seguridad en el acceso y el monitoreo.
Desde SonicWall, Cantadore define cómo sería una práctica eficiente de ciberseguridad en Edge:
1- Almacenamiento y movimiento de datos: identificar lo relevante para ser tratado y transmitido, reduciendo el volumen de datos a proteger ya sea en almacenamiento local o en transmisión y compartición con otros sistemas corporativos centralizados.
2- Desafíos en la configuración de plataformas de seguridad distribuidas y dispositivos/usuarios de red: asegurar que las políticas de seguridad aplicadas a los diferentes sistemas sean consistentes y actualizadas de forma centralizada, evitando posibles errores de configuración que se reflejen en la exposición innecesaria e indeseada de las plataformas y los datos involucrados. Estos

Edilson Cantadore
Director, Solutions Engineering, LATAM, SonicWall

mismos criterios de configuración y control de las plataformas de seguridad deben extenderse a los sistemas y dispositivos protegidos, identificando y mitigando las posibles fallas que estos puedan ofrecer si están mal configurados y conectados a las redes de servicio.
3- Selección cuidadosa de

dispositivos: Edge Computing implica también un uso intensivo de IoT. La selección de dispositivos desarrollados por fabricantes que siguen estándares seguros en el ciclo de desarrollo de sus productos es relevante para la adopción de plataformas menos vulnerables a ataques.

4- Diseño de red adecuado

Javier Bernardo
Head of Strikers de Strike

que segrega los dispositivos según su uso y exposición: las redes segmentadas y correctamente diseñadas reducen el riesgo de propagación de amenazas cuando logran superar las barreras de seguridad implementadas, reduciendo así los impactos negativos a enfrentar cuando potencialmente se presenten-

5- Mantenimiento y monitoreo: es relevante la necesidad de un monitoreo permanente de las plataformas, sistemas y dispositivos implementados, buscando consistencia y efectividad en las políticas de protección estipuladas. La volatilidad inherente de los sistemas modernos implica un monitoreo permanente para garantizar que cualquier falla se detecte de manera efectiva y se corrija de manera oportuna.

"Empezar por la visibilidad. Tener una comprensión completa del entorno de Edge Computing es el único primer paso real que se debe dar para luego construir un mejor programa de ciberseguridad. A partir de ahí, determina lo que los dispositivos y puntos finales que estás utilizando son capaces de hacer en términos de controles de seguridad y comienza a aplicar cualquier medida para protegerlos", sostiene Wenzler, de Tenable.

Wenzler, de Tenable agrega que esto puede consistir en centrarse en la seguridad de los datos o en los límites de la segregación de la red, si se trata de dispositivos informáticos ligeros como los dispositivos IoT de tipo comercial. O bien, podría significar la creación de configuraciones de endurecimiento estándar y su aplicación en todos los dispositivos para bloquear el posible acceso o uso externo.

Las mejores prácticas que utilizamos en nuestros entornos en la nube y en las instalaciones no son diferentes para los entornos de Edge Computing, pero estas prácticas pueden ser más difíciles de implementar debido a la naturaleza limitada de los puntos finales involucrados.

> "La naturaleza altamente distribuida de las soluciones de Edge computing y tecnologías IT híbridas hace que sea más difícil protegerlas de los ciberdelincuentes. Cualquiera que sea el enfoque que adopten las organizaciones deben considerar a la seguridad desde el comienzo de sus implementaciones"

Por su lado, Muñoz-Vivas, de Vertiv, señala que Algunas buenas prácticas son: configuración de la red que pueda reforzar el control de los sistemas de IT mediante la

creación de una red de administración fuera de banda (OOB) que esté separada de la red de producción y luego bloquear el acceso directo a la red a los dispositivos OOB. También hacer cumplir el uso de software de administración central como punto de entrada único a la red OOB es ideal para mejorar la seguridad y el control. Más allá del software, los líderes de IT deben asegurarse de que los siguientes activos de hardware sean parte de una estrategia de administración remota: procesadores de servicio, infraestructura virtual, dispositivos de red y almacenamiento, unidades de distribución de energía en rack (rPDU), unidades de fuente de alimentación ininterrumpida (UPS) o cualquier dispositivo IP direccionable.

Los desafíos en una era multi-cloud y la IoT

"Es importante mencionar la diferencia entre IoT (Internet of Things) y el IIoT (Industrial Internet of Things). Los dispositivos IIoT requieren mayor nivel de seguridad y tolerancia a fallos, compatibilidad con muchas otras tecnologías, mayor precisión en tiempos de respuesta, y otras características que los hacen más especializados que los típicos IoT's de consumidores finales, como televisores o cámaras inteligentes. Un ejemplo de IIoT puede ser un interruptor eléctrico, capaz de ser habilitado o deshabilitado por software", indica Lugo, de BeyondTrust.

Lugo, de BeyondTrust, agrega que un desafío muy importante es el aumento de la complejidad de la arquitectura, porque especialmente en redes industriales es necesario mantener la resiliencia y disponibilidad de los servicios, y con el aumento en la cantidad de dispositivos es más difícil decidir cómo asegurarse de que accedan únicamente los sujetos requeridos por la organización, y también se hace más difícil monitorear para encontrar accesos no autorizados. Esto, sumado al aumento de la convergencia entre redes IT y OT, en muchos casos requerida para Edge Computing, hace aún más difícil proteger estos dispositivos que comúnmente ejecutan software inseguro.

Para Villa, de Fluid Attacks, el mayor riesgo que representan el entorno multi nube y la IoT es la fuga de datos. Este tipo de incidentes es propiciado por vulnerabilidades en el software o en su cadena de suministro. En el primer caso, principalmente, la seguridad de los datos personales y de marca depende especialmente de la autenticación.

"Si una aplicación tiene problemas con el mecanismo de autenticación, entonces todos los demás controles están comprometidos. Otras vulnerabilidades que los hackers éticos encuentran frecuentemente son credenciales guardadas en el código fuente o el que las aplicaciones generen tokens que tienen una vida útil muy prolongada, propiciando el robo de sesión. En cuanto a los ataques a las cadenas de suministro, se encuentra como factor facilitador el uso de dependencias y software de terceros con vulnerabilidades conocidas en la tecnología. Por lo anterior, el desafío de ciberseguridad se encuentra en el desarrollo del software", indica Villa, de Fluid Attacks.

"Al iniciar un ecosistema IoT pueden generarse obstáculos en el manejo de las identidades, principalmente cuando están basadas en certificados. En ese momento, surgen problemas cuando las credenciales se pueden exportar desde el dispositivo para habilitar suplantación de identidad, sostiene Dias, de GlobalSign Brasil. según Dias, de GlobalSign Brasil, otro desafío importante está dado por la diferencia en

los protocolos que utilizan los fabricantes. Se debe resaltar que el ciclo de vida de los dispositivos es más largo que el de una computadora, por lo que requieren muchas más actualizaciones de firmware, procesamiento, almacenamiento, ancho de banda limitado y consumo de energía. Lo que requiere un esfuerzo adicional al momento de aprovechar la vida útil de los dispositivos.

El crecimiento en escala de los dispositivos también presenta un desafío para la seguridad. Con el desarrollo de nuevas tecnologías como 5G, IoT puede vivir una explosión en cantidad de dispositivos, lo que representa miles de millones de puertas de entradas para nuevos ataques.

Sobre el tema, Patiño, de Lumu Technologies, comparte que "Los desafíos consisten principalmente en asegurar la visibilidad de amenazas y compromisos en la red. Es de vital importancia que las organizaciones puedan medir de forma continua e intencional la existencia de contactos entre sus dispositivos y la infraestructura de los adversarios. De esta forma pueden anticiparse con precisión y eficacia ante los ataques de forma temprana".

Riveros, de Netskope, propone otro escenario: "Adoptar una estrategia Multi-cloud no significa que la seguridad pueda ser delegada en los proveedores de nube, quienes obviamente disponen de controles y herramientas de seguridad. Al contrario, son los clientes quienes deben responsabilizarse de mantener una estrategia integral de protección que no abarque la seguridad en la nube, sino la arquitectura Multicloud completa (usuarios remotos, acceso a las aplicaciones, protección de datos, amenazas, etc.)"

En el caso de IoT, además de la protección del acceso a la información local, también se debe considerar que, en muchas ocasiones, los dispositivos IoT acceden a aplicaciones basadas en nube en contextos y proveedores de nube diferentes comparte Riveros, de Netskope, que agrega que No obstante, si hablamos de desafíos, podemos citar de manera concreta el riesgo derivado de la existencia de múltiples plataformas en la nube, las cuales suponen una superficie de ataque más amplia con nuevas vulnerabilidades, que requieren nuevas herramientas para mantener la seguridad y el cumplimiento en entornos de nubes.

Riveros, no deja de señalar que en lo que respecta a gobernanza de los datos y cumplimiento de la normativa, no hay que pasar por alto el hecho de que trasladar las aplicaciones a la nube no excluye de la necesidad de cumplir ciertos requisitos de gobernanza de datos. Asimismo, dice que es imprescindible mantener políticas de seguridad uniformes y consistentes en varias nubes, y que es necesario saber qué está conectado a mi red y cómo se comporta. "Como la seguridad debe ser un esfuerzo constante, es necesario realizar un monitoreo permanente del comportamiento del dispositivo, de tal forma que, si se presenta una conducta anómala, se puedan tomar las acciones pertinentes", enfatiza Riveros, de Netskope.

Taich, de PwC Argentina señala entre los desafíos de seguridad:

- Diseño no seguro: la mayoría de los dispositivos IoT no ha sido diseñado considerando principios de seguridad, por lo tanto, uno de los desafíos es que las próximas generaciones de dispositivos contemplen aspectos básicos de autenticación, autorización y registro de eventos de seguridad.
- Gestión de identidades: la gestión de las identidades de los usuarios y procesos a los que acceden recursos de

las distintas Nubes son clave para reconocer si estamos o no ante la misma identidad en cada pedido de acceso a un recurso, y qué permisos se le deben conceder.
- Estandarización de la gestión de seguridad de la nube: la falta de estandarización de los entornos Cloud lleva al despliegue de múltiples soluciones de seguridad que se solapan en distintos puntos, así también como a distintos procesos de gestión, y a la necesidad de contar con conocimientos muy variados.
- Confidencialidad: la protección de la confidencialidad de los datos es un verdadero desafío, considerando que la Nube es utilizada muchas veces como plataforma para el aprendizaje de máquina en procesos que incorporan IA, y que se suelen utilizar sets de datos muy grandes que pueden contener información sensible y que no se encuentra protegida de forma adecuada.

> “Los dispositivos Edge Computing pueden no parecer un objetivo valioso, porque tienen pocos datos almacenados en ellos, pero son puntos de entrada clave en el resto de tu red, especialmente porque son muy fáciles de comprometer. No asumas que los ciberatacantes no están interesados en estos dispositivos. Al contrario, son objetivos ideales para poner un pie en la puerta y lanzar ataques más devastadores contra el resto del entorno”

Desde SonicWall, Cantadore comparte que el reto es entender y asimilar el modelo de responsabilidad compartida inherente al entorno de la nube, qué tipo de servicio en la nube se contrata y, de esta manera, atender los aspectos de seguridad que se demandan de acuerdo con su responsabilidad directa. Y señala que para la parte en la cual el usuario es responsable de administrar, es necesario utilizar algunas estrategias:
- Cifrado: garantizar que los datos almacenados estén protegidos y que el transporte de datos también se realice a través de canales cifrados.
- Asegúrese de que los dispositivos de acceso se manejen correctamente (parches, protecciones de punto final), que los IoT sean dispositivos seguros de origen conocido y que cumplan con los requisitos de seguridad predefinidos.
- Controle a los usuarios a medida que los necesite con un enfoque ZTNA; controle cada conexión remota, considerando siempre el contexto de la demanda, y ponga a disposición solo lo que el usuario necesita y cuando lo necesita.

Nathan Wenzler
Chief de estrategia de seguridad en Tenable

“La transmisión de datos entre dispositivos IoT y la nube, y entre ellos, también plantea riesgos de seguridad. Las topologías de Edge Computing pueden combinar múltiples estándares de red, incluidos protocolos de red específicos de IoT como NB-IoT y Sigfox, así como tecnologías más con-

vencionales como WiFi o 4G. La capacidad informática limitada de algunos dispositivos IoT se suma a los desafíos de proteger dichas redes", propone Bernardo, de Strike.
Bernardo comenta aparte que los sistemas de IDS/IPS y Firewalls son la medida de seguridad adoptada con mayor frecuencia en los diversos tipos de redes de Edge computing. Afortunadamente, dada la creciente complejidad de las redes perimetrales, la seguridad de la red se ve impulsada cada vez más por herramientas de IA, como los sistemas de análisis de comportamiento de usuarios y entidades. Estas son herramientas que aumentan o complementan lo que hace el profesional de la seguridad, creando una detección más rápida de anomalías.

> "Edge no es una extensión de la nube ni un subconjunto de 5G. Edge Internet es una transformación fundamental de cómo se realiza la computación. Estamos pasando de una nube centralizada a una arquitectura habilitada por el borde, y eso significa que comienza a implementar nodos más cerca del usuario con más mayor capacidad de procesamiento de los datos"

Por otro lado, Wenzler, de Tenable, explica que El mayor desafío proviene de la naturaleza de estos dispositivos. Al estar construidos para la velocidad y la eficiencia, en contraposición a la seguridad y la privacidad, son intrínsecamente vulnerables y fáciles de atacar y comprometer.
"Muchos fabricantes se centran únicamente en la funcionalidad y ven la seguridad como un factor de coste innecesario. Aunque muchos consideran que estos dispositivos son casi desechables y que no necesitan ser protegidos, ya que tienen pocos datos críticos almacenados en ellos, la verdad es que a medida que se conectan más y más dispositivos IoT a las redes de todo el mundo, crean una enorme superficie de ataque que es fácil de comprometer y aprovechar para atacar objetivos internos más valiosos. Son fáciles de instalar, fáciles de escalar en grandes cantidades y pueden desplegarse en cualquier tipo de nube pública o incluso en un entorno local. Por ello, suponen un enorme reto de seguridad desde el punto de vista de la visibilidad básica, además de contar con capacidades limitadas a bordo para asegurar los dispositivos antes de ponerlos en servicio", agrega Wenzler, de Tenable.

Claudio Muñoz-Vivas
TELECOM DC POWER & OSP, Sales Application Engineer Team Leader en Vertiv

"Con 5G y crecimiento perimetral, IoT dará un gran paso adelante. Muchas organizaciones tienen dispositivos que se pueden conectar para obtener nuevos conocimientos, pero carecían de las capacidades de integración de datos, la potencia de procesamiento y el presupuesto para que

esto sucediera", comparte Muñoz-Vivas, de Vertiv.

La propuesta desde los proveedores

BeyondTrust

En general, alguien debe administrar los sistemas y dispositivos de la red industrial y en el Edge, y BeyondTrust puede proteger a los administradores de estos sistemas; evitando que conozcan contraseñas de altos privilegios, que tengan accesos directos hacia los mismos, y evitando también que requieran cuentas de altos privilegios en sistemas operativos de propósito general. Incluso cuando estos administradores necesitan accesos remotos a dispositivos IoT o IIoT, y cuando se necesita segregar estos accesos mediante zonas de recursos, BeyondTrust puede aportar en aspectos de Identidades Privilegiadas, Autenticación, Autorización y Auditoría.
Esto mitiga riesgos de phishing, robo de credenciales, explotación de vulnerabilidades mediante conexiones directas, y distribución de malware que se ejecuta con privilegios de administrador.
Es necesaria la entrega de sesiones privilegiadas hacia sistemas industriales (ICS - Industrial Control Systems), para los operadores o los encargados del mantenimiento, y es donde principalmente BeyondTrust puede ayudar.
En redes industriales (OT - Operational Technologies), es muy importante el manejo de tráfico de red, básicamente flujos, puertos y protocolos; conocer estos puertos es conocer las funcionalidades de sensores y otros dispositivos, y por esto último, administrar las sesiones privilegiadas que se transportan con este tráfico de red es también administrar la seguridad de sensores y otros dispositivos.

Fluid Attacks

Fluid Attacks se especializa en pruebas de seguridad continuas en una gran variedad de sistemas, entre los que se encuentran la infraestructura de la nube y el software de dispositivos IoT. Usamos una combinación de herramientas automáticas y métodos manuales para evaluar, desde el comienzo del ciclo de vida del desarrollo del software, la arquitectura e integridad de los controles de seguridad, las capacidades de detección y respuesta a las amenazas y las funcionalidades de la infraestructura susceptibles de ser explotadas. Por nuestro enfoque integral, los resultados de nuestras pruebas muestran tasas muy bajas de falsos positivos y falsos negativos. Además, dado que facilitamos la priorización y la asignación de responsabilidades de remediación inmediata de las vulnerabilidades que se detectan durante el desarrollo, nuestros clientes pueden evitar fallos en producción, costos mayores de remediación o ataques como fugas de datos.

GlobalSign

Es importante contar con infraestructura para la generación de certificados en velocidad compatible con la línea de producción de dispositivos. Así como también contar con certificados y llaves compatibles con chips TPM de mercado, que proporcionan seguridad sin impactar en la performance del dispositivo.
El TPM permite un sistema en el que ciertas garantías de seguridad se pueden demostrar criptográficamente a una parte remota, pero la identidad estándar integrada en el dispositivo TPM es insuficiente por sí sola para la tarea

Lumu Technologies

Queremos que cualquier organización, sin importar su tamaño, sector de la industria,

o arquitectura de red, puedan implementar una práctica de medición continua e intencional de compromisos. Para esto tenemos disponible nuestra herramienta Lumu Free, que permite en 3 pasos identificar si la red está presentando contactos con atacantes, de esta forma cualquier organización puede iniciar su viaje hacia el estado de cero compromisos.

Netskope

En el marco de la estrategia de SASE (Secure Access Service Edge) de Netskope, contamos con soluciones que permiten a las organizaciones simplificar su estrategia de seguridad manteniendo altos estándares de protección y rendimiento.

- Netskope Security Service Edge ayuda a eliminar los puntos ciegos al entender el SaaS, el IaaS y la web con extrema. La protección de datos de 360° salvaguarda los datos en todas partes a través de la galardonada DLP en la nube y cifrado. La protección avanzada contra amenazas detiene los ataques evasivos que atraviesan SaaS, IaaS y la web para infligir daños. Una nube Control total de SaaS, IaaS y web, desde una plataforma nativa en la nube que se escala automáticamente.
- Netskope SD-WAN ofrece un acceso seguro y de alto rendimiento a todos los usuarios remotos, dispositivos, sitios y nubes, por lo que los clientes se benefician de la seguridad de confianza cero con la optimización de la red. Como complemento a la SSE inteligente, la seguridad de la red está integrada en el SASE Gateway para abordar los requisitos locales como el stateful firewall para asegurar el tráfico este-oeste. La computación de borde, incluida en el Gateway, soporta aplicaciones de valor añadido, incluyendo IDS/IPS, Azure IoT Edge, Thousand Eyes, y otros desplegados como contenedores a través de la orquestación de un solo clic y la gestión automatizada del ciclo de vida.
- Netskope IoT: La solución de seguridad IoT de Netskope proporciona un contexto granular de dispositivos, con un identificador único de dispositivos y una tecnología de clasificación de autenticidad para descubrir dispositivos gestionados y no gestionados en la red corporativa. La solución analiza además cientos de parámetros de los dispositivos descubiertos y aprovecha la rica inteligencia contextual para la clasificación de dispositivos, la evaluación

de riesgos, el control de acceso granular y la segmentación de la red, facilitando la seguridad de confianza cero para los dispositivos IoT.

PwC Argentina

Brindamos -entre otros- servicios de Ciberseguridad ofensiva (pentesting, ejercicios de ingeniería social, identificación de vulnerabilidades, análisis de código, etc.), defensiva (SOC – monitoreo 7x24 de eventos de seguridad y generación de alarmas ante ciber-ataques, CiberInteligencia, Respuesta a incidentes, etc.), Hardening de sistemas y redes, etc. Ayudamos a asegurar los entornos físicos, así como a concientizar y capacitar a las personas sobre temas de ciberseguridad.

SonicWall

La propuesta de SonicWall de "Boundless Cybersecurity" o Ciberseguridad sin límites apunta exactamente a satisfacer esta demanda hiperdistribuida, donde tanto los recursos informáticos y de datos como los usuarios utilizan una movilidad intensa. Al colocar las soluciones de seguridad donde se encuentran los usuarios, los datos y los sistemas, logramos una capacidad de seguridad ilimitada y sin fronteras.
Con soluciones que pasan por protección perimetral, Data center, Cloud y SaaS, SonicWall se integra a la perfección al mundo digital rediseñado bajo los conceptos de Multi-Edge Computing.

Strike

En Strike ayudamos a las empresas a acceder a ciberseguridad de alta calidad de manera rápida y flexible. Nuestra plataforma cuenta con Strikers de primera línea entre los cuales tenemos especialistas expertos en realizar pentest sobre dispositivos IoT y Edge Computing. En el pasado hemos ayudado a mejorar la seguridad de gran variedad de este tipo de tecnologías.

Tenable

Nuestras soluciones nos permiten descubrir y actualizar continuamente la superficie de ataque, es decir, el inventario de dispositivos y recursos en la nube que el cliente tiene expuestos. Estos incluyen algunos que no sabían que estaban ahí. Entonces podemos evaluar ese inventario para encontrar las vulnerabilidades que tienen un riesgo significativo de convertirse en un ataque. Estas incluyen vulnerabilidades de software y de configuración, y pueden ser descubiertas incluso antes de que las nuevas aplicaciones entren en producción.
La cobertura total de la superficie de ataque es la clave.

Vertiv

Las soluciones en contenedores específicos y acondicionados para Centro de Datos, así como la infraestructura integrada, los microcentros de datos y los centros de datos modulares prefabricados, brindan potentes capacidades informáticas y de otro tipo, al tiempo que ofrecen velocidad de comercialización y seguridad física.
Las soluciones de Edge IT integran Equipos de aire acondicionado de precisión, con controles climáticos y de enfriamiento con eficiencia energética, distribución de energía eléctrica y conectividad de red como UPS con baterías de Litio o VRLA. Los equipos de TI generalmente también optan por software y dispositivos de monitoreo y administración remotos para ayudar a garantizar que las soluciones del borde de la red funcionen como se espera. En nuestras soluciones se destacan: infraestructura integrada, micro data centers y data centers modulares prefabricados.

Tasas mágicas de detección Antiphishing

Por Nicolás Gustavo Bruna, Product Manager de SMARTFENSE

Nicolás Bruna

En el ambiente de la ciberseguridad es común encontrarnos con herramientas Antiphishing que nos prometen tasas de detección del 99% o más.

A cualquier persona que lleve un par de meses en el rubro esto le debería sonar un poco raro. Todos sabemos que la seguridad al 100% no existe. ¿Cierto? La cuestión es que yo no soy nadie para juzgar a los gigantes tecnológicos, por lo tanto, voy a creer que, por ejemplo, Microsoft Office 365 tiene una tasa de detección de Phishing del 99,9995%.

¿Quién dijo problema?

Dicho de esta manera, esta tasa de detección me sugiere que me olvide del problema del Phishing. Estadísticas comunes como que "Más del 90% de los ciberataques comienzan con un Phishing" dejan de tener sentido.

El tema está en la cantidad absurda de correos de Phishing que se envían por día. Múltiples fuentes coinciden en que al menos 3 billones de correos de Phishing fueron enviados cada día en el año 2021.

Algunos cálculos

Si tomamos la tasa de detección del 99,9995% y la combinamos con el dato de los 3 billones de correos de Phishing diarios, vemos que incluso con esa tasa mágica, a una herramienta Antiphishing se le estarían escapando por día un millón y medio de correos de Phishing.

100% - 99,9995% * 3.000.000.000 = 1.500.000

Por lo menos a mí, esto está lejos de causarme cualquier tipo de tranquilidad.

Por supuesto, en nuestra organización particularmente no vamos a recibir todos los correos de Phishing diarios del mundo cada día, pero así tengamos la suerte de recibir el 0,0001%, con esta tasa mágica de detección nos aseguramos un ataque de Phishing por día.

La triste realidad

Resulta que cuando las herramientas de ciberseguridad se ponen a prueba en la práctica, los resultados terminan estando lejos de las tasas mágicas prometidas.

Un ejemplo de esto es la combinación de Microsoft 365 Email Security con Microsoft Defender. Luego de ser puestos a prueba durante el año 2022 en entornos reales, lograron una tasa de detección del 81.2%.

Otras empresas ya invierten en concienciación.

Los ciberdelincuentes prefieren “pescar” en la tuya.

SMARTFENSE

www.smartfense.com
info@smartfense.com

Dicho de otra manera, 18.8% de los correos de Phishing evaluados pudieron bypassear esta protección.
Me da miedo hacer esta multiplicación, y espero que sientan lo mismo, pero tenemos que hacerla:
3 billones de correos de Phishing por día * 18.8% = 354 millones de correos de Phishing que se pueden escapar por día a esta combinación de herramientas.

Ideas finales

Por suerte, las organizaciones inteligentes no se dejan engañar.
En estas organizaciones, se combinan diferentes capas de protección técnicas para aprovechar así las tasas de detección reales que resultan de esa combinación.
En adición a esto, cuentan con políticas claras para disminuir la probabilidad de que los usuarios sean víctimas de un ataque de Phishing exitoso, como el uso mandatorio de MFA.

Finalmente, consideran a las personas como una capa más de seguridad (si no la más importante) para disminuir el riesgo que la ingeniería social representa hoy para la información.
SMARTFENSE es la plataforma online de concienciación en Seguridad de la Información que genera comportamientos seguros en los usuarios. Si a su organización se le exige formar a su personal, nuestros contenidos abarcan todos los temas que necesite.

Innovación y Liderazgo Empresarial.

Noticias del sector Pymes en Argentina.

¡Publica con nosotros y llega a las Pymes de todo el pais!

TECNOPYMES·AR
innovación y liderazgo empresarial

Información actualizada para medianas empresas del sector de tecnología.
Entrevistas Exclusivas.

TecnopymesNews
company/tecnopymes
info@tecnopymes.com.ar
TecnoPymesNews
Tecnopymes

www.tecnopymes.com.ar

El rol de la Inteligencia Artificial en la era de trabajo remoto y ciberdelincuencia generalizada

Miguel Llerena

Por Miguel Llerena, Vicepresidente para Latinoamérica de Tanium

La Inteligencia Artificial (IA) se trata de un sistema al que se le ha enseñado a realizar tareas específicas sin que se hayan programado explícitamente. Este es el factor que permite a las soluciones de ciberseguridad analizar y aprender datos con mayor eficiencia y precisión, esto la convierte en la nueva prioridad de la ciberseguridad en los departamentos TI en las empresas.

La IA es una tecnología en constante evolución, y sus algoritmos permiten el aprendizaje automático, conocido como machine learning, que ayuda al sistema a aprender patrones, y adaptarse para simplificar la respuesta a los riesgos de incidentes.

Los profesionales de la ciberseguridad son inundados por muchas tareas, exceso de datos, falta de tiempo y poca disponibilidad de habilidades, por lo que la IA puede tener un gran impacto para los gerentes de IT.

Un enfoque de Inteligencia Artificial proporciona una mayor conciencia de eventos que suceden en el punto final y a través de múltiples disparadores. La Inteligencia Artificial puede entonces aumentar la cantidad de señal para priorizar eventos para que no se pierda en el ruido.

La Inteligencia Artificial también ofrece otro beneficio, ya que los puntos finales comúnmente tienen mucho espacio libre en disco y pueden almacenar datos en ellos más económica y eficientemente que en un Data Lake (lago de datos). Si esto se hace, también ofrece una mayor profundidad de los datos históricos para las investigaciones y la respuesta.

Los sistemas de IA de Tanium conocidos como Intelligent Edge colaboran categorizando los ataques según el nivel de amenaza.

Protección de datos

Intelligent Edge de Tanium, funciona mediante la implementación de técnicas de aprendizaje automático de IA para escanear y calificar rápidamente datos en movimiento, tales como correos electrónicos, mensajes de texto, documentos y archivos adjuntos asociados.

Protección en endpoint

El administrador de seguridad de Tanium logra un nivel más avanzado de prevención a través de recomendaciones de políticas y automatización que combina inteligencia de comportamiento de administradores y usuarios, indicadores de compromiso (IoC) y anomalías históricas para identificar amenazas.

La simplicidad lo es todo

Los líderes de TI y seguridad necesitan datos rápidos, procesables y confiables para optimizar su seguridad y operaciones y gestionar continuamente su riesgo. La Inteligencia Artificial puede proporcionar todo eso, y con una poderosa simplicidad.

Al llevar la inteligencia y el análisis de datos al límite, las organizaciones obtienen la velocidad, la visibilidad y los conocimientos necesarios para sobrevivir y prosperar en esta nueva era de trabajo remoto y ciberdelincuencia generalizada.

TANIUM.

Vea y control todos los endpoints dondequiera que esten!

Administre, asegure y proteja su red con la única plataforma que ofrece datos de sus endpoints de calidad, precisos y completos.

PRUEBA TANIUM GRATIS

Diana Torres, Asistente Administrativo de SourcePoint; Dámaris Carrero, Área de Marketing de SourcePoint; y Elmer Carrero, Gerente Comercial de SourcePoint

SourcePoint llevó a cabo un curso Portafolio WithSecure donde certificó a socios de negocios

SourcePoint es un distribuidor mayorista de soluciones corporativas de TI en Perú y la región andina, especializado en ciberseguridad, mayorista exclusivo de WithSecure en el ese país. Realizaron un evento en que capacitaron y certificaron a sus socios, donde tuvimos la oportunidad de entrevistar a Elmer Carrero, Gerente Comercial de SourcePoint.

¿Cuáles son las líneas más fuertes para su negocio?

WithSecure, anteriormente conocido como F-Secure Business, desde 1988 lidera la investigación y el desarrollo de la seguridad cibernética, que hoy por hoy son indispensables en la industria actual. Se trata de una empresa finlandesa, una de las más importantes y reconocidas en Europa en ciberseguridad, que cotiza en el NASDAQ desde 1999.

¿Qué soluciones corporativas están comercializando?

Hoy nos convoca en el evento la certificación de nuestros Socios de Negocios en los productos de WithSecure: EndPoint, EDR, Gestión de Vulnerabilidades, Protección de Microsoft 365 y Salesforce.

¿Cuáles son las ventajas/bondades de su programa de socios?

Nuestro enfoque es crecer con nuestros Partners y Socios Evangelizadores, conservando la lealtad y respeto del trabajo con nuestros clientes actuales y buscando lograr nuevos.

Es primordial para nosotros la fidelidad y lealtad en nuestra palabra y compromiso; la protección 100% de sus proyectos y clientes; garantía en renovaciones; y acompañamiento profesional en ciberseguridad y cierre de ventas. Gracias a la confianza y comunicación directa con SourcePoint, la marca no solo espera que hagamos números, sino que creemos un ecosistema de Socios de Negocios satisfechos y que identifiquen que vender WithSecure es un negocio y no una decepción y dolor de cabeza cuando lleguen las renovaciones, donde otras marcas fallan tremendamente.

¿Cuál es el valor agregado que le brindan a sus clientes?

Contamos con un Hub de Ciberseguridad WithSecure. Ello nos permite brindarles a nuestros socios y clientes comunicación y acceso directo al soporte local 8x5 o 24/7 del portafolio de productos en el idioma local, así como dar valor agregado a la compra de sus licencias. Siempre desarrollamos un trabajo coordinado con nuestros partners y socios de negocios.

¿Cuáles son hoy las categorías más demandadas?

Actualmente, son la protección del EndPoint con Gestión de Vulnerabilidades y el EDR o Detección y Respuesta de Incidentes. Vemos que aún el nicho de mercado para la protección

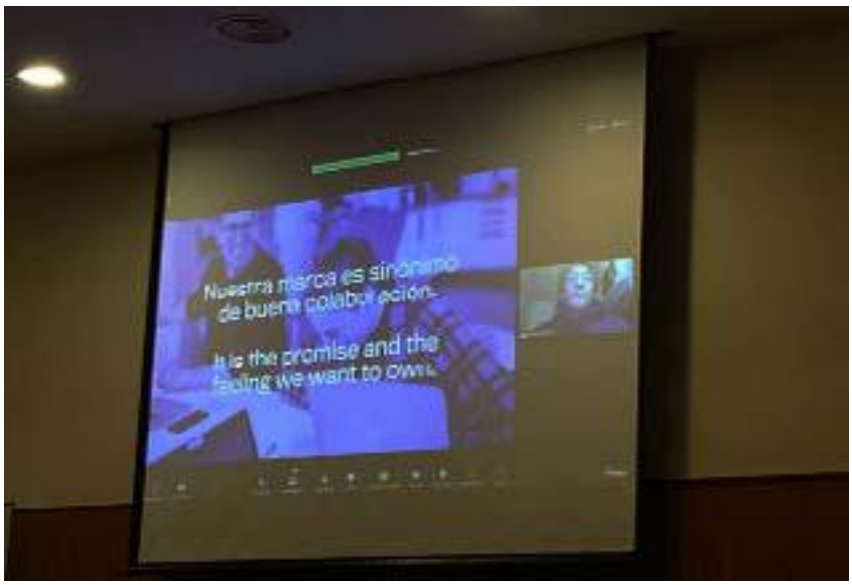
de Microsoft 365 es mínimo, ya que las empresas aún no comprenden el tipo de seguridad compartida que han aceptado con los proveedores de la nube.

¿Cuál es el objetivo principal de este curso Portafolio WithSecure?

Ante las constantes amenazas y ciberataques, el objetivo primordial de esta capacitación es dotar a nuestros partners y socios evangelizadores con las herramientas, el conocimiento adecuado y la comprensión de cómo pueden ayudar a frustrar la ciberdelincuencia y crear una cultura de ciberseguridad.

¿Qué expectativas tienen o qué esperan de eventos como los de hoy? ¿Qué perfil de empresas invitaron? ¿Cómo van a trabajar con estos canales en el futuro?

Los presentes son 100% nuestros Socios de Negocios. Es un evento cerrado de especialistas en ventas y técnicos que hoy se han certificado para lograr subir sus niveles de descuento con el fabricante y, además, pudieron tomar un conocimiento más amplio de los productos que ofrecemos, de la filosofía del fabricante y,



ya que nuestro objetivo es que ningún cliente que use nuestros productos sufra un incidente de seguridad, como un ataque de ransomware o la intrusión a sus equipos o redes.

Pero todo esto, como lo indica nuestro nombre WithSecure, lo podemos hacer solo con el socio, con el apoyo de las áreas de TI de los clientes, que cuentan con nuestro apoyo para el cierre exitoso de los negocios.

sobre todo, de cómo hacer negocio respetando el trabajo de los que tienen a la derecha o izquierda de sus mesas.

¿Cómo se están preparando para el próximo año?

Tenemos buenas expectativas con nuestros Socios de Negocios; tenemos diferentes opciones de negocio, desde los que recién entran al nicho de mercado de la ciberseguridad a los más especializados, y con ellos hemos estado conversando para diseñar estrategias de protección de alto nivel,

Ekoparty: volvió presencial el gran evento de seguridad de la Argentina

Del 2 al 6 de noviembre se celebró el mayor evento de la comunidad de hacking de Latinoamérica. La edición 2021 contó con charlas, talleres, networking, contenido audiovisual y actividades de todo tipo, workshops, espacios de Red Team, Blue Team, Bug Bounty, Mobile Hacking, Lockpicking, DevSecOps, Ingeniería Social y más componen fueron parte de la agenda del evento que desde hace más de 16 años expone los últimos hallazgos en seguridad ofensiva, complementados con las mejores prácticas de seguridad defensiva. Por Fernando Juliá

Charlas y conferencias

DÍA 1

Crypto Crimen

En los últimos 10 años, 154 ataques costaron a la sociedad casi 4 mil millones de dólares El mundo de los blockchains, criptomonedas y contratos inteligentes crece cada día más, y junto con ello lo hacen también los ataques. La alta demanda y la inminente adopción masiva generan un interés colectivo frente a una oportunidad que promete ser el futuro. Pero también existen cientos de atacantes alrededor del mundo que utilizan esta tecnología para sus propios beneficios, apuntando a víctimas de bajo riesgo y alta recompensa.

La charla de Francis Guibernau hizo un recorrido por los fundamentos del blockchain, la anatomía de los ataques más comunes, y su impacto en el lavado de activos. Entre ellos, se destacan: Inside Jobs - Exit Scams, Criminales y Amenazas avanzadas persistentes (APTs), “Ataques a Exchanges Centralizados” (CEX), y HTTP Response Smuggling.

Hasta hoy, muchas veces cuando se reportan estas vulnera-

bilidades, no se consideran críticas. Sin embargo, las técnicas de Request smuggling permiten evadir controles de seguridad, obtener acceso no autorizado a datos sensibles, y hasta comprometer usuarios de una aplicación web.

SAP

Los ataques para conseguir datos sumamente confidenciales son cada vez más frecuentes. Frente a ello, las empresas más importantes del mundo confían en otras el cuidado de su información financiera, de recursos humanos y todos sus procesos de negocios. Una de las empresas encargada de estas tareas, y elegida por miles de empresas alrededor del mundo, es SAP.

Sin embargo, pese a su experiencia en el campo, existen vulnerabilidades en el sistema que, de ser explotadas por atacantes, pueden generar consecuencias muy graves. Durante 2020, el equipo de investigadores de seguridad de Onapsis se enfocó en tres, y presentó sus hallazgos en Ekoparty: SAP RECON, SAP CM P2P Communication, SAP JAVA RCE.

Big Data, ¿cómo protegerse de las inseguridades y vectores de ataques?

Si bien cuando hablamos de

Big Data, hablamos del almacenamiento de grandes volúmenes de información, hay que tener en cuenta además los numerosos factores que hacen a su ecosistema y que son indispensables a la hora velar por la seguridad de los datos. Existen 4 capas que componen el Big Data y por las que pasa la información: Data Ingestion, Data Storage, Data Processing y Data Access. En este caso, Sheila A. Berta desarrolló una metodología para el análisis y cuidado de los datos que consiste en analizar la estructura, desarmando capa por capa, para ver la seguridad de cada componente y estar seguros de estar cubriendo todas las fases con las que se quiere trabajar. A su vez, brindó una serie de recomendaciones de seguridad a tener en cuenta para evitar los vectores de ataque que pueden aparecer en las distintas capas: Reducir la superficie de ataque, uso Firewall, cambio de credenciales, Implementar la autenticación, Administrar autorización, e implementar comunicaciones seguras.

DÍA 2

Ataques y amenazas informáticas: ¿qué herramientas ayudan a prevenirlos, ¿cómo actúan las empresas y cómo darnos cuenta a tiempo?

La segunda jornada de Ekoparty dio lugar al conocimiento de numerosos ataques que reciben los usuarios cada día. Para algunos de ellos hay he-

rramientas y métodos de prevención, otros aún le ganan al sistema.

El comienzo del día estuvo a cargo de Saransh Rana, Divyanshu Mehta y Harsh Varagiya, de India, quienes brindaron una gran explicación sobre la seguridad centralizada y la detección de configuraciones de AWS Lambda, a través de un sistema escalable que otorga visibilidad sobre amenazas, configuraciones inseguras como bases de datos expuestas, y políticas de permisos laxas.

Luego, tuvieron lugar Pablo Artuso e Ignacio Favro con su charla "De 0 a millones de dólares en un par de paquetes: Comprometiendo sistemas SAP en Internet sin autenticación", donde revelaron 3 vulnerabilidades de una de las empresas que maneja los datos de las empresas más importantes del mundo.

Más tarde y desde Hawaii, Patrick Wardle, top security researcher y speaker habitual de Ekoparty, mostró una de las últimas vulnerabilidades de macOS, su área de especialización. Se trata de una vulnerabilidad que logró evadir diversos mecanismos de seguridad del sistema operativo, como File Quarantine, Gatekeeper y Notarization, y les permitió a los atacantes comprometer sistemas macOS con apenas un par de clics por parte del usuario.

Para cerrar el día, Rafael Selema Marques, desde Brasil, con su charla "Revisiting ring3 API hooks: tricks to defeat analysis tools… Even the famous ones". En ella, presentó dos técnicas que son utilizadas actualmente, a las cuales nombró "Egg hook" y "Hollow hook", que utilizan distintos tipos de malware (código malicioso) para evadir herramientas de análisis.

DIAL: ¿la herramienta ideal para la detección de amenazas en la nube?

DIAL es una herramienta pronta a lanzarse, desarrollada para prevenir y detectar amenazas específicamente en AWS -Amazon Web Services, un proveedor de servicios en la nube-. Entre sus beneficios se encuentran:

- Detectar de forma nativa un evento de AWS en tiempo real (<5 segundos)
- Es infinitamente escalable
- Facilita el aumento de la cobertura de seguridad de cualquier recurso de AWS
- Es fácil de implementar en varias cuentas de AWS al ser una implementación de un solo clic
- Es altamente rentable, ya que no tiene servidor sobre AWS Lambda.

DÍA 3

Durante la tercera jornada de Ekoparty, expertos en ciberseguridad revelaron sus últimos hallazgos, así como las herramientas y métodos más factibles para hackear diversos sistemas y brindar seguridad

a la sociedad.
Por la mañana, desde Estados Unidos, Douglas McKee y Philippe Laulheret brindaron una charla sobre vulnerabilidades en dispositivos médicos y el peligro de que una de las herramientas más utilizadas en estas instituciones, la bomba de infusión, sea comprometida y mal utilizada para robar información, subir o bajar dosis de medicación a los pacientes, o mostrar indicadores falsos.
Más tarde, desde Israel, Raul Onitza-Klugman y Kirill Efimov contaron cómo se podrían explotar vulnerabilidades en entornos de desarrollo integrado (IDE) para perpetrar ataques no solo a una organización, sino a toda su cadena de suministro.
Desde Estados Unidos, Valentina Palmiotti brindó su charla llamada "Kernel Pwning with eBPF: a Love Story", donde comenta lo popular que se ha vuelto eBPF entre los desarrolladores, una tecnología que permite extender las capacidades del kernel de Linux de forma fácil y segura sin necesidad de escribir código; así como vulnerabilidades en esta herramienta que podrían permitir la ejecución de código malicioso por parte de un atacante.
Para cerrar, Salvador Mendoza reveló las claves de "Pinata" o "PIN Automatic Try Attack", un método que podría permitir dar con el número PIN de una tarjeta mediante técnicas de fuerza bruta.

Una historia de amor: eBPF, la herramienta preferida de los desarrolladores para hackear de forma fácil el Kernel
En informática, un núcleo o Kernel es un software que constituye una parte fundamental del sistema operativo. Debido a su importancia, es frecuente que los atacantes desarrollen mecanismos para comprometer este componente y así afectar al sistema por completo. Para trabajar con el kernel, los desarrolladores utilizan distintas herramientas; una de las más populares actualmente es eBPF -Extended Berkeley Packet Filter-, un filtro de paquetes de Berkeley que permite que los programas se ejecuten sin tener que cambiar el código fuente de Kernel o agregar módulos adicionales.

Ataque Pinata: ¿cómo conseguir el pin de una tarjeta de contacto EMV?
La utilización de tarjetas de contacto EMV bancarias para realizar transacciones es muy común en muchos países. Su proceso es simple: autenticación (cuando se ingresa y reconoce la tarjeta), verificación de la transacción (por medio de firma, pin) y autorización (cuando se acepta o declina la transacción). Allí, el factor importante que realiza la acción es el chip de la tarjeta al ponerse en contacto con el lector de la terminal.

Sin embargo, tal como descubrió y expuso Salvador Mendoza en su charla en Ekoparty, existen métodos que podrían permitir dar con el PIN de una tarjeta. El ataque "PINATA" (PIN Automatic Try Attack) utiliza técnicas de fuerza bruta para probar miles de combinaciones bajo las siguientes condiciones:

Talleres

¿Cuántas vidas le quedan a un hacker? Cuando evitar la cárcel no es un juego
La criminalización de la actividad de los hackers muchas veces está ligada a la falta de información y de actualización de las normativas de cada país. Para quienes trabajan en ciberseguridad el hecho de denunciar inconsistencias o sistemas vulnerados se torna en ocasiones un potencial peligro personal.
Dotar al hacktivismo de ilegalidad hace verosímiles las cau-

sas que se inician alrededor de los que se aventuran a contar que algo no está funcionando bien en términos de seguridad informática. Durante la última jornada de Ekoparty, la conferencia de ciberseguridad más importante de Latinoamérica, algunos de los debates se centraron en el insuficiente marco legal que existe en la región y casos de aquellos que fueron procesados por el uso de legislación obsoleta.

El taller de Avoiding Jail (evitando la cárcel) empezó en 2020. "Buscamos concientizar sobre la informalidad de actividades de seguridad no autorizadas, y dar a conocer sus límites legales", comenta Marcelo Temperini, Abogado especializado en cibercrimen y director de la propuesta.

En Argentina existe una ley de delitos informáticos, del año 2008 (Ley Nº 26.388), que, si bien vino a realizar un ajuste necesario desde el punto de vista social, se considera que, en la actualidad, parte de esa normativa termina afectando el desarrollo de los investigadores de infosec. "Puntualmente, desde Ekoparty se ha propuesto desde el año pasado, una modificación al art. 153 bis, que pretende agregar una excepción a la pena para el caso que el/la investigador/a reporte una falla de buena fe y con la intención de proteger un interés público (por ejemplo, los datos de los ciudadanos)", detalla Temperini.

"Entendemos que es importante formar parte de una libertad necesaria para poder aportar conocimiento a la sociedad, y que los verdaderos propietarios de los sistemas sean los que tengan consecuencias por estar enriqueciéndose a costa de un sistema informático inseguro, que termina poniendo en riesgo información (sensible o no) de las personas", finaliza Temperini.

Wardriving

Desde la Ekoparty, el mayor encuentro de expertos en ciberseguridad de Latinoamérica, desarrollaron un año más el "Wardriving", una actividad que tiene como objetivo hacer una comparativa en el tiempo para analizar la evolución de la seguridad de las redes Wi-Fi. A través de este desafío, los participantes recorrieron la ciudad en micro este jueves 4 de noviembre, buscando redes WI-FI usando un software con un GPS y antenas especialmente diseñadas. Luego, identificaron geográficamente estas redes en un mapa y analizaron su nivel de seguridad en base a los protocolos que utilizan.

"Los datos demuestran que está aumentando la seguridad de las redes en la ciudad. Sin embargo, este campo se actualiza y cambia constantemente. Hoy en día existe un protocolo nuevo llamado WPA3, que hemos visto en una sola red a lo

largo de nuestro recorrido. Si bien esto nos demuestra que hay bastante para evolucionar, comparando con resultados de años anteriores, podemos decir que estamos yendo por un buen camino", explicó Agustín Osorio, coordinador del Wardriving de Ekoparty.

Empresas presentes

Tuvimos la oportunidad de poder charlar con algunas de las empresa presentes durante las jornadas. Esto es lo que compartieron con ITware Latam.

DELL

Para Dell la Ciberseguridad es uno de los tópicos más importantes dentro de las organizaciones y una de las prioridades de la empresa, nada nos detiene para ayudar a frustrar las amenazas cibernéticas con infraestructura y dispositivos intrínsecamente seguros, con detección completa de amenazas, capacidad de respuesta y protección de datos.
Estuvimos mostrando nuestras soluciones sobre Seguridad con la complejidad tecnológica que garantizan la protección de los datos. Nuestro mensaje principal fue: Los ataques cibernéticos nunca cesarán, pero con Dell Technologies puede tener la tranquilidad de que sus datos y recursos de TI están seguros, protegidos y disponibles. Nada nos detiene para ayudar a frustrar las amenazas cibernéticas con infraestructura y dispositivos intrínsecamente seguros, detección completa de amenazas y respuesta a ellas, protección de datos y Cyber Recovery.

Otro tema fue cómo la Resiliencia cibernética, como una mirada holística, desde la prevención hasta la recuperación. Existe una incertidumbre de los CISO, ya que cerca del 65% de los tomadores de decisiones de TI no confían mucho en que sus datos/sistemas puedan recuperarse por completo, adicional a que las organizaciones están administrando 10 veces los datos en comparación con hace 5 años, casi 15 PB en promedio ahora y más del 60% de las organizaciones han experimentado una pérdida de datos debido a una vulnerabilidad explotada.

STRIKE

Santiago Hernández, Cloud Engineer
Desde Strike nos parece clave estar presentes como Sponsors oradores en este evento, que es la conferencia de ciberseguridad más grande de Latinoamérica y reúne a los referentes del sector de ciberseguridad en la región. Somos una empresa que provee ciberseguridad de alta calidad a todo tipo de compañías, y por eso nos pareció fundamental estar en contacto con las compañías más importantes de Latam en un evento tan emblemático como Ekoparty.

Además, fuimos speakers del Sponsors Track y expusimos la charla “The Bugs Kitchen”, donde analizamos cómo funciona el mundo del pentesting por dentro, los bugs más comunes con los que se encuentran en sus actividades y las técnicas más creativas que se pueden utilizar para evitarlos. Por último, contamos con un Stand con juegos, demos en vivo y premios.

Sin dudas, Ekoparty es un evento donde se explora la importancia de la ciberseguridad. Desde Strike, fue fundamental poder transmitir la relevancia de contar con seguridad de calidad desde el primer día, sin importar la industria o tamaño de la empresa. En ese aspecto, la CISOs Summit y el Sponsors Track fueron piezas claves para transmitirles a los asistentes cómo nuestros Strikers (hackers éticos) trabajan y encuentran vulnerabilidades de formas creativas, tanto en startups como en compañías de gran escala. Fue muy importante que nos hayan escuchado y haber conocido a los asistentes, y estamos muy agradecidos por toda la experiencia.

CloudHesive

Soy Axel Bria, nosotros brindamos consultoría a compañías para todo lo que es migración de cargas de trabajo a la nube, consultoría y soluciones de AWS específicamente, y estamos acá porque estamos incursionando en lo que tiene que ver con seguridad informática, ampliando nuestro stock de productos y también reforzando nuestro abanico de servicios.
Trabajamos en base a servicios gerenciados de seguridad, y estamos apuntando a mejorar más sobre este tipo de tareas.

Del evento esperamos poder difundirlo que hacemos en CloudHesive, poder conocer tecnología de vanguardia, lo que se está haciendo en el mercado, estar al tanto de todo lo que se vaya hablando en las conferencias y poder justamente también acercarnos a las personas que trabajan de esto, para que sepan que hacemos, y que con todo gusto puedan sumarse a nuestro equipo.

Fortinet y Consulting Services

Rosa Perín, marketing manager Consulting Services
Hoy en día estamos presentes en el Centro de Convenciones, acompañando a Fortinet. Nosotros de nuestro lado somos Consulting Services, uno de los principales partners de Fortinet, que es una de las principales marcas mundiales a nivel global en ciberseguridad.
Fortinet principalmente está abocado sí a empresas, pero justamente las empresas es-

tán formadas por personas, entonces tratamos de que por lo menos todas las personas que asistan puedan conocer, sobre todo desde la vocación laboral, que puedan saber que pueden contar con capacitaciones laborales, que pueden certificarse, pueden tener un montón de cosas que se llevan ellos mismos en cuanto a conocimiento técnico que hoy en día en el mercado es lo más importante, y desde ese lado Fortinet acompaña a cada personal de cada empresa para que pueda generar un conocimiento y tener certificaciones que son fundamentales para ingresar al mercado laboral.

Banco Galicia

Banco Galicia fue parte de la conferencia de ciberseguridad con un enfoque especial en el metaverso; permitiendo explorar las nuevas aplicaciones de las tecnologías inmersivas en la prestación de servicios bancarios.

El banco visualizó al metaverso como un elemento clave en el futuro de la banca; sobre todo en las áreas de atención y fidelización de los clientes.

Pedro Adamovic, chief information security officer (CISO) de Banco Galicia, dijo “Trajimos una experiencia inmersiva donde podés pasar un rato en otro ámbito, recorrer dos habitaciones e interactuar con sus objetos. Con esto queremos mostrar lo que se viene, la posibilidad de que desde una casa hasta un banco existan en una vida paralela”.

Acerca de esta meta futura, Banco Galicia reconoció que el mayor obstáculo en el uso de esta tecnología es su propia novedad, encontrándose de momento, en una especie de estado embrionario. Logrando superar esto, el metaverso tendría posibilidades ilimitadas para la apertura y ejecución de sucursales y transacciones tecnológicas sin ningún tipo de frontera más que el mismo metaverso.

Ekoparty: reivindicar al talento local

Durante las jornadas vividas tuvimos la oportunidad de charlar con Leonardo Pigñer, CEO de Ekoparty y uno de los fundadores del evento también.

“Bueno, la Eko vos sabes que tiene 18 años de historia y un poco respondiendo a tu pregunta por qué hay tantos cambios en la Eko. En el 2019, que fue la última eco presidencial, que daba para mucho más, pero no podíamos realizar o materializar todo lo que queríamos. Porque nos faltaba tiempo. Siempre fue un proyecto colaborativo donde el tiempo que te queda es el que utilizas para el evento, es un esfuerzo de la Comunidad. Pero nosotros sentíamos que se podía hacer mucho más”, comenta

Ya en 2020, los primeros meses como que hicieron un cambio y crearon una organización alrededor de Ekoparty, que se

Leonardo Pigñer, CEO de Ekoparty

dedicara solamente a organizar la conferencia. Pigñer comenzó ahí a trabajar para ponerle foco solamente a esto, y a los pocos meses les agarró la pandemia. Pero fue una gran oportunidad para reinventar la Ekoparty, como les pasó a todos.

"Y nos pusimos a repensar el evento, qué podíamos hacer ya que no teníamos un evento grande, presencial. Hicimos virtual durante la pandemia, y fue muy bien, fue tremendo, y también nos permitió hacer un montón de cosas más, y fuimos trabajando mucho en eso. Y la verdad que nosotros en la pandemia no paramos ni un solo segundo y desde la Comunidad se generaron muchísimas cosas, y se sumó mucha gente a la Comunidad de Ciberseguridad, por el esfuerzo que todos veníamos haciendo y también por cosas que pasaba, por el aumento de los ciberataques y el cibercrimen", sostiene Pigñer.

Y es natural ahora que ya volvió la presencialidad con un evento más grande, porque se sumó más gente y quieren darle lugar a todos. Cuando arrancaron los fundadores de 18 años atrás no había una Ekoparty, no había nadie que pudiera compartir conocimiento. Era difícil, y el evento nació por eso, nació para compartir, porque hacía falta un espacio para aprender y compartir. Había espacio para empresas que les hablaban a empresas, pero no para el que después terminaría trabajando en ellas.

"Para el que tenía esa pasión por la tecnología, por el conocimiento, no había un espacio para aprender, todo era más comercial, y queremos seguir manteniendo ese espíritu, haciendo ese esfuerzo para incluir y dar todas las oportunidades a los que están comenzando, porque fueron las que no tuvimos nosotros cuando arrancamos hace 20 años atrás", indica el directivo.

Y por eso están contentos que se sume tanta gente joven, y trabajan hasta con escuelas secundarias técnicas, que empiezan a palpar lo que es trabajar en equipo, trabajar con otra gente del exterior. "Recién preguntaba en el au-

ditorio ¿para quiénes era su primera Eko?, y la mitad levantó la mano, eso es impactante. Ellos son el futuro de todo lo que estamos haciendo y van a terminar adueñándose de la Eko y dándole formas que todavía no imaginamos", agrega.
"Cuando arranqué mi sueño era conseguir trabajo en ciberseguridad. Ahora vienen los chicos acá y tienen a empresas de todas partes del mundo contratando, buscando talento. Se hacen amigos que también te facilitan el acceso a conseguir un empleo. Eso de seguir generando oportunidades está buenísimo, y por eso fuimos también creando la Ekoparty Academy, la Academia de Hackers, por donde ya pasaron 600 chicos", cuenta Pigñer.
Este año nació Eko Jobs, que lo que hace es conectar a las empresas con los chicos que cruzaron, la gente que fue a compartir, para que puedan conseguir su primer trabajo, darles una mano en ese sentido, porque el ambiente ya necesitaba una profesionalización, pero estaba muy disperso.
Había un déficit enorme a nivel mundial de profesionales ya de antes de la pandemia, y con ella se incrementó. Pero lo que Pigñer siempre dice es que faltan oportunidades, porque talento tenemos muchísimo en Argentina. Los buenos consiguen trabajo rápido. Una vez que te insertaste en el mercado, puedes trabajar para Estados Unidos para un montón de lugares. "Lo que tenemos que facilitarles a los que están comenzando. Que se metan y después ya está, hacen su camino. Esa primera oportunidad es la más difícil".
Tuvieron 40 charlas en total, un récord, y de altísimo nivel. De entre ellas Pigñer rescataría la charla de Juan Guerrero sobre cibercrimen en Latinoamérica, más que nada porque es un tema del que no se conoce y no se habla acá en la región y no hay muy pocos estudios regionales. Como no hay un interés económico atrás de los estudios, pocos se dan a conocer, y se necesita background local. Otra charla que le gustó mucho fue la de Sebastián García y Verónica Valero, que son dos argentinos que van a estar en Praga haciendo una investigación en una universidad, y van a contar los riesgos de privacidad en las redes de telefonía. Que uno piensa en WhatsApp, Facebook, y otras redes sociales, pero telefonía ya es vieja, y como toda tecnología tiene sus falencias, y hay que tener cuidado para no exponer nuestra privacidad.
"Y otra charla que señalaría es la de Dan Borgogno y la de Iliana Barrionuevo, que son dos investigadores cordobeses. Dan famoso acá en la Eko porque ganó dos veces el premio a la mejor charla, por la charla de cómo hackear la SUBE, cómo hackear el DNI Digital al año siguiente, y este año va a contar cómo armar, clonar un sistema de pagos con tu teléfono celular", añade el directivo.
Pigñer finaliza con un mensaje a la comunidad: "Me parece que el esfuerzo de generar nuevo talento es una de las cosas más importantes de la Eko. Lo que creo es que para una tener una sociedad más segura necesitamos más hackers, porque es un poco el luchador de la libertad, el que expone los riesgos de privacidad, que va a cuidar tus datos, y a veces las empresas y los países no lo hacen. Para los que estamos en la industria es importante entender que es un esfuerzo de todos, que Ekoparty lo estamos haciendo, necesitamos que nos acompañen, y todos los que quieran participar desde la comunidad, desde las empresas a venir a colaborar acá están las puertas abiertas para hacerlo".

Desafío: La fuerza de trabajo en ciberseguridad

Persiste una necesidad crítica de profesionales de ciberseguridad en medio de un año de evolución cultural y laboral. Les compartimos un resumen del extenso estudio realizado por (ISC)2

2022 es un año altamente formativo para la profesión de ciberseguridad, y continúa cambiando y evolucionando con el mundo que la rodea.
Estimamos el tamaño de la fuerza laboral de seguridad cibernética global en 4,7 millones de personas, el más alto que jamás hayamos registrado. Sin embargo, según nuestra investigación, el campo de la ciberseguridad todavía necesita urgentemente más profesionales. Para proteger adecuadamente a las empresas interindustriales de amenazas modernas cada vez más complejas, las organizaciones están tratando de llenar el vacío mundial de 3,4 millones de trabajadores de ciberseguridad.
Si bien la fuerza laboral de seguridad cibernética está creciendo rápidamente, la demanda está creciendo aún más rápido. El análisis de la brecha de la fuerza laboral de seguridad cibernética de (ISC)2 reveló que, a pesar de agregar más de 464 000 trabajadores el año pasado, la brecha de la fuerza laboral de seguridad cibernética ha crecido más del doble que la fuerza laboral con un aumento interanual del 26,2 %, por lo que es una profesión que necesita más gente.

Abordando la brecha en la fuerza laboral

Algunos factores ciertamente están fuera del control de una organización: la demanda de empleados de seguridad cibernética aumentará a medida que el panorama de amenazas continúe creciendo en complejidad y la oferta no siempre pueda mantenerse al día.
Este análisis sugiere que los problemas con un impacto más negativo son aquellos que las organizaciones pueden controlar: no priorizar la ciberseguridad, no capacitar suficientemente al personal y no ofrecer oportunidades de crecimiento o promoción. No poder encontrar talento calificado fue en realidad el problema de menor impacto según este análisis.
Aunque casi todas las iniciativas tuvieron un impacto positivo en la dotación de personal, descubrimos que las organizaciones con iniciativas para capacitar al talento interno (asignaciones de trabajo rotativas, programas de tutoría y alentar a los empleados fuera de la seguridad cibernética a unirse al campo) tenían menos probabilidades de tener escasez.

La automatización también se está volviendo más frecuente en la ciberseguridad: el 57 % la ha adoptado hoy y un 26 % adicional planea adoptarla en el futuro, y aunque no es probable que reemplace a los trabajadores de ciberseguridad en ningún momento en el futuro previsible, la automatización de procesos que son coherentes y repetibles libera a los trabajadores para que se concentren en tareas de

mayor nivel.
El estudio encuentra que los gerentes de contratación de seguridad cibernética que tenían una relación laboral sólida con su departamento de recursos humanos tenían muchas menos probabilidades de tener una escasez significativa de personal en sus organizaciones. Sin embargo, solo el 52 % de los encuestados dijo que los gerentes de contratación tienen una relación laboral sólida con RR. HH., y el 40 % de los gerentes de contratación dijeron que el departamento de RR.

Qué significa esto para las organizaciones

Combatir la escasez de personal no es una tarea fácil, pero los hallazgos de nuestra investigación arrojan algunos puntos clave donde las organizaciones pueden enfocarse: Comprenda cuál es su brecha; Hacer hincapié en la formación interna; los desafíos más asociados con la gran escasez de personal fueron la falta de énfasis en la seguridad cibernética en toda la organización, la capacitación insuficiente del personal y la falta de vías para el crecimiento; Trabaje con RRHH, no contra ellos cuando contrate para ciberseguridad. Aquellos que no lo hicieron tenían más de 2,5 veces más probabilidades de tener una escasez significativa de personal en comparación con aquellos que han construido una relación sólida con RRHH.

Cultura del equipo de ciberseguridad

La cultura de la empresa define en gran medida la experiencia de los empleados. Da forma al entorno social en el que operan los empleados afecta la forma en que se comunican y colaboran con colegas dentro de su propio equipo y en toda la organización. Y puede influir en qué tan satisfechos y apoyados se sienten por su empleador en general, lo que en última instancia influye en las respuestas a la pregunta "¿debo quedarme o debo irme?"

Entender la experiencia del empleado de seguridad

El estudio encuentra que, para muchos, la satisfacción laboral sigue siendo alta. Sin embargo, la satisfacción de los encuestados fue menor con sus equipos específicos (68 %), departamentos (62 %) y organización general (60 %). La infelicidad tendía a provenir de la cultura y los problemas del lugar de trabajo, más que del propio trabajo de ciberseguridad. Las siguientes tres razones para dejar un trabajo están todas relacionadas con las condiciones del lugar de trabajo: cultura negativa, agotamiento y equilibrio deficiente entre el trabajo y la vida personal.

Que influye en la experiencia del usuario

¿Cuáles son los factores más impactantes que impulsan tanto las puntuaciones altas como las bajas?
- No invitar y valorar los aportes de los trabajadores contribuye significativamente a una EX deficiente
Se preguntó a los encuestados qué problemas tenían un impacto negativo en su satisfacción laboral. La respuesta más común fue tener "demasiados correos electrónicos/Tareas". Esto no es sorprendente, considerando la prevalencia de la escasez de personal. Sin embargo, el exceso de trabajo de los empleados, ya sea que esté relacionado con una dotación de personal inadecuada o no, no afectó negativamente los puntajes EX tanto como una variedad de problemas culturales y organizacionales.
- Las organizaciones que hacen que los empleados se sientan escuchados

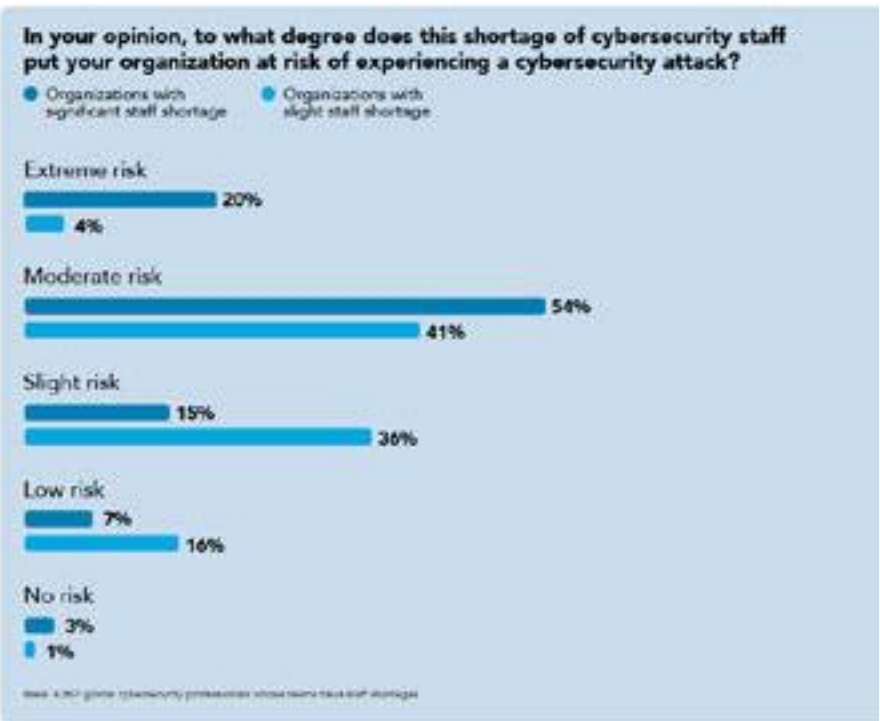
tienen personal más feliz
Por otro lado, las iniciativas más comunes que las organizaciones han implementado para mejorar el EX de los empleados se centran en la flexibilidad laboral, incluido el trabajo remoto. Sin embargo, tales programas, aunque ahora muchos trabajadores los consideran adaptaciones esenciales, no son los más impactantes.

El trabajo remoto duplica la adopción

El trabajo remoto tiene un impacto sustancial en la experiencia de los empleados. Las calificaciones EX promedio de los encuestados que trabajan completamente a distancia (54,4) y el trabajo flexible (53,4) son más altas que las que se requieren para estar a tiempo completo en la oficina (48,0). Un 59% dijo que siempre prefiere trabajar de forma remota. Más de la mitad consideraría cambiar de trabajo si ya no se les permitiera trabajar de forma remota. El 62 % de los profesionales de ciberseguridad que no son gerentes dicen que son más productivos cuando trabajan desde casa; esto se compara con solo el 35% de los gerentes que dijeron que el personal remoto no es tan productivo como el personal en el sitio.

Qué significa esto para las organizaciones

La cultura del equipo de ciberseguridad es crucial para reducir la rotación de empleados y aumentar la productividad. Nuestro estudio encontró que al personal de seguridad cibernética generalmente le encanta el trabajo de seguridad cibernética, pero eso no significa que siempre estén contentos en su organización o equipo en particular. Los empleados insatisfechos son menos productivos y es más probable que se vayan, lo que les cuesta a las organizaciones tiempo y recursos valiosos para reemplazarlos.



Además de los problemas de retención, el 68 % de los empleados Low EX dicen que la cultura del lugar de trabajo afecta su efectividad para responder a los incidentes de seguridad cibernética. Los hallazgos clave para las organizaciones que buscan prevenir problemas con la experiencia de los empleados son los siguientes: Valore la voz de su empleado; Las iniciativas EX dan sus frutos; Las opciones de trabajo flexibles se han convertido en la norma; Prepárese para una fuerza laboral cambiante.

Trayectorias profesionales

Están surgiendo nuevas tendencias y perspectivas, es decir, la evolución está motivando a las personas ya las organizaciones a valorar la educación, las certificaciones y las habilidades prácticas de manera diferente a como lo hacían en el pasado.

Para los trabajadores más jóvenes, más caminos conducen a la ciberseguridad. Casi la mitad de los encuestados menores de 30 años pasan a la ciberseguridad desde una carrera fuera de TI. Es más probable que los profesionales más jóvenes usen su

educación en seguridad cibernética o un campo relacionado (23 %) como un trampolín para ingresar a la profesión o pasar de un campo totalmente diferente (13 %) fuera del panorama de TI o seguridad cibernética.
Algunos incluso son reclutados después de su propia educación en ciberseguridad (12%). A medida que los encuestados se acercan a las edades de 50 a 54 años, observamos un pico en la cantidad de empleados que han utilizado una carrera en TI como su camino hacia el campo (74 %), lo que demuestra que esta práctica muy popular ya no es la fuente principal para contratar a personas más jóvenes.
talento en ciberseguridad
Para los nuevos empleados, la experiencia y las habilidades prácticas son cada vez más importantes. De 2021 a 2022, las habilidades prácticas y la experiencia se han convertido en calificaciones más importantes para quienes están considerando trabajar en la profesión de ciberseguridad. En particular, se está poniendo más énfasis en la experiencia laboral de TI relevante (29% a 35%), habilidades sólidas para resolver problemas (38% a 44%) y experiencia laboral relevante en ciberseguridad (31% a 35%).
La importancia omnipresente de las certificaciones recibió menos prioridad este año (29 % frente a 32 %), al igual que las calificaciones o capacitaciones en ciberseguridad (17 % frente a 23 %), los títulos de posgrado (10 % frente a 13 %) y los títulos universitarios (10 % vs 14%)
El doble de personas ve la promoción interna como su próximo hito profesional vs cambio de trabajo. A pesar de la alta rotación de ciberseguridad en 2022, los encuestados indicaron que generalmente preferirían la promoción interna (30 %) a conseguir un nuevo trabajo (15 %); esto se compara con mudarse a un nuevo campo dentro de la ciberseguridad (12 %), convertirse en un contratista independiente (6 %) o iniciar un negocio (6 %)

Certificaciones

Las certificaciones están evolucionando como un instrumento para el crecimiento de habilidades, a diferencia de una plataforma de lanzamiento de carrera. El 96 % de los encuestados de nuestra muestra obtuvo al menos un tipo de certificación. En el pasado, la mayoría de los profesionales de ciberseguridad eligieron las certificaciones como un medio de progresión profesional y desarrollo profesional (53 %). El principal impulsor para obtener certificaciones en el futuro está impulsado por la necesidad de mejorar sus habilidades (64 %) y mantenerse al día con las tendencias de ciberseguridad (53 %).
Aquellos empleados con un año de experiencia o menos en su organización están aún más ansiosos por utilizar las certificaciones como un medio para mejorar sus habilidades (69 %) frente a aquellos que han estado en sus empresas durante más de dos años (62 %)
El 89 % de nuestros encuestados afirmó que obtuvo al menos una certificación independiente del proveedor, por ejemplo, (ISC)2 , ISACA o CompTIA, o del proveedor, por ejemplo, Microsoft, Amazon, CISCO.
El 50 % de los encuestados obtuvo una certificación de proveedor neutral en los últimos tres años frente al 52 % que obtuvo una de un proveedor en el mismo período de tiempo.

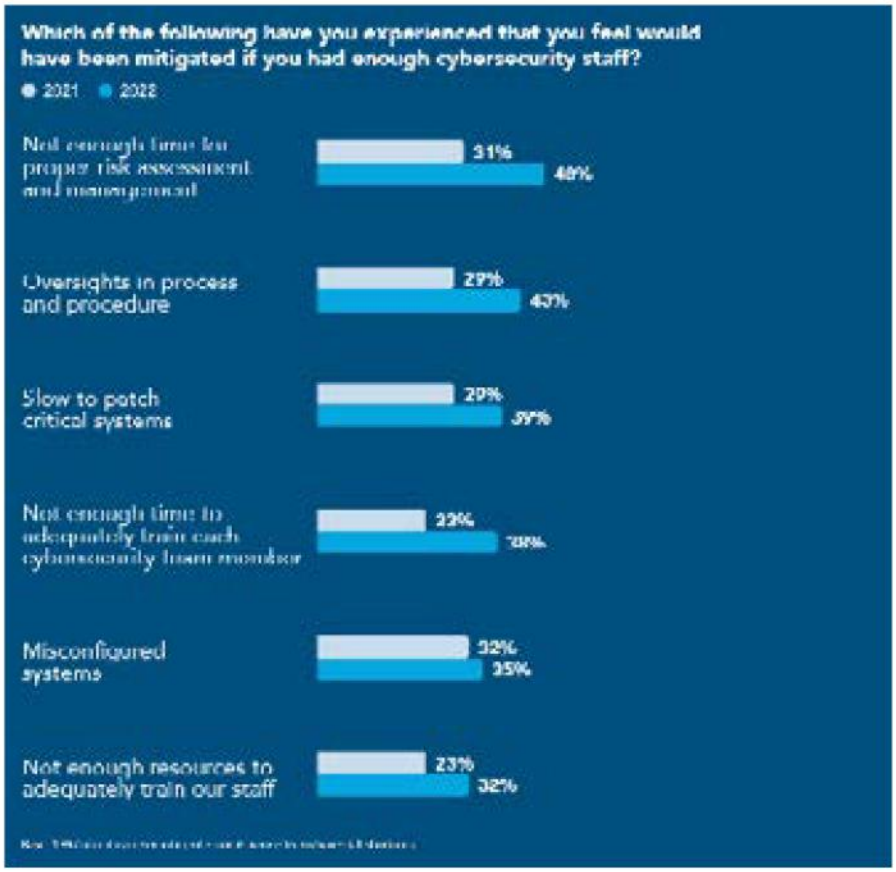
Cómo impacta esto en las organizaciones

La fuerza laboral está cambiando de abajo hacia arriba, y hemos observado que la próxima generación de empleados de seguridad cibernética está reemplazando las expectativas tradicionales con nuevos caminos y conjuntos de habilidades obtenidos de una amplia gama de antecedentes educativos, experiencias y certificaciones.
Reclute para una gama más diversa de habilidades y perspectivas. Ampliar los esfuerzos de contratación de su equipo más allá de aquellos con experiencia en TI es una oportunidad para mejorar su estrategia de mitigación de riesgos.
Certificaciones: utilícelas como constructores de carrera, no como barreras.
Esta tendencia ya ha comenzado, con más de la mitad de las organizaciones ofreciendo reembolsos por certificaciones de terceros y otras simplificando sus requisitos en torno a certificaciones específicas de proveedores; esto representa una disminución del 55 % en 2021 al 38 % en 2022. Casi la mitad de los empleados menores de 30 años son ingresar a la profesión de ciberseguridad con antecedentes fuera de la industria de TI.

Futuro del trabajo de ciberseguridad

Los desafíos futuros tienen sus raíces en la tecnología emergente, el panorama regulatorio cambiante y la escasez de habilidades. Nuestra investigación muestra que, durante los próximos dos años, el 61 % de los profesionales de la seguridad cibernética están principalmente preocupados por los riesgos potenciales de la tecnología emergente (por ejemplo, blockchain, IA, VR, computación cuántica, etc.). Le sigue de cerca el 60 % que está preocupado por mantenerse al día con los requisitos reglamentarios (p. ej., PCI DSS v4, GDPR, regulaciones de IA, etc.) y aquellos que consideran que la escasez de trabajadores/habilidades es un riesgo continuo (60 %)

A pesar de los riesgos y las diferencias regionales, los profesionales esperan que el personal crezca a un ritmo mucho mayor en el futuro. Dentro de los próximos 12 meses, el 72% de los encuestados espera que el personal aumente un poco o significativamente. Preguntamos a nuestros encuestados en qué medida estaban de acuerdo en que su organización tiene las herramientas y las personas necesarias para responder a los incidentes de ciberseguridad en los próximos dos o tres años. Las respuestas más seguras que recibimos fueron del 66% de los profesionales de ciberseguridad que trabajan en empresas de desarrollo de software/hardware de ciberseguridad. Además, el 65 % de los encuestados que trabajan en la construcción, alimentos/bebidas/hotelería/viajes y comercio minorista/mayorista estuvieron de acuerdo o muy de acuerdo en que



cuentan con las herramientas y las personas que necesitan para mitigar los riesgos futuros. Los servicios de TI (61 %) también se encontraban entre las cinco industrias más seguras.

Conclusión

Nuestra investigación sugiere que la fuerza laboral de ciberseguridad está impulsada por la pasión por lo que hace; y tienen la mejor experiencia cuando son capaces de trazar su camino y progresión en el campo. Sin embargo, esta experiencia se diluye cuando los empleados no se sienten respaldados por los grupos para los que trabajan. Los empleados individuales necesitan el apoyo de sus equipos colectivos y organizaciones. La retención del personal sigue siendo un problema y, aunque hay optimismo sobre la contratación/reclutamiento en el futuro, las empresas deben tomar más medidas para inspirar lealtad y mitigar el desgaste.

Mostrar a los empleados que son valorados y escuchados mejorará su experiencia en el lugar de trabajo (ya sea remoto o presencial).

Descargue aquí el informe

mediaware MARKETING

Servicio 360
MARKETING Y VENTAS

Especializado en Tecnología y Consumo

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

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

mediaware.org

Enfoque basado en el riesgo para los informes de seguridad cibernética

Un informe de BitSight

Enfoque basado en el riesgo para los informes de seguridad cibernética
Un informe de BitSight
No hay duda al respecto: el panorama actual de la ciberseguridad está evolucionando más rápido que nunca. Desde la migración en curso a la nube hasta el cambio generalizado al trabajo remoto, hay una variedad de factores que hacen que la superficie de ataque de su empresa se expanda rápidamente, lo que lo expone a riesgos cibernéticos nuevos y cambiantes, al tiempo que hace que sea cada vez más difícil obtener una visibilidad amplia y continua en sus activos críticos.
Al mismo tiempo, se le asigna la tarea de cumplir con las expectativas cambiantes de su rol con tiempo y recursos cada vez más limitados.
La comunicación efectiva entre los diferentes niveles de una organización de seguridad cibernética, desde los profesionales hasta los gerentes, el C-suite y el board, puede marcar la diferencia entre los sistemas seguros y los incidentes masivos. Y los informes, lejos de ser un trámite o un trabajo pesado, son el mecanismo central de esta comunicación.
Al adoptar un enfoque basado en el riesgo para los informes de seguridad cibernética, puede evaluar el rendimiento en función de la exposición real a las amenazas cibernéticas, proporcionar un contexto procesable, resaltar el valor de sus esfuerzos de seguridad cibernética y asegurarse de aprovechar al máximo su tiempo y recursos limitados.

INFORMES VS. ALERTAS

Una distinción importante: cuando nos referimos a informes, nos referimos a recopilaciones de datos e información recopilada por personas, no a alertas generadas automáticamente por herramientas de software.
Las alertas automáticas, aunque enormemente valiosas, no pueden sustituirse por una comunicación interpersonal real. En primer lugar, simplemente hay demasiadas alertas para tomarlas todas en serio.
En segundo lugar, las alertas generadas por las máquinas son demasiado fáciles de descartar sin que un ser humano las entienda, las traduzca a un lenguaje no técnico y las use para abogar por un cambio procesable.
En una encuesta de Imperva, el 53% de los encuestados indicó que, entre todo el ruido, el Centro de Operaciones de Seguridad (SOC) de su organización ha tenido problemas para identificar qué incidentes de seguridad son críticos. Para hacer las cosas más complejas, el SOC se estira más que nunca, y muchos equipos tienen que abordar funciones adicionales, como el soporte remoto, en nuestro entorno operativo "nuevo normal".
En muchos casos, las alertas por sí solas son insuficientes. Para tomar las alertas y convertirlas en informes procesables, los equipos de seguridad deben evaluar el contexto y tener instrucciones sobre cómo separar la señal del ruido.

¿QUÉ ES LA NOTIFICACIÓN BASADA EN RIESGO?

El contenido de los informes de ciberseguridad es muy variable

y depende de la naturaleza del informe, su creador y su destinatario. Sin embargo, hay ciertos factores que se pueden utilizar para determinar si cualquier informe de ciberseguridad es efectivo:

-¿Transmite el informe información procesable en contexto?

-¿Es el informe lo suficientemente conciso para que los hallazgos clave no queden enterrados?

- ¿Es el lenguaje del informe lo suficientemente claro para que lo entienda una audiencia no técnica?

-¿El informe relaciona los hallazgos con el riesgo cibernético?

Cuando las organizaciones carecen de informes internos significativos sobre seguridad cibernética, generalmente se puede atribuir a la falta de cumplimiento de uno o más de los criterios enumerados anteriormente.

Es más probable que se pasen por alto los informes que brindan números sin información o contexto, especialmente si el lector no tiene las habilidades o el conocimiento para sacar conclusiones de los datos. Los informes que contienen demasiada información o información que es demasiado técnica pueden causar frustración, lo que lleva a los lectores a desear tener "un traductor de mano, como el que usan en Star Trek", como dijo un alto ejecutivo.

Entre estos componentes, el último: ¿relaciona el informe los hallazgos con el riesgo cibernético?, puede ser el más importante. Esta pregunta constituye la base de un enfoque de información basado en el riesgo. Los informes de seguridad cibernética basados en el riesgo, a diferencia de los informes integrales, basados en el cumplimiento o basados en incidentes, son el enfoque más adecuado

para reducir la exposición real de una organización a las amenazas cibernéticas.
Seguir un enfoque basado en el riesgo para los informes de seguridad cibernética puede ayudar a las personas y los equipos en todos los niveles de una organización a concentrarse en los problemas más importantes sin ser víctimas de la fatiga de alertas y las advertencias ignoradas.
¿Qué aspecto tienen los informes de ciberseguridad basados en riesgos?
Hay muchas formas de practicar la elaboración de informes basados en el riesgo, pero las siguientes recomendaciones pueden ayudar a su organización a lograrlo.
- Coloque los elementos de mayor riesgo al frente y al centro del informe.
- Asigne una "puntuación de riesgo" a los hallazgos o recomendaciones clave.
- Ponga los hallazgos en contexto comparando las métricas con el desempeño anterior, los pares y los competidores.
- Enmarcar el riesgo en términos comerciales para ayudar a los ejecutivos y líderes
- Una guía práctica para la elaboración de informes de ciberseguridad basados en el riesgo para comprender las ramificaciones de los hallazgos.

PISTAS DE CONTEXTO

Las métricas presentadas en el vacío rara vez son procesables. ¿Qué significa, por ejemplo, que su firewall haya detenido 1.500 intrusiones este mes? ¿Es eso mucho o poco?
Un informe de ciberseguridad basado en el riesgo ofrece hallazgos en contexto, lo que ayuda al destinatario a comprender qué papel juega un número en el panorama general de riesgos de la organización. Este contexto puede incluir cualquiera de los siguientes:
Desempeño pasado: ¿Cómo fueron estos mismos números el mes pasado o el último trimestre? ¿Estás mejorando o empeorando con el tiempo?
Concentración de riesgos: ¿Cómo se están desempeñando las diferentes unidades de negocios y subsidiarias en su organización?
Puntos de referencia de la industria: ¿Cómo se compara su desempeño con el de sus pares y competidores?
Cuantificación financiera: ¿Qué está en juego financieramente con su postura de riesgo actual?
Marcos de seguridad cibernética: ¿Cómo se alinean sus hallazgos con los marcos de seguridad cibernética para su industria, como el marco NIST para mejorar la seguridad de la infraestructura crítica, los controles de seguridad crítica CIS, ISO 27001 o PCI DSS?
Con el contexto apropiado, los profesionales, gerentes, ejecutivos y miembros de la Junta pueden tomar decisiones más seguras sobre ciberseguridad, asignando los recursos apropiados a los proyectos con mayor probabilidad de reducir el riesgo en toda la organización.

INFORMES BASADOS EN RIESGOS PARA MIEMBROS DEL BOARD

Las juntas directivas se han involucrado cada vez más en la supervisión de la seguridad cibernética durante la última década. El inicio de esta tendencia se remonta a la filtración de datos de Target en 2013, después de la cual una firma asesora recomendó que se reemplazaran siete de los diez miembros de la junta por no supervisar adecuadamente el riesgo cibernético como parte de sus funciones. Este informe marcó un cambio importante en la política de seguridad cibernética corporativa, con ejecutivos y miembros de la Junta asumiendo un papel mucho más práctico.
Como el eslabón superior en la cadena de informes de seguridad cibernética, las juntas tienen la responsabilidad de crear una cultura en la que cada eslabón posterior, desde ejecutivos hasta

gerentes y profesionales, informe sobre información procesable y basada en el riesgo cibernético real.

-Riesgo frente a cumplimiento
Para los miembros de la Junta, es imperativo comprender la diferencia entre la seguridad cibernética en lo que respecta al cumplimiento y la seguridad cibernética en lo que respecta al riesgo cibernético real.
Las juntas, al ser responsables ante los reguladores, tienen motivos para preocuparse por el cumplimiento de la seguridad cibernética. Sin embargo, a menudo hay una gran diferencia entre el cumplimiento y la verdadera seguridad. Lograr el cumplimiento y alcanzar un nivel aceptable de riesgo son objetivos discretos y deben tratarse como tales.
Con este fin, los directores deben asegurarse de que los informes de los CISO y los CIO al Directorio no se centren exclusivamente en el cumplimiento o el riesgo, sino que sigan el progreso hacia los objetivos en cada una de esas áreas.
-Creación de una cultura de transparencia
Para operar de manera efectiva, las juntas necesitan una imagen completa del riesgo cibernético de su organización, lo que a su vez requiere que los miembros

de la junta puedan confiar en la información que proviene de sus ejecutivos de seguridad cibernética.
Construir esta confianza requiere que las juntas se concentren en crear una cultura en la que nadie tenga miedo de decir la verdad sobre los problemas de seguridad cibernética, incluso si el riesgo son objetivos discretos, y esa verdad es potencialmente dañina, como un error humano que permitió que una amenaza que debía ser tratada como tal ingresara a una red o la falla de un individuo para parchear un determinado programa.
Si bien las juntas normalmente no tienen el tiempo o la experiencia para verificar puntos de datos individuales, pueden aprovechar las herramientas de monitoreo continuo, como calificaciones de seguridad, para ver de un vistazo si la información que proviene de sus ejecutivos refleja el estado real y en tiempo real del riesgo cibernético en toda la organización.
- Preguntas que las juntas deberían estar haciendo Sobre Ciberseguridad
• ¿Cuál es el estado actual del riesgo cibernético en la organización?
• ¿Cuáles son las mayores brechas en nuestros programas de ciberseguridad?
• ¿Qué estamos haciendo para cerrar estas brechas y mitigar el riesgo cibernético?
• ¿Estamos asignando recursos en función del nivel de riesgo?
• ¿Somos conscientes de las amenazas importantes que afec-

tan a nuestra industria?
• ¿Nuestra estrategia de ciberseguridad está alineada con nuestra estrategia comercial?
• Si ocurre un ataque cibernético o una violación de datos, ¿estamos preparados para responder?
• ¿Están claramente articuladas las responsabilidades del personal de ciberseguridad?

INFORMES BASADOS EN RIESGO PARA EJECUTIVOS

"Las juntas y los comités están repletos de informes, que incluyen docenas de indicadores clave de rendimiento e indicadores clave de riesgo (KRI). Sin embargo, los informes a menudo están mal estructurados, con niveles de detalle inconsistentes y, por lo general, demasiado altos. Las investigaciones indican que la mayoría de los ejecutivos de TI y seguridad usan hojas de cálculo compiladas manualmente para informar los datos de riesgo cibernético a sus directorios; Como era de esperar, muchos miembros de la junta están insatisfechos con los informes que reciben", Medición del Riesgo Cibernético y la Ciberseguridad Holística Enfoque, McKinsey, 2018

En sus informes a otros ejecutivos y juntas directivas, los ejecutivos de seguridad cibernética deben hacer el difícil trabajo de poner los conceptos técnicos en contexto para las personas no técnicas. Los informes basados en riesgos proporcionan un marco para lograr esto.

Para responder a la pregunta "¿qué significa esto?", no es necesario que los ejecutivos eduquen a sus superiores sobre la tecnología que sustenta un determinado KPI. En cambio, deben relacionar el hallazgo con el riesgo cibernético. Por ejemplo: ¿Qué significa que tenemos un número de puertos abiertos superior a la media? Significa que tenemos un 9 % más de riesgo de sufrir una filtración de datos que la empresa promedio de nuestra industria.

- Informes estratégicos

Además de agregar contexto y hacer que los informes sean menos técnicos, los ejecutivos de seguridad y riesgo pueden realizar presentaciones más atractivas para la junta directiva y otros ejecutivos al incluir un componente estratégico.

En lugar de informar estrictamente sobre la postura de seguridad cibernética actual, los ejecutivos pueden aumentar el impacto de los informes al diseñar una hoja de ruta de su visión estratégica. Al incluir sus objetivos a corto, mediano y largo plazo para la seguridad cibernética de la organización y poner las métricas de seguridad cibernética en el contexto de estos objetivos, los CIO y CISO pueden demostrar la efectividad de ciertas iniciativas.

Además, los ejecutivos de seguridad y riesgo deben tratar de poner sus informes en el contexto de la estrategia comercial general. La gestión de riesgos cibernéticos siempre debe estar alineada con el marco más amplio de gestión de riesgos empresariales de una organización. Los directores financieros, los directores ejecutivos y los miembros de la junta tomarán la información de un informe de seguridad cibernética y tratarán de comprender cómo afectará sus objetivos más amplios; los ejecutivos pueden ayudar en este proceso llegando a sus propias conclusiones e incluyéndolas en sus informes.

- Obtener los recursos adecuados

Una de las funciones principales de los informes de seguridad cibernética en este nivel es ayudar a los superiores con sus decisiones presupuestarias y de asignación de recursos. Por ejemplo, si un CISO está solicitando una nueva solución tecnológica para mejorar la ciberseguridad general, una buena Junta considerará los informes anteriores como parte de su proceso de diligencia debida.

Un problema común que surge

en este proceso es la incapacidad por parte del departamento de ciberseguridad para probar la efectividad de una solución determinada, ya sea un programa de software, una nueva contratación o alguna otra iniciativa. Históricamente, esto ha sido difícil; después de todo, aparte de algunos KPI complejos que una junta puede comprender o no, la única medida visible de la eficacia de una solución de ciberseguridad es si la organización es víctima de un ciberataque o no. La información basada en riesgos tiene el poder de revolucionar este proceso.

Usando una solución como las calificaciones de seguridad, los ejecutivos pueden rastrear los cambios en el riesgo cibernético real contra los plazos de ciertas implementaciones de soluciones.

Por ejemplo, si su organización invirtió mucho en capacitación de concientización sobre seguridad y su calificación de malware disminuyó significativamente, esa correlación se puede usar para solicitarle a la Junta una mayor inversión. Este tipo de contexto y visibilidad es más importante que nunca ya que, según los datos de BitSight, hasta el 85 % de la fuerza laboral en algunas industrias cambió al trabajo remoto en marzo de 2020.

Si bien este nuevo entorno operativo abre la red corporativa a nuevas vulnerabilidades, también requiere una variedad de nuevos tipos de inversiones para permitir que los equipos trabajen de manera segura y eficiente en casa.

- KPI que los ejecutivos pueden usar en sus informes

Los directores ejecutivos y los miembros de la junta a menudo se quejan de la naturaleza altamente técnica de los KPI de ciberseguridad. Para combatir esto, los ejecutivos pueden usar KPI como los siguientes, que son fáciles de entender o contienen un contexto integrado:

- Clasificación de seguridad
- Calificación promedio de seguridad del proveedor a lo largo del tiempo
- Calificación de seguridad promedio de la industria
- Intentos de intrusión dentro de un período dado
- Cadencia de parches
- Tiempo medio de detección
- Tiempo medio para resolver
- Frecuencia de respaldo
- Tasa de éxito de la prueba de phishing
- Puntuaciones de capacitación en concientización sobre seguridad

INFORMES BASADOS EN RIESGOS PARA GERENTES

Los administradores de seguridad y riesgos tendrán responsabilidades diferentes según sus funciones específicas y el tamaño y la estructura de sus organizaciones. Sin embargo, todos comparten una responsabilidad crítica: sintetizar la información y reportarla a la alta gerencia y ejecutivos.

Los gerentes juegan un papel único. Son responsables de hacer operativas las decisiones tomadas por el liderazgo y asignar recursos para ejecutar la estrategia. En muchas organizaciones, los gerentes pueden experimentar una desconexión entre lo que creen que su equipo necesita y lo que se le ha dado a su equipo para trabajar.

Los informes basados en riesgos pueden resolver este problema. Si un gerente puede comprender el impacto comercial que ciertos problemas tienen en el riesgo cibernético general de su organización y comunicar este impacto de manera efectiva, puede alinear más estrechamente la comprensión de sus superiores sobre la seguridad cibernética de la organización con la suya propia.

- Escoger y elegir

Un administrador de ciberseguridad podría tener acceso a miles de puntos de datos. Lo que elijan para informar puede tener un impacto en el significado que pue-

den transmitir a la cadena. Elija pasar demasiados o muy pocos datos (o datos sin contexto), y la falta de una comunicación clara podría conducir a un incidente de seguridad importante.

Para los gerentes, gran parte del trabajo de los informes basados en riesgos se reduce a elegir los indicadores de desempeño más relevantes. Este no es un llamado para seleccionar los datos para cumplir con una agenda, sino más bien para limitar la cantidad de indicadores totales informados para evitar inundar a los destinatarios y relacionar los hallazgos con el contexto más amplio de las metas y estrategias de toda la empresa y KPI. ¿Cómo debe un gerente decidir qué indicadores incluir en sus informes?: Usando una metodología de informes basada en el riesgo, los indicadores que se correlacionan más estrechamente con el riesgo cibernético real deben tener prioridad.

- Informes continuos mediante paneles

Los informes seleccionados son extremadamente importantes para garantizar que la información importante se comunique a las personas adecuadas. Sin embargo, la generación de informes es solo una pequeña entrada en una larga lista de responsabilidades de los administradores de seguridad y riesgos. Muchos gerentes simplemente estarán demasiado ocupados para compilar informes detallados con la frecuencia que les gustaría.

Ingresa al tablero. Muchas soluciones nuevas de ciberseguridad incluyen integraciones que les permiten exportar continuamente ciertos datos al software del tablero. Los gerentes ahora tienen la opción de seleccionar un tablero que la alta dirección y los ejecutivos pueden consultar siempre que deseen obtener una imagen rápida de la ciberseguridad o el riesgo. Al crear un tablero, es importante que los gerentes recuerden la importancia del contexto: los tableros deben estar alineados con los KRI y los KPI para maximizar el impacto.

Equipados con esta herramienta de referencia continua, los ejecutivos pueden tomar decisiones que consideren más de cerca las condiciones reales en el departamento de ciberseguridad.

- Tablero de Ciberseguridad

Calificación de seguridad: estas medidas sintetizadas del desempeño de ciberseguridad de una organización se actualizan continuamente.

Se ha demostrado de forma independiente que algunas clasificaciones de seguridad se correlacionan con el riesgo de violación de datos. Incluya un promedio de la industria o una meta preestablecida para agregar contexto a esta calificación.

Grados de vector de riesgo: algunas plataformas de clasificación de seguridad brindan

a los usuarios la capacidad de ver grados en vectores de riesgo específicos, como servidores de malware o cadencia de parches. Estos se pueden elegir en función de su relevancia para la función específica que se informa.
Incidentes recientes: una fuente de datos de un SIEM puede mostrar a los ejecutivos cuántas y qué tipos de amenazas se están detectando en los sistemas de una organización.
Inteligencia de amenazas: ¿Qué tipos de malware se han encontrado en los sistemas de la organización? ¿Qué amenazas están afectando a la industria en general?
Datos de capacitación de concientización sobre seguridad: el riesgo relacionado con el usuario es una de las áreas de riesgo menos abordadas en muchas organizaciones. Incluir datos que ilustren la efectividad de la capacitación de concientización (tasas de finalización, puntajes de pruebas, resultados de pruebas de phishing, etc.) puede ayudar a ilustrar su importancia.

INFORMES BASADOS EN RIESGOS PARA PRACTICANTES

Para las personas encargadas de realizar el trabajo práctico real de mitigar el riesgo cibernético en una organización, la vida diaria es una serie constante de decisiones de asignación de recursos. Y en nuestro entorno operativo de "nueva normalidad", tomar estas decisiones puede ser más difícil que nunca. Después de todo, muchos profesionales de la ciberseguridad están asumiendo nuevas responsabilidades, como el soporte general de TI, mientras enfrentan el desafío de trabajar con presupuestos cada vez más reducidos. Tener el tiempo de uno atado a un proyecto significa necesariamente una incapacidad para trabajar en otro.
-Pronóstico del éxito
Los profesionales pueden utilizar informes basados en riesgos para demostrar su eficacia y ayudar a sus gerentes a decidir dónde se necesitan más sus habilidades.
Uno de los mejores métodos para generar informes basados en riesgos a nivel profesional es la previsión, que puede identificar el curso de acción óptimo para mejorar su postura de riesgo de ciberseguridad modelando diferentes escenarios y rutas de remediación. Armado con estos conocimientos, es más fácil que nunca obtener respuestas a preguntas difíciles pero importantes sobre dónde gastar los presupuestos de seguridad, qué conjuntos de actividades reducirán el riesgo más rápidamente y si se deben cambiar las implementaciones de tecnología.
Al demostrar que el impacto evitará que la organización alcance sus objetivos de riesgo establecidos, el profesional puede argumentar con éxito que la seguridad del correo electrónico debe seguir siendo una prioridad.

CONCLUSIÓN

En un panorama de riesgo cibernético definido por infracciones de alto perfil y amenazas en constante evolución, todos los tipos de organizaciones deben analizar detenidamente el estado de su comunicación interna. Y ahora, dado que las empresas trabajan con una fuerza laboral cada vez más remota, tener conversaciones claras y basadas en datos sobre el riesgo cibernético nunca ha sido más importante. Ya se han aprendido las lecciones de que la mala comunicación puede conducir a incidentes devastadores: es hora de que los líderes tomen esas lecciones en serio.
Los informes de ciberseguridad basados en riesgos son el mejor mecanismo para mejorar la comunicación interna sobre ciberseguridad y desarrollar una estrategia de gestión del rendimiento de la seguridad verdaderamente eficaz.

Cómo convertir una estrategia de ciberseguridad en realidad

Un marco holístico de gestión del rendimiento. Cómo convertir una estrategia de ciberseguridad en realidad. Por Kaustubh Wagle, Shoaib Yousuf, Yasser Alswailem, Mohammed Almengash, and Fatimah Alturkistani, para BCG -Boston Consulting Group.

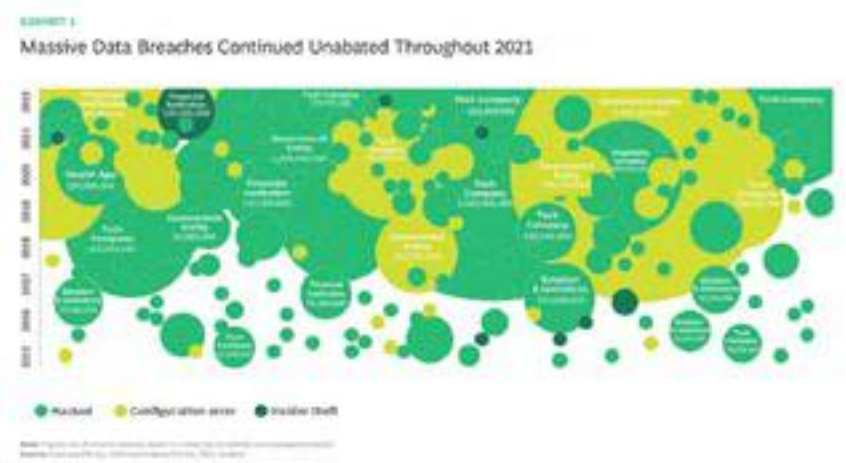
La frecuencia y el costo de los ataques cibernéticos se está acelerando. A nivel mundial, se estima que el costo del delito cibernético aumentó de u$s 445 mil millones en 2015 a más de u$s 2,2 billones en la actualidad. La frecuencia y el tamaño de las violaciones de datos están creciendo exponencialmente en todas las industrias (Gráfico 1). En 2021, organizaciones líderes en casi todos los sectores informaron ataques importantes, incluidas empresas tecnológicas, automotrices y entidades gubernamentales.

Mientras tanto, los avances en IA e Internet de las cosas (IoT), combinados con la adopción acelerada por la pandemia de arreglos de trabajo flexibles y la digitalización generalizada de las organizaciones, han aumentado exponencialmente tanto nuestra dependencia de la ciberseguridad (CS) como el potencial de ataques. La transición a 5G introduce otra gama completa de vulnerabilidades peligrosas relacionadas con el software.
Según el Instituto Brookings, "las redes y los servicios esenciales que definen nuestras vidas, nuestra economía y nuestra seguridad nacional nunca habían tenido tantos participantes, cada uno dependiente del otro, y ninguno de los cuales tiene la responsabilidad final de la seguridad cibernética".
Mirando hacia el futuro, la computación cuántica, que puede generalizarse en tan solo 5 a 10 años, dejará obsoletos los estándares de cifrado actuales, con importantes implicaciones adicionales para la ciberseguridad.
La ciberseguridad se ha convertido en una prioridad crítica de gestión de riesgos para las organizaciones del sector público y privado por igual. El gasto en seguridad de la información y tecnología de gestión de riesgos ha aumentado drásticamente y se estima que alcanzará los 168.000 millones de dólares a finales de 20222. La competencia por el escaso talento es feroz: Se estima que 3,5 millones de puestos de trabajo en ciberseguridad en todo el mundo quedarán vacantes este año.
En este contexto, los directores ejecutivos, las juntas directivas y los accionistas están ansiosos por comprender la efectividad y el valor de su inversión en seguridad cibernética y su contribución general al negocio.
Un artículo reciente de Gartner enumeró las siguientes "cinco preguntas de seguridad que definitivamente hará su Junta", así como su justificación subyacente y cómo podría responder un líder de seguridad:
-Incidente: ¿Cómo sucedió esto? ¿Pensé que tenías esto bajo control? ¿Qué salió mal?
-Compensación: ¿Parece que estamos 100% seguros? ¿Está seguro?
-Paisaje: ¿Qué tan malo es ahí afuera? ¿Qué pasa con lo que pasó en la empresa X? ¿Cómo nos va en comparación con los demás?
-Riesgo: ¿Sabemos cuáles son nuestros riesgos? ¿Qué te mantiene despierto en la noche?
-Desempeño: ¿Estamos asignando adecuadamente los recursos? ¿Estamos gastando lo suficiente? ¿Por qué gastamos tanto?
Ante tales preguntas, los CISO

deben poder evaluar e informar sobre la madurez de su programa de seguridad cibernética en función de los riesgos y resultados de alto nivel y demostrar a los miembros de la Junta cómo se está desempeñando su organización en comparación con su industria y sus pares. Discutir los riesgos con los altos ejecutivos también ha demostrado ser un desafío, en ausencia de un lenguaje común que puedan entender tanto las partes interesadas técnicas como las no técnicas.

El problema para los CISO es que estas partes interesadas generalmente carecen del conocimiento técnico necesario para comprender los detalles de las iniciativas de seguridad cibernética, incluso a nivel de la Junta. Las métricas de seguridad altamente técnicas deben resumirse en información precisa, fácil de entender y relevante para el negocio para la administración, la Junta y las reuniones de accionistas. Aquí es donde la gestión del rendimiento de la ciberseguridad puede ayudar.

La gestión del desempeño de la ciberseguridad es un proceso para evaluar la madurez de su programa de ciberseguridad, vinculando sistemáticamente múltiples niveles de riesgo, métricas, inversiones y retornos. Cuando forman parte de un



proceso continuo y coherente, estas mediciones dinámicas basadas en datos son indicadores valiosos de la postura de ciberseguridad de una organización.

Establecer un programa de gestión del desempeño de la seguridad cibernética ayuda a establecer una línea de base y priorizar lo que es importante para el negocio, asegurando la alineación con los objetivos organizacionales y el apetito por el riesgo, mejorando la visibilidad y logrando mejores resultados de su inversión en seguridad. Medir el desempeño de la seguridad cibernética a través de una variedad de métricas relevantes permite a las organizaciones enfocarse en mejoras, reduciendo la vulnerabilidad a través de acciones correctivas.

La gestión del rendimiento de la ciberseguridad permite a los CIO y CISO responder a las preguntas anteriores, además de:

- ¿Cómo nos estamos desempeñando frente a nuestro(s) marco(s) de control de ciberseguridad adoptado(s)?
- ¿Cuál es nuestro nivel de madurez actual?
- ¿Estamos haciendo las inversiones adecuadas? De no ser así, ¿dónde es necesario aumentar las inversiones y por qué?
- ¿Cuál es nuestra inversión futura ideal en términos de tasa de ejecución en ciberseguridad?
- ¿Cuánto riesgo tendremos una vez que se alcance nuestra tasa de ejecución?

A partir de 2019, Saudi Telecom Company (stc) se asoció con Boston Consulting Group (BCG) para introducir un marco sólido de gestión del desempeño de la ciberseguridad como parte

EXHIBIT 2

Top- Down Approach for Performance Management

de un programa de transformación de la ciberseguridad más amplio. Su propósito era rastrear el progreso y el impacto de la ejecución del programa al tiempo que proporcionaba una imagen completa de la madurez de la ciberseguridad de stc. El marco ha sido implementado, revisado y mejorado durante los últimos tres años y ha permitido a stc realizar con éxito su estrategia de ciberseguridad. En este documento, stc y BCG desean compartir la experiencia y las lecciones aprendidas a lo largo de este viaje.

Marco de Gestión del Desempeño

Dé forma a la práctica de ciberseguridad y establezca la dirección

Un marco de gestión del desempeño efectivo se deriva de la estrategia de seguridad cibernética, que a su vez está impulsada por la visión y la misión del programa CS. La visión y la misión de la ciberseguridad juegan un papel fundamental en la comunicación del propósito de la ciberseguridad a las partes interesadas, el desarrollo de una estrategia de CS y la medición de su desempeño y éxito. Alinear la dirección de la ciberseguridad con la estrategia comercial es extremadamente importante para reflejar el contexto interno y externo, mitigar los riesgos y habilitar el negocio.

Un marco sólido de gestión del desempeño se define de arriba hacia abajo. Los indicadores clave de rendimiento (KPI) y las métricas se derivan de iniciativas para lograr objetivos estratégicos relacionados con áreas de enfoque y capacidades de CS (por ejemplo, riesgo, gobierno, cumplimiento, defensa) que dan forma a la práctica de seguridad cibernética y aseguran la alineación comercial.

Cuantificación de la postura y madurez de la ciberseguridad

Si bien la mayoría de las organizaciones son conscientes de los riesgos cibernéticos, la madurez del programa de seguridad cibernética es desigual. Es de vital importancia para las organizaciones tener una comprensión precisa de dónde están y cuál es la mejor manera de mejorar. El desempeño robusto de la ciberseguridad comienza con un marco bien definido que permite a las organizaciones elevar y comparar el desempeño en una amplia gama de capacidades de CS, incluida la estrategia, la alineación comercial, los modelos operativos, la gobernanza, el riesgo, el cumplimiento, la defensa, etc.

En 2019, con soporte de BCG, stc estableció un Marco de

Ciberseguridad detallado. El marco identifica 30 iniciativas para dar forma a las prácticas de ciberseguridad y establecer la dirección, hacer cumplir la estrategia, desarrollar capacidades de CS y asegurar el negocio. Refleja los estándares internacionales y las mejores prácticas de NIST, ISO 27001 y Gartner. Junto con el marco, se estableció y definió un modelo de madurez personalizado (Anexo 3), que muestra los niveles de madurez para cada capacidad de ciberseguridad. El modelo se utiliza en las evaluaciones de verificación de estado para determinar la línea de base, así como los objetivos anuales progresivos para la madurez de la ciberseguridad.

La gestión y la medición del desempeño de la seguridad cibernética deberían permitir que los CISO generen automáticamente tableros visuales dinámicos para que los utilicen la junta directiva, el equipo ejecutivo y las operaciones de seguridad. Además de proporcionar una imagen de los riesgos y el rendimiento actuales, los tableros cuidadosamente construidos se vinculan con objetivos estratégicos y de madurez a más largo plazo, destacando las brechas y los requisitos de inversión y las responsabilidades.

EXHIBIT 3

Levels of Cybersecurity Maturity

Definir la gestión y las métricas del rendimiento de la ciberseguridad

stc adoptó una estrategia de seguridad cibernética y desarrolló su marco de gestión del desempeño con la asistencia de BCG, como parte de un esfuerzo mayor para transformar y avanzar en la madurez de sus capacidades de seguridad cibernética. El marco de gestión del rendimiento mide el éxito a través de tres conjuntos de métricas, cada una centrada en un aspecto diferente del rendimiento. Del más granular al más estratégico:

El índice de ejecución rastrea la implementación de iniciativas estratégicas. Responde a la pregunta: ¿vamos por buen camino?

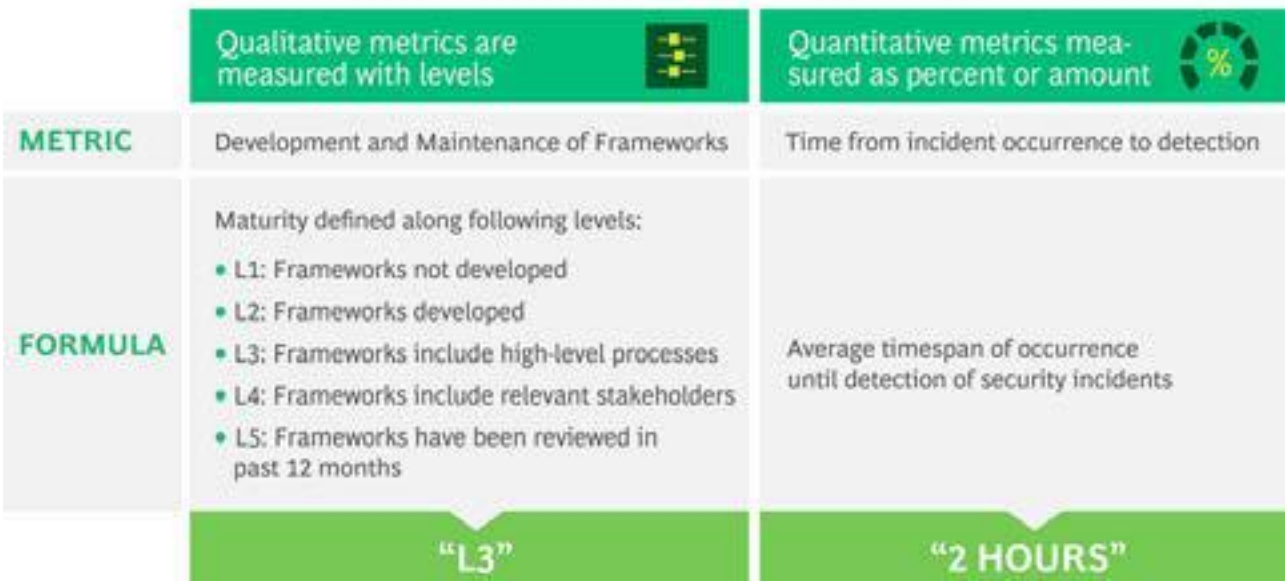
El índice de madurez mide los avances en las capacidades de seguridad. Responde a la pregunta: ¿estamos mejorando?

Los KPI transformacionales monitorean el impacto de cumplir con nuestros objetivos estratégicos hacia una organización de seguridad más sólida. Responden a la pregunta: ¿estamos logrando un impacto en el negocio?

Cada métrica de rendimiento se compone de conjuntos conectados de KPI. Los KPI son los indicadores críticos del progreso hacia un resultado previsto. Proporcionan un enfoque para la mejora estratégica y opera-

EXHIBIT 4

Qualitative vs. Quantitative Metrics Example



tiva, crean una base analítica para la toma de decisiones y ayudan a mantener la atención en lo que más importa. Como dijo Peter Drucker, "lo que se mide, se hace".

Dentro del marco de gestión del desempeño, cada iniciativa de estrategia de seguridad cibernética se traduce en KPI de madurez, que luego se agregan en un índice de madurez para el programa de seguridad cibernética en todas las iniciativas. El nivel de madurez por iniciativa se calcula agregando los niveles de madurez individuales de sus KPI. Por ejemplo, 'Arquitectura de seguridad' es una iniciativa que puede incluir KPI de madurez en torno a la arquitectura de la red, la arquitectura de la aplicación y la arquitectura del punto final. Otro ejemplo es 'Protección de puntos finales', que podría traducirse en KPI relacionados con una suite de protección de puntos finales, una solución DLP y la integración del Centro de ciberdefensa (CDC).

Todos los KPI se basan en mediciones. Pueden ser cualitativos o cuantitativos, con métricas cualitativas reportadas como palabras en niveles, declaraciones y letras y las cuantitativas reportadas como números, incluyendo proporciones y proporciones. Por ejemplo, 'Desarrollo y Mantenimiento de Marcos' es un KPI cualitativo, medido en términos de niveles de madurez: Marcos L1 no desarrollados, Marcos L2 desarrollados, Marcos L3 incluyen procesos de alto nivel, Marcos L4 incluyen partes interesadas relevantes y Marcos L5 han sido revisado en los últimos 12 meses.

Los propietarios de métricas cualitativas deben proporcionar pruebas de finalización para garantizar una medición objetiva, como el marco revisado en los

últimos 12 meses, la alineación validada o los cambios implementados y documentados. El tiempo desde la ocurrencia del incidente hasta la detección es un KPI cuantitativo, medido por el tiempo promedio de ocurrencia hasta la detección de incidentes de seguridad.

Implementando el Nuevo Enfoque

Al igual que con tantos programas de transformación, la implementación fue clave para el éxito de la estrategia de ciberseguridad de stc. En esta sección, compartimos lo que funcionó para stc: algunas decisiones que valieron la pena y las lecciones aprendidas en el camino.

El apoyo ejecutivo es fundamental

El apoyo ejecutivo es el factor clave de éxito más importante. La gestión efectiva del desempeño de la ciberseguridad depende de la voluntad de los ejecutivos de priorizar, reforzar y participar de manera continua en los esfuerzos de mejora de la ciberseguridad. No es solo la tecnología la que debe cambiar, sino el comportamiento de las personas en toda la organización, y eso requiere el compromiso del liderazgo. Los ejecutivos pueden demostrar su apoyo de varias maneras, por ejemplo:

- Participando en el desarrollo de KPIs que conectan la visión y estrategia de negocio con el desempeño en ciberseguridad.
- Educarse a sí mismos y a la Junta para que puedan hacer mejores preguntas y tomar decisiones comerciales que se alineen con los objetivos de ciberseguridad.
- Invertir los recursos necesarios para cumplir con los objetivos de madurez de ciberseguridad.
- Alentar a los dueños de negocios a involucrarse y alinearse en torno a sus KPI y objetivos de ciberseguridad.

Comience con su estrategia de ciberseguridad

La estrategia es el punto de partida para lograr un valor comercial real de un programa de ciberseguridad. La estrategia de ciberseguridad incluye visión, misión, objetivos estratégicos, iniciativas estratégicas, KPI y métricas. Su alineación con la estrategia corporativa y el plan de inversiones es crucial; La ciberseguridad es un habilitador comercial clave a medida que las organizaciones se vuelven cada vez más grandes consumidoras de tecnología y datos. Busque KPI que vinculen la estrategia de ciberseguridad con los objetivos estratégicos corporativos.

Asegúrese de que su estrategia de ciberseguridad no sea solo un documento estático, sino que incluya un proceso definido para la ejecución y el seguimiento de resultados. Especialmente porque está vinculado a la gestión del desempeño, este es un esfuerzo continuo. stc descubrió que la clave del éxito era mantener el progreso encaminado y eliminar los obstáculos de manera oportuna, por lo que integrar ese proceso en el desarrollo de la estrategia evitará retrasos posteriores.

Elija y defina los KPI correctos

Desarrollar indicadores clave de rendimiento puede ser complicado. Los KPI deben estar bien definidos y ponderados de acuerdo con los objetivos críticos o centrales del negocio. El Anexo 4 ilustra el enfoque de stc para definir los KPI. El titular no es suficiente. stc creó una tarjeta para cada KPI que resume su nombre, ID, afiliación a la iniciativa, propietario, frecuencia de medición, fuente de datos, descripción y justificación, fórmula de medición, nivel de rendimiento, objetivo y ponderación del índice. Además de hacer que CS y las partes interesadas del negocio piensen en los detalles de cada KPI, las tarjetas aumentan la confiabilidad del seguimiento y brindan

una consistencia importante en diversos KPI.
- Nombre de KPI: refleja lo que este KPI debe medir en un lenguaje fácil de entender
- ID de KPI: código de identidad único que se utilizará en el catálogo de KPI
- Iniciativa: nombre de la iniciativa que se vincula a este KPI
- Propietario: persona responsable de proporcionar métricas de KPI al Equipo de Gestión del Desempeño junto con evidencia
- Frecuencia de medición: ciclo de informes para el KPI: puede ser mensual, trimestral o anual
- Fuente de datos: herramienta o método acordado para proporcionar evidencia de la métrica de KPI informada, posteriormente validada por el Equipo de Gestión del Desempeño
- Justificación y descripción: explique el KPI en sí y por qué es importante
- Fórmula: cómo calcular el valor de KPI
- Nivel de desempeño: escala para definir diferentes niveles de madurez, para ser evaluados contra el objetivo establecido
- Objetivos: nivel de madurez esperado que se logrará, generalmente aumentando con el tiempo
-Peso: si tiene un KPI que tiene sub-KPI, la ponderación se asigna a través de los sub-KPI proporcionalmente según la importancia y la contribución.

Garantice un proceso claro para la recopilación y validación de KPI

clave para un programa efectivo en curso

stc estableció un equipo de gestión del rendimiento formal responsable de identificar los KPI, recopilar informes y validar datos. Los informes de KPI se recopilan en función de su ciclo definido (mensual, trimestral, anual) o por solicitud específica de la gerencia. Los propietarios de KPI proporcionan valores actuales al equipo de gestión del rendimiento, incluida la evidencia relevante para garantizar la transparencia sobre cómo se derivaron los valores y corroborar los valores proporcionados. Esta clara rendición de cuentas (propietarios de KPI, equipo de gestión del rendimiento) es clave para un programa efectivo y continuo.

Luego, el equipo de rendimiento valida los valores. Si la evidencia proporcionada no se corresponde con los valores enviados, solicitan al propietario del KPI que vuelva a enviarla. Hay dos niveles generales de validación para cada KPI:

Nivel 1: Precisión de la fuente de datos. Asegurarse de que la evidencia enviada sea de la fuente de datos identificada en la definición de KPI.

Nivel 2: Consistencia de los da-

tos. Asegurarse de que la evidencia respalde y sea consistente con el valor asignado. Por ejemplo, si la métrica cualitativa dice "los marcos se han revisado en los últimos 12 meses", entonces el registro de documentación debe mostrar los cambios durante los últimos 12 meses.

Después de validar los datos, el equipo de gestión del rendimiento agrega todos los valores recopilados en el tablero para informar a la gerencia.

Utilice el análisis de tendencias para realizar un seguimiento del rendimiento de la ciberseguridad a lo largo del tiempo frente a los objetivos de madurez

Una vez que se completa la etapa de validación y se aceptan los valores enviados para el ciclo, comienza el análisis, comparando los valores reales de KPI con sus objetivos. Este es esencialmente el paso que nos lleva de la medición del desempeño a la gestión del desempeño.

Los informes de análisis de tendencias deben capturar cualquier desviación importante del objetivo de madurez de ciberseguridad del KPI o de las iniciativas de ejecución de la estrategia de ciberseguridad. Luego, los resultados se proporcionan a la alta dirección, que puede evaluar estas tendencias frente a los objetivos de ciberseguridad y los objetivos estratégicos.

EXHIBIT 5

Sample KPI Card: Development and Maintenance of Frameworks

Monitoreo, Revisión y Mejoras Continuas de Métricas de Ciberseguridad

Informes periódicos y reuniones de comités

Las mediciones de KPI de ciberseguridad y los niveles de madurez a los que se agregan son información importante para la toma de decisiones de CISO. Pero también deben compartirse más allá del departamento de seguridad cibernética e incorporarse en las revisiones del cuadro de mando integral del liderazgo. Esto debería ocurrir al menos trimestralmente o, más comúnmente, mensualmente según las necesidades de la organización. Especialmente cuando una organización está tratando de rastrear los efectos de un cambio importante, o en otras situaciones donde se necesita una retroalimentación rápida, los informes deben generarse y compartirse mensualmente. Permiten a los líderes empresariales monitorear los problemas de rendimiento y brindar soporte oportuno.

stc utiliza dos informes principales de rendimiento de ciberseguridad:

Informe de Alto Nivel de Métricas de Desempeño de Ciberseguridad. Indicadores seleccionados, incluido el puntaje general del nivel de madurez junto con los

puntajes de madurez para cada iniciativa estratégica. Esto le da a la alta dirección el "panorama general" del desempeño de la seguridad cibernética.
Informe detallado de métricas de rendimiento de ciberseguridad. Utilizado junto con el informe de alto nivel, este informe más detallado incluye puntajes de nivel de madurez y análisis para cada KPI, desglosado por iniciativa y departamento. Este informe generalmente lo utiliza la alta dirección de ciberseguridad, en discusión con los propietarios de KPI.
Un Comité de Gestión del Desempeño (PMC) de seguridad cibernética es responsable de monitorear el desempeño y guiar la ejecución de las Operaciones y Estrategias Cibernéticas. Usando el informe detallado de métricas de desempeño de ciberseguridad como su principal fuente de referencia, este comité se reúne mensualmente para:
- Revise los KPI de cada departamento (KPI de la unidad de estrategia y función)
- Valide los KPI y confirme que siguen siendo adecuados para su propósito
- Supervise el estado de ejecución de las iniciativas estratégicas y los hitos objetivo
- Resalte y aborde las dependencias y desafíos multifuncionales

-Proporcionar apoyo según sea necesario
- Realinear, actualizar y mejorar la dirección estratégica del sector y la excelencia operativa Supervise los riesgos de ejecución de la estrategia y asegúrese de que se consideren los pasos de mitigación adecuados
-Mejore la ejecución estratégica y operativa, actualizando proyectos, tareas, procesos y procedimientos según sea necesario
- Aprobar cualquier solicitud de cambio de KPI

Gestión de cambios de KPI de ciberseguridad

Los índices de madurez se utilizan para medir la postura de seguridad general de la organización. Siguiendo el principio de "obtienes lo que mides", es importante elegir las métricas correctas y ajustarlas si es necesario. Especialmente en el primer año de operación, o cuando las condiciones cambian rápidamente, el enfoque debe ser lo suficientemente flexible para adaptarse al aprendizaje de la experiencia. No es necesario esperar hasta el final de un ciclo de mejora. Los KPI pueden ajustarse durante el año si es necesario, por ejemplo, si:
- Los mandatos o la estructura de ciberseguridad han cambiado
- Se han publicado nuevas regulaciones
- Se necesitan nuevas capacidades.

El KPI existente o su definición no está dando la información necesaria

Para ajustar un KPI, stc requiere que su propietario complete una Solicitud de cambio (CR), incluida la justificación del cambio. Una vez que el gerente del propietario del KPI aprueba la solicitud, pasa al equipo de gestión del rendimiento de ciberseguridad para su revisión y comentarios. Finalmente, después de que el propietario del KPI y el equipo de gestión del desempeño estén alineados, el PMC debe aprobar el CR.
Además de los cambios ad hoc del tipo mencionado anteriormente, una organización debe incluir revisiones y mejoras periódicas de las métricas en su proceso de gestión del desempeño de la seguridad cibernética. Tal revisión podría cubrir el fundamento, la fórmula, los objetivos y el ciclo de informes de cada KPI.

Descubriendo los Beneficios

Las empresas de todo el mundo están redoblando su enfoque en la ciberseguridad como una capacidad crítica para el negocio. Cada vez más, están reconociendo la necesidad de enfoques holísticos, integrados con su estrategia y objetivos comerciales. Desde que presentó su estrategia de ciberseguridad y su programa de gestión del desempeño en 2019, stc ha visto una serie de beneficios que incluyen:
Una estrategia de ciberseguridad integral que crea capacidades, fortalece los controles básicos, implementa controles avanzados y agudiza el monitoreo.
Gestión robusta del rendimiento de la ciberseguridad que juega un papel importante en la elevación de la madurez de la ciberseguridad, mejorando la responsabilidad y la propiedad de las tareas.
Mayor madurez en ciberseguridad y alineación de la estrategia en las subsidiarias del grupo. (stc amplió el apoyo y la orientación a las subsidiarias para implementar la estrategia de seguridad cibernética y medir sus capacidades de seguridad cibernética a través de paquetes de rendimiento personalizados para cada subsidiaria).
Con aumentos dramáticos en el ritmo, la frecuencia y el costo de los ataques cibernéticos, las empresas buscan aprender unas de otras, identificando y adaptando las mejores prácticas para moverse más rápido y adelantarse a las amenazas en evolución.

2022: El año de la voz del CISO

Un informe de ProofPoint

Después de un año de una interrupción sin precedentes, los CISO de todo el mundo pasaron 2021 enfrentándose a nuevas formas de trabajar. Pero después de haber superado la prisa inicial por implementar configuraciones híbridas y en la nube y mantener el negocio como de costumbre, muchos ahora parecen sentirse más en control de su entorno.

La lucha contra incendios ad hoc ha sido reemplazada por una estrategia más coherente. Se han introducido nuevas políticas, módulos de capacitación y controles técnicos, todos diseñados para los equipos más distribuidos y dependientes de la nube de hoy.

Como resultado, menos de la mitad de los CISO encuestados (48 %) sienten que su organización está en riesgo de sufrir un ciberataque significativo en los próximos 12 meses, en comparación con el 64 % del año pasado.

La creciente familiaridad con el entorno de trabajo posterior a la pandemia también ha hecho que los CISO se sientan más equipados para hacer frente a las ciberamenazas. Si bien el 66 % creía que no estaba preparado para un ataque dirigido en 2021, se redujo al 50 % este año.

Pero sentirse preparado o en riesgo de un ciberataque es completamente diferente a estar preparado. En la mayoría de los casos, esta creciente confianza de los CISO es probablemente el resultado de superar con éxito un evento sísmico en lugar de cualquier cambio tangible en los niveles de riesgo o preparación.

Además, el hecho es que la mitad de los CISO globales no creen que su organización esté lista para detectar, disuadir y recuperarse de un ataque cibernético. En el Reino Unido y Alemania, esta cifra sube a alrededor de dos tercios. Y en Australia, más de las tres cuartas partes dicen que su organización no está preparada.

También existe una desconexión preocupante entre el riesgo percibido y la preparación.

Muchos CISO aparentemente son conscientes del problema, pero no pueden o no quieren implementar una solución efectiva mientras luchan por identificar cuál de las muchas amenazas comunes es probable que ataque.

Ataques desde todos los ángulos

A medida que el panorama de amenazas continúa creciendo y evolucionando, una vez más preguntamos a los CISO sobre los métodos de ciberataque que los mantienen despiertos por la noche. Al igual que el año pasado, los resultados demuestran una preocupante falta de visibilidad de las amenazas a las que se enfrentan.

Las amenazas internas negligentes, accidentales o criminales (31 %), el compromiso del correo electrónico empresarial (BEC) (30 %), el compromiso de la cuenta en la nube (30 %) y los ataques distribuidos de denegación de servicio (DDoS) (30 %) lideran el camino. Mientras tanto, la preocupación por el ransomware aumentó solo 1 punto porcentual desde el año pasado, a pesar de varios ataques de perfil increíblemente alto en los últimos 12 meses.

Por supuesto, no hay nada de malo en una cautela general ante una variedad de amenazas. Pero cuando los equipos de seguridad no están seguros de dónde provendrá el próximo ataque, es casi imposible apuntar a las protecciones y la capacitación donde más se necesitan.

Se puede perdonar a los CISO

por esta falta de claridad después de una incertidumbre tan reciente. El rápido ajuste a las nuevas formas de trabajo, la mayor dependencia de la nube y los patrones de comportamiento cambiantes han hecho que sea increíblemente difícil clasificar las amenazas y construir defensas adecuadas.

Si bien la falta de claridad es una preocupación, no es un problema insuperable. Más del 90 % de los ciberataques comienzan con el correo electrónico. Ya sea ransomware, BEC o compromiso de cuenta en la nube, proteger la bandeja de entrada siempre es el mejor lugar para comenzar.

Las personas como el nuevo perímetro

Con dos años de trabajo remoto a sus espaldas, la mayoría de los CISO creen que los empleados comprenden el papel que desempeñan en la protección de sus organizaciones contra las ciberamenazas. En general, 3 de cada 5 encuestados (60 %) están de acuerdo con esta afirmación, frente al 58 % del año pasado.

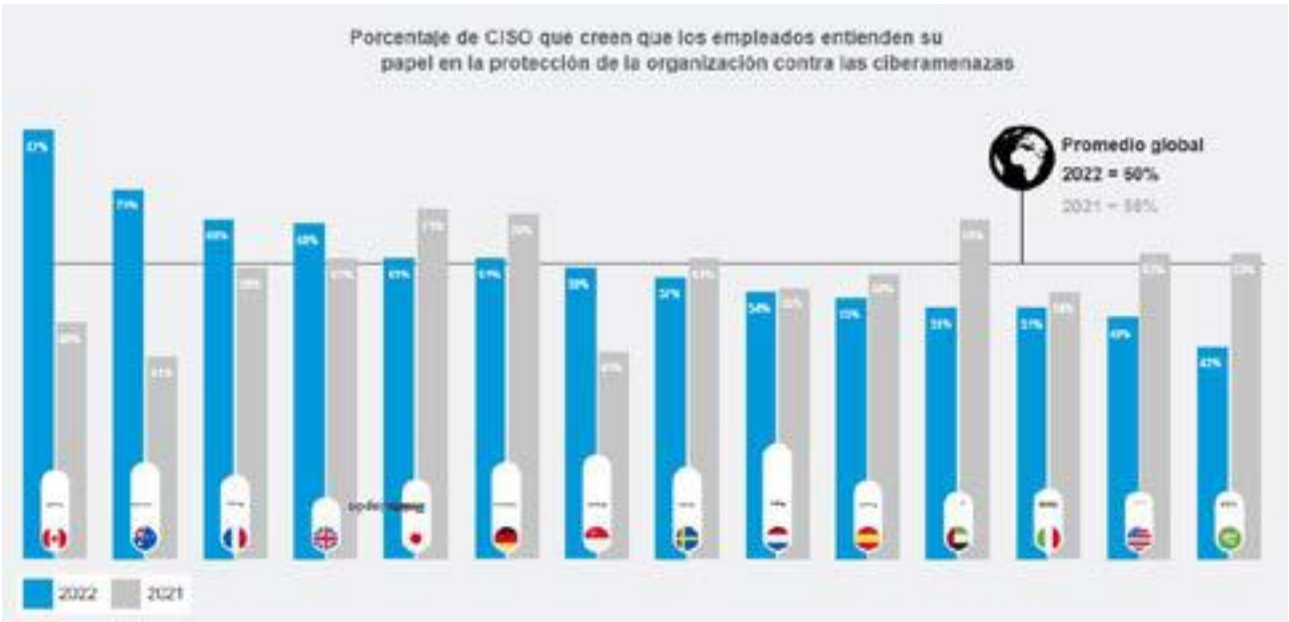
Alrededor de una cuarta parte, el 24%, está totalmente de acuerdo.

La tendencia es más pronunciada en Canadá y Australia, donde la creencia en la comprensión de los empleados ha aumentado 39 y 34 puntos porcentuales, respectivamente, hasta el 87 % y el 75 %.

Podemos atribuir gran parte de este aumento en la comprensión de los empleados a las medidas implementadas para admitir configuraciones remotas e híbridas a largo plazo. Muchas organizaciones pasaron los últimos dos años invirtiendo en capacitación y protecciones de seguridad cibernética que se centraron en las personas.

Con equipos trabajando desde cualquier lugar, hay menos énfasis en proteger el centro de datos o la red de la oficina. Los CISO ahora se dan cuenta de que el perímetro es el usuario y están tomando medidas para equiparlos para defenderlo en consecuencia.

En el otro extremo de la escala,



los países con entornos empresariales más formales o rígidos pueden haber tenido dificultades para realizar este ajuste. Por ejemplo, en Arabia Saudita y los Emiratos Árabes Unidos, la creencia en la comprensión de los empleados cayó más bruscamente, 19 y 18 puntos porcentuales, respectivamente, hasta el 51 % y el 43 %.

La creciente creencia en la inteligencia de los empleados en torno a la seguridad también se refleja en otros lugares. Este año, menos CISO creen que el error humano es la mayor vulnerabilidad cibernética de su organización, con solo el 56 % de acuerdo.

La noción de que el 60 % de los CISO cree que los usuarios entienden sus responsabilidades de seguridad, pero el 56 % cree que son la ciberamenaza número uno, genera varias señales de alerta. Sugiere que muchos CISO entienden que la mayoría de los usuarios no están adecuadamente capacitados para el rol de ciberdefensa.

El Foro Económico Mundial informa que el 95 % de los problemas de seguridad cibernética se deben a errores humanos,5 lo que destaca que muchos CISO aún subestiman significativamente el grado de riesgo que representan sus usuarios. Solo el 38 % de los CISO saudíes consideran a sus empleados su mayor vulnerabilidad cibernética, seguidos de Italia (43 %) y Japón (46 %).

Este también es el caso en el sector de la educación, donde solo el 47% cree que los usuarios son su riesgo más importante. En el otro extremo del espectro, los CISO de servicios comerciales y profesionales y manufactura lideraron el camino con un 61 % y un 60 %, respectivamente, de acuerdo.

En otros lugares, las actitudes han cambiado entre los CISO de atención médica en los últimos 12 meses. Un poco más de la mitad (52 %) cree que su gente puso en riesgo su negocio este año en comparación con el 48 % en 2021. Lo contrario es cierto en los servicios financieros,

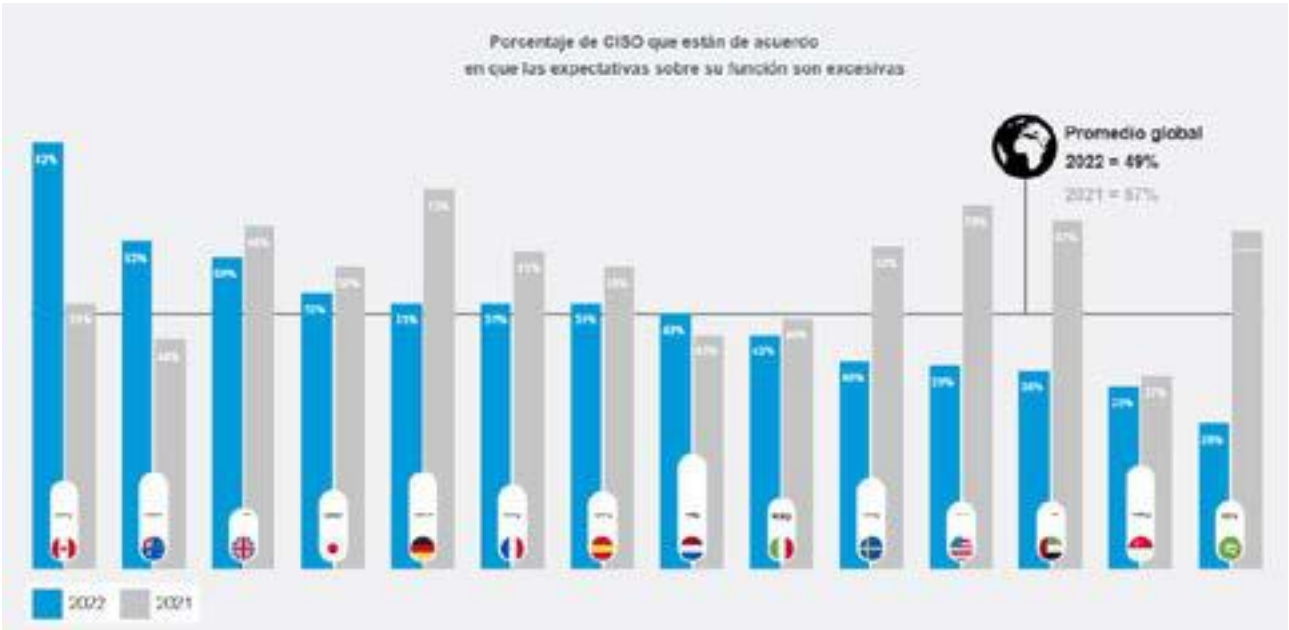
donde el 52 % ahora cree que su gente es el mayor riesgo cibernético, en comparación con el 61 % anterior año.

Riesgo, Trabajo Remoto y La Gran Renuncia

La migración forzada a configuraciones remotas e híbridas en los últimos años ha servido como un enorme caso de prueba. Unos 24 meses después de esta nueva forma de trabajar, las organizaciones ven lo que puede ofrecer en términos de flexibilidad, ahorro de costos y productividad.
También es popular entre los empleados, y es probable que esté aquí para quedarse. Ahora que las personas forman el perímetro defensivo dondequiera que trabajen, las organizaciones necesitan una nueva estrategia.
Como muchos están descubriendo, el trabajo híbrido y remoto hace que los usuarios sean más vulnerables a los ataques. Como mínimo, representan un objetivo mucho más atractivo para los ciberdelincuentes.
Más de la mitad de los CISO de todas las regiones están de acuerdo en que los ataques dirigidos a sus organizaciones han aumentado desde que adoptaron el trabajo híbrido masivo. Con muchos ahora mucho más cómodos en este entorno, no debería sorprender que esta cifra haya bajado del 58% en esta época del año pasado. Aun así, eso es un pequeño cambio; la mayoría de los CISO aún se enfrentan a un panorama de ciberamenazas elevado.
Y este factor de riesgo está lejos de ser el único problema que ha surgido desde que el trabajo híbrido se convirtió en la norma.
-La Gran Renuncia: un nuevo reto para los equipos de seguridad
Los empleados están dejando sus trabajos en números récord por razones que van desde el agotamiento posterior a la pandemia hasta problemas de cuidado de niños y cambios en las prioridades de la vida laboral. Pero cualquiera que sea la causa, las implicaciones de seguridad cibernética no están sujetas a debate.
Cuando un empleado se va, sus datos a menudo se van con él. A veces, no es intencional, como cuando las credenciales guardadas residen en un dispositivo personal. Pero en muchos casos, es deliberado. Los ex empleados pueden sentirse dueños de los datos en los que trabajaron o llevárselos para ayudarlos en su nuevo trabajo. Cualquiera que sea la razón, la tendencia ha hecho que a muchos CISO les resulte más difícil proteger sus datos.
Esto se siente más en las organizaciones más pequeñas que pueden tener menos controles implementados: el 55 % de los encuestados de empresas con menos de 500 empleados está de acuerdo en que proteger los datos se ha convertido en un desafío mayor en comparación con sólo el 47 % de los CISO de empresas más grandes (5.000 o más empleados)

Los datos no se van...

Los empleados lo mueven, y no siempre intencionalmente. Las personas que dejan un trabajo presentan otro problema de protección de datos.
Los empleados distraídos por la perspectiva de pastos más verdes a menudo son más propensos a los tipos de acciones que aprovechan los ciberdelincuentes; comportamientos como la mala gestión de contraseñas, soluciones alternativas de seguridad y el uso de dispositivos comerciales para uso personal.
Este tipo de comportamiento es la causa más común de amenazas internas, con investigaciones recientes que muestran que el 56 % de los incidentes se deben a negligencia.6 A pesar de esto, con más personal fuera de la oficina con mayor



autonomía sobre su higiene de seguridad, internos comprometidos, negligentes y maliciosos son de igual preocupación para los CISO del mundo.

Cómo están respondiendo las organizaciones a los desafíos del trabajo híbrido

La respuesta a esta creciente amenaza ha sido mixta. Si bien los CISO en países como Canadá han fortalecido las políticas de la era COVID para apoyar el trabajo híbrido en curso, solo alrededor de la mitad (51%) de los CISO globales han hecho lo mismo.

La mitad de los CISO globales encuestados han aumentado la frecuencia de la capacitación en seguridad cibernética para los empleados. Si bien es alentador, esto deja al 50 % en riesgo frente a niveles crecientes de ataques dirigidos. Las estrategias de mitigación centradas en la implementación de una arquitectura de confianza cero y la revisión de las soluciones de protección contra la pérdida de datos fueron una prioridad para la mitad de los encuestados.

Finalmente, la subcontratación de controles clave a proveedores de servicios administrados fue más frecuente entre las empresas con 500 a 1000 empleados.

Directorios, Buy-In y el resultado final—Cómo Los CISO se sienten

Dado el impacto duradero de la ciberseguridad durante una pandemia global, el trabajo del CISO nunca ha sido más desafiante o más crítico. Las increíbles demandas de los últimos dos años han hecho que el rol sea aún más destacado y han alentado a los CISO a hacer oír sus voces, alto y claro.

En general, los CISO de todas las regiones creen que las expectativas de sus superiores y colegas son excesivas. Dicho esto, las opiniones de los CISO varían ampliamente según el país y han cambiado mucho en el último año. Aun así, 1 de cada 2 CISO siente que se enfrenta a una tarea imposible.

En todos los verticales, los

CISO de empresas de negocios y servicios profesionales (57 %) son los que más sienten la presión de las expectativas excesivas entre sus pares. Los CISO del sector educativo son los menos presionados (39 %), seguidos de los del comercio minorista (42 %).

A la exigente y, a menudo, ingrata carga de trabajo del CISO se suma la percepción de falta de apoyo de la sala de juntas, que ha aumentado desde 2021. Poco más de la mitad (51 %) de los CISO globales coincidieron en que estaban de acuerdo con la junta en asuntos de ciberseguridad. en 2022. Esa es una fuerte caída del 59% del año anterior.

Este cambio coincide con el número de empleados de la empresa, lo que subraya las dificultades que enfrentan los CISO en organizaciones más pequeñas. Aún así, la caída en el apoyo percibido de la junta directiva la sienten más los CISO a cargo de grandes organizaciones (5000 empleados y más), quienes pasaron del 71 % de acuerdo el año pasado a solo el 51 % este año.

Esta falta de apoyo y acuerdo no solo afecta la aceptación y los presupuestos. Muchos CISO también informan que sus superiores afectan directamente su capacidad para desempeñar sus funciones.

Más de la mitad (51 %) de los CISO globales están de acuerdo en que su línea jerárquica puede obstaculizar la eficacia de su trabajo. Esta opinión es más prominente en el mundo de los servicios empresariales (58 %) y la tecnología (54 %). Pero es un problema mucho menor en los sectores de servicios financieros, medios y educación, donde solo el 46% estuvo de acuerdo con el sentimiento.

Las relaciones entre el CISO y el C-suite también son tensas en otras áreas. Solo la mitad de los CISO globales encuestados ahora cree que su organización los posiciona para tener éxito, en comparación con el 60 % hace un año.

Los CISO de salud y educación se sintieron menos respaldados por su organización, mientras que los de fabricación y tecnología se sienten más respaldados para llevar a cabo con éxito sus responsabilidades.

-Enfoque en las prioridades del CISO y las preocupaciones de la junta

En lo que respecta a las prioridades de seguridad de TI para los próximos dos años, los CISO a nivel mundial calificaron a sus tres principales como:

- Mejora de la protección de la información (39 %)
- Mejora de la concienciación sobre ciberseguridad (38 %)
- Consolidación y externalización de soluciones y controles de seguridad (36 %)

Si bien las dos primeras categorías siempre ocupan un lugar destacado en la agenda del CISO, es casi seguro que la última está impulsada por los eventos desde 2020. Con los empleados trabajando desde casa, en la oficina y en cualquier lugar intermedio, las configuraciones de TI son cada vez más complejas. Eso significa que requieren nuevas habilidades y más recursos para asegurarlos.

La Gran Renuncia jugará un papel aquí también. A medida que los empleados cambian de trabajo en gran número, las organizaciones deben asegurarse de tener siempre la experiencia y el conocimiento para implementar su estrategia cibernética. La subcontratación puede ser una forma asequible y sencilla de hacer precisamente eso.

Naturalmente, las prioridades difieren entre industrias y organizaciones. Para las grandes empresas con más de 5000 empleados, que probablemente tengan las configuraciones más complejas, la subcontra-

tación es la prioridad principal con un 41 %. Esto está muy por encima del porcentaje entre todos los demás tamaños de empresa.

Entre las industrias, mejorar la protección de la información es la iniciativa más apremiante para aquellos en TI, tecnología, telecomunicaciones, servicios financieros, manufactura y el sector público.

Las prioridades también varían de un país a otro. En el Reino Unido, educar a los usuarios es una prioridad, mientras que el 46 % dice que la conciencia sobre la seguridad es vital, un ligero aumento con respecto al año pasado. La educación también se considera crítica en otros lugares, encabezando la lista en los EE. UU., Canadá, los Países Bajos, España y Australia. En Italia, el riesgo de los proveedores sigue siendo una preocupación principal, ya que el 38 % de los CISO lo mencionan como una de sus tres principales prioridades durante los próximos dos años. La eficiencia es la mayor prioridad para los CISO en Alemania, Suecia y Japón, quienes ven la consolidación y simplificación de las soluciones y controles de seguridad como su máxima prioridad.

- Preocupaciones de la junta

No hay duda de que los titulares de seguridad cibernética en los últimos dos años han

despertado las salas de juntas de todo el mundo a los riesgos cibernéticos de hoy.
Preguntamos a los CISO globales sobre sus principales preocupaciones al considerar el impacto de un ataque cibernético en su negocio en función de sus interacciones con su directorio. Enumeraron el tiempo de inactividad significativo (37 %), la interrupción de las operaciones (36 %) y el impacto en la valoración del negocio (36 %) como lo más importante para los miembros de la junta.

Por el contrario, la pérdida de ingresos quedó en último lugar, tal vez vista por algunos como una consecuencia de las principales preocupaciones en lugar de un impacto directo. Dicho esto, las organizaciones más grandes (con más de 5000 empleados) eran las más preocupadas.
En todo el mundo, los consejos de administración de EE. UU., el Reino Unido y Francia ven el impacto de un ataque cibernético material en la valoración del negocio como la preocupación más apremiante. En los Países Bajos, Italia y España, el daño a la reputación es la principal preocupación. El tiempo de inactividad significativo es lo más importante para aquellos en Alemania, Emiratos Árabes Unidos, Australia y Singapur.

Conclusión

A medida que los CISO se han adaptado en los últimos dos años, muchos de ellos se sienten más cómodos con el nivel de riesgo al que se enfrentan. Los sistemas de retazos y las políticas ad hoc han sido reemplazados por defensas cibernéticas más estratégicas. Al mismo tiempo, los empleados ahora están bien versados en trabajar fuera de la oficina. Como resultado, los CISO globales ahora creen que los empleados comprenden mejor sus responsabilidades de seguridad y que sus organizaciones están mejor equipadas para hacer frente a un ataque cibernético.
Sin embargo, muchos pueden estar cayendo en una falsa sensación de seguridad. Los ataques dirigidos, el ransomware y las amenazas internas van en aumento. Y dado que la mayoría de los ataques cibernéticos requieren interacción humana, las personas siguen siendo el mayor factor de riesgo. Que relativamente pocos CISO hayan reforzado las defensas para proteger el perímetro de personas a la luz del trabajo híbrido es un motivo de gran preocupación.
Pero, una vez más, puede darse el caso de que no puedan, o no estén dispuestos, a empoderar a su gente. Al igual que el año pasado, muchos CISO no están de acuerdo con su directorio en materia de ciberseguridad. Y más de la mitad cree que su línea jerárquica obstaculiza la efectividad del trabajo.
La buena noticia: los CISO de todo el mundo saben dónde deben mejorar las cosas. Muchos están tomando medidas para mejorar las soluciones de protección de la información y la capacitación en concientización sobre seguridad, las cuales serán vitales en entornos híbridos a largo plazo. También se reconoce la escasez de habilidades y recursos, y muchos CISO planean subcontratar soluciones de seguridad en los próximos años.
En general, los CISO parecen haber abrazado el 2022 como la calma después de la tormenta. Pero con el aumento de las tensiones geopolíticas y el aumento de los ataques centrados en las personas, se deben cerrar las mismas brechas de concienciación, preparación y prevención de los usuarios antes de que el mar de la ciberseguridad se vuelva agitado una vez más.

Guía para la seguridad de la fuerza laboral remota

By Check Point Software

El mundo como lo conocemos ha cambiado. En este nuevo mundo, el trabajo ya no se realiza principalmente en la oficina corporativa.
Esto significa que ser productivo requiere que estemos siempre conectados, en todas partes, sin importar dónde estemos, qué dispositivo estemos usando, y sin importar a qué aplicación necesitemos acceder.
Lo que esto también significa es que la superficie de ataque nunca ha sido más amplia.
Para combatir el desafío y defenderse de ataques cada vez más sofisticados, como el phishing y el ransomware, las organizaciones pueden seguir agregando productos de seguridad individuales. Pero unir soluciones puntuales las deja con brechas de seguridad, visibilidad fragmentada, administración compleja y opciones limitadas para escalar.
En este documento, cubriremos las diferentes amenazas cibernéticas que surgen del nuevo espacio de trabajo distribuido y las cinco protecciones imprescindibles para mantener seguros a los usuarios remotos en todos los vectores de amenazas.

EL TRABAJO GLOBAL SE VUELVE REMOTO

El empleado en todas partes
El trabajo remoto es el nuevo estándar, con el 81% de las organizaciones que han adoptado el trabajo remoto masivo y el 74% planea habilitar el trabajo remoto a gran escala de forma permanente.
Esto hace que el empleado de hoy sea el “empleado en todas partes”, que puede (y trabaja) en cualquier lugar y que utiliza múl-

tiples dispositivos para acceder a Internet, a la red corporativa ya muchas aplicaciones. El resultado es que los datos comerciales confidenciales fluyen continuamente desde los dispositivos corporativos y BYOD hacia la nube, IaaS y los centros de datos, lo que expande la superficie de ataque más que nunca.
Las organizaciones deben habilitar el acceso a cualquier aplicación desde cualquier ubicación a través de cualquier dispositivo, y asegurarse de que no solo sea transparente.

La inevitabilidad de los errores no intencionales

Para complicar aún más el desafío de la seguridad, los usuarios remotos son más susceptibles a las ciberamenazas. Según una encuesta reciente de la industria a 2000 empleados remotos de todo el mundo, el 67 % admite encontrar soluciones a las políticas de seguridad corporativas para ser más productivos.
Esto incluye enviar documentos de trabajo a direcciones de correo electrónico personales, compartir contraseñas e instalar aplicaciones no autorizadas.
Desafortunadamente, mejorar la concienciación sobre la seguridad no hace completamente el trabajo de reducir el riesgo. Según la misma encuesta, más de la mitad (54 %) de los empleados dijeron que habían recibido capacitación en seguridad específica para el trabajo remoto, pero aproximadamente el 70 % admite usar dispositivos corporativos para uso personal. Y ~60% admite que permite que otros miembros de su hogar usen sus dispositivos corporativos para actividades como tareas escolares, juegos y compras.

El aumento global de los ciberataques

Todo esto no ha pasado desapercibido para los hackers. Para ilustrar, en el informe de seguridad cibernética de Check Point de 2021, se señaló que:

- Hubo un aumento del 93 % en ransomware, y la cantidad de organizaciones afectadas a nivel mundial se duplicó con creces durante la primera mitad de 2021 con respecto a 2020.
- Durante 2020, se descubrieron diariamente 100.000 nuevos sitios web maliciosos y 10.000 nuevos archivos maliciosos.
- En promedio, una nueva organización se convirtió en víctima cada 10 segundos en todo el mundo.

Y la amenaza es muy real y puede ser muy dañina. Por ejemplo, en marzo de 2020, el gigante de la industria hotelera, Marriott, reveló una nueva violación de datos que afectó a 5,2 millones de huéspedes del hotel. La infracción ocurrió cuando un pirata informático uti-

lizó las credenciales de inicio de sesión de dos empleados de la propiedad de la franquicia para acceder a la información del cliente desde los sistemas de back-end de una aplicación.

Como podemos ver, para mantener seguras las redes corporativas y los datos confidenciales, las organizaciones no tienen otra opción que recalibrar el enfoque de seguridad en torno a los usuarios y accesos remotos.

Y el primer paso es asegurarse de que cuentan con los cinco elementos imprescindibles para proteger eficazmente a la fuerza laboral remota.

LAS 5 PROTECCIONES IMPRESCINDIBLES PARA USUARIOS REMOTOS PUESTO FINAL DE SEGURIDAD

Con un aumento del 93 % en los ataques de ransomware en todo el mundo durante los últimos 6 meses, los dispositivos de punto final nunca han sido más vulnerables, y la seguridad de punto final desempeña un papel fundamental para habilitar a su fuerza de trabajo remota. Sin embargo, nunca ha habido más puntos finales para proteger, ya que las empresas abrieron el acceso a sus aplicaciones corporativas desde computadoras portátiles para garantizar la continuidad del negocio. Mientras mantienen la productividad, los usuarios remotos son más propensos a un comportamiento imprudente y al incumplimiento de la política corporativa.

Como resultado, están más expuestos a ataques de phishing, malware y ransomware. Y una vez que la PC o computadora portátil de un usuario está infectada, la amenaza puede moverse lateralmente e infectar fácilmente otros dispositivos de punto final y activos corporativos.

La protección de punto final (EPP) y la detección y respuesta de punto final (EDR) sirven como la primera y última línea de defensa contra la creciente ola de ataques de ransomware.

Los 5 pilares de una solución robusta de seguridad para endpoints

Anti-phishing

Defender a los usuarios de los ataques de phishing (incluido el phishing de día cero) mientras usan sus buzones de correo o navegan por Internet.

Anti-ransomware

Capacidades que monitorean los cambios en los archivos en las unidades de los usuarios para identificar el comportamiento del ransomware, como el cifrado de archivos ilegítimos, y para bloquear un ataque, así como para recuperar archivos cifrados automáticamente.

Desarme y reconstrucción de contenido (CDR)

CDR puede eliminar contenido explotable al desinfectar documentos de cualquier elemen-

to dañino y entregar versiones 100% desinfectadas en segundos.

Antibot
Protección contra infecciones impulsadas por bots y exposición de datos confidenciales.

Detección, remediación y respuesta automatizadas posteriores a la infracción
Análisis, contextualización y remediación de incidentes impulsados por la automatización, junto con una vista de ataque de extremo a extremo, que cubre los puntos de entrada, el movimiento lateral y el impacto en el negocio.

ACCESO SEGURO A INTERNET

Trabajar fuera del firewall corporativo expone a los usuarios a una gran cantidad de amenazas basadas en Internet que, de lo contrario, estarían bloqueadas a nivel de red. Los trabajadores remotos pueden poner en riesgo a sus organizaciones sin querer al descargar archivos infectados y visitar sitios de phishing donde se roban las credenciales corporativas.
Dado que Check Point descubre más de 10 000 nuevos archivos maliciosos y 100 000 nuevos sitios web maliciosos todos los días, evitar que las amenazas lleguen a los usuarios se vuelve crítico, y la detección y mitigación retroactivas a menudo resultan ser demasiado poco y demasiado tarde.
Entonces, ¿cómo protege de manera preventiva a los usuarios remotos cuando acceden a Internet para el trabajo y el uso personal y previene los últimos ataques de phishing y malware?
Seis principios para seleccionar una solución de acceso seguro a Internet
Al seleccionar una solución para garantizar un acceso seguro a Internet, hay seis principios que deben tenerse en cuenta:

Protección completa
Contra phishing, descargas y sitios web maliciosos, pérdida de datos, ransomware, exploits de navegador, entre otros.

Seguridad preparada para el futuro
Tecnologías de seguridad avanzadas que pueden bloquear archivos maliciosos y ataques de phishing nunca antes vistos.

Una experiencia de usuario perfecta
Bloquee los ataques basados en Internet con un impacto mínimo en la velocidad y la experiencia de navegación del usuario.

Escala y simplicidad
Evite el tráfico de retorno a través del centro de datos adoptando un servicio de seguridad global basado en la nube o, mejor aún, implementando la seguridad directamente en el navegador.

Privacidad
Mantenga privado el historial de navegación de los usuarios para garantizar el cumplimiento de GDPR y otras regulaciones de protección de datos.

100% inspección de tráfico
Asegúrese de que se pueda inspeccionar todo el tráfico, incluidas SSL y las nuevas versiones del protocolo HTTP.

ACCESO DE RED DE CONFIANZA CERO (ZTNA) A APLICACIONES CORPORATIVAS

Los empleados remotos no pueden hacer su trabajo sin acceso a sus aplicaciones corporativas. Y para asegurarse de mantener una productividad mejorada (incluso cuando están fuera de la oficina), necesitan un fácil acceso desde cualquier dispositivo, ya sea un teléfono móvil, una PC doméstica u otro dispositivo. Si bien el acceso rápido es obligatorio, también es fundamental poder examinar a cada usuario antes de que acceda a la red y a las aplicaciones empresa-

riales confidenciales, ya sea alojadas en las instalaciones o en la nube.
Tradicionalmente, las organizaciones han confiado en la seguridad basada en VPN para lograr la tarea y luego proporcionar a los usuarios un amplio acceso a la red una vez autenticados. Este enfoque ya no es viable. Hoy en día, es necesario proteger una superficie de ataque en constante cambio y tener visibilidad de lo que los usuarios están haciendo realmente.
Esta es la razón por la cual la protección actual requiere una arquitectura de confianza cero que permita a los administradores eliminar el riesgo de acceso no autorizado y evitar el movimiento lateral dentro de la red.
6 principios para elegir la solución ZTNA óptima
Al emprender el camino hacia el acceso de confianza cero, es importante adherirse a los siguientes seis principios y asegurarse de que la solución que elija permita su implementación:

Considere a todos los usuarios
Ofrezca acceso de confianza cero en toda la organización, incluidos terceros, como socios y contratistas, al mismo tiempo que brinda soporte para aplicaciones web, bases de datos, escritorios remotos y terminales remotos SSH.

Acceso remoto cliente y sin cliente
Elija una solución que ofrezca tanto métodos de implementación como la capacidad de escalar de forma segura el acceso remoto en cuestión de minutos.

Experiencia de usuario
Elija una estrategia y productos que creen la experiencia más fluida y similar a SaaS para el equipo.

Política de acceso con privilegios mínimos
A un usuario en particular solo se le deben otorgar los privilegios suficientes para permitirle completar una tarea en particular. Por ejemplo, un ingeniero que solo se ocupa de actualizar líneas de código heredado no necesita acceder a los registros financieros.

Autenticación multifactor (MFA)
Verifique estrictamente la identidad de cada usuario que accede a la red utilizando múltiples factores. Asegúrese de que estos factores se puedan ajustar según la sensibilidad de los datos/recursos a los que se accede.

Supervisar y auditar todo
Supervise y revise toda la actividad de los usuarios en la red para identificar cualquier actividad sospechosa en tiempo real.

CORREO ELECTRÓNICO Y SEGURIDAD EN LA OFICINA

En el mundo empresarial moderno de hoy, ningún empleado, remoto o no, puede ser productivo sin acceso a aplicaciones de productividad y correo electrónico, como Office 365, Teams, SharePoint, One Drive, Gmail, Google Drive y más. Estas herramientas no solo son fundamentales para hacer las cosas. También son uno de los canales más explotados por los piratas informáticos, con ataques de compromiso de correo electrónico comercial (BEC), por ejemplo, que representan más del 50% de las pérdidas causadas por el ciberdelito.
Las 5 protecciones clave para el correo electrónico y la oficina

Protección contra phishing en tiempo real
Está totalmente automatizado y basado en IA para evitar ataques avanzados de phishing y spear phishing nunca antes vistos antes de que sucedan.

Protección de malware
Con CDR (desarme y reconstrucción de contenido) para entregar archivos adjuntos y archivos limpios en segundos, mientras bloquea el malware evasivo a través del análisis de archivos estático y dinámico

basado en IA.

Prevención de fugas de datos
Eso permite que se establezcan políticas personalizadas para necesidades específicas y que bloquee automáticamente la información confidencial saliente en el correo electrónico y las aplicaciones de colaboración.

Prevención de amenazas internas
Para escanear y bloquear amenazas que se originan en correos electrónicos desde dentro de la red corporativa, y para evitar el movimiento lateral.

Todo en torno a la seguridad en una ventanilla única
Para garantizar una seguridad total fácil de administrar y reducir la complejidad operativa.

DEFENSA CONTRA AMENAZAS MÓVILES (MTD)

Proteger los dispositivos móviles corporativos nunca ha sido fácil. Las tiendas de aplicaciones contienen muchas aplicaciones maliciosas, es más difícil detectar contenidos y archivos adjuntos de correo electrónico sospechosos cuando llegan a un dispositivo móvil, y los phishers a menudo explotan vulnerabilidades que son específicas de las aplicaciones móviles y para las que a menudo no existen filtros.
Pero el desafío ahora es mayor que nunca. La movilización masiva de la fuerza laboral global al hogar significa que los empleados remotos acceden a datos corporativos desde dispositivos móviles más que nunca, a menudo a través de redes Wi -Fi públicas que son fáciles de comprometer, envían más correos electrónicos, envían mensajes con más frecuencia y comparten más archivos que nunca.
De hecho, durante el año pasado, los investigadores de Check Point observaron un aumento en la cantidad de ataques relacionados con dispositivos móviles, así como métodos de ataque completamente nuevos, como ransomware móvil sofisticado y MDM que se arman para atacar a las organizaciones. Solo en 2020, el 97 % de las organizaciones se enfrentó a amenazas móviles que usaban varios vectores de ataque, y el 46 % de las organizaciones tenía al menos un empleado

que descargaba una aplicación móvil maliciosa.
5 principios de la seguridad móvil óptima

Protección 360° de todos los vectores de ataque
Incluyendo aplicaciones móviles maliciosas, ataques basados en la red y sistemas operativos y dispositivos vulnerables.

Visibilidad completa del nivel de riesgo
Con una visión completa de la postura de seguridad móvil de la organización para mitigar el riesgo de manera efectiva y acelerar la respuesta cuando sea necesario.

Despliegue escalable
Con soporte para cada tipo de dispositivo, sistema operativo y modelo de propiedad del dispositivo.

Maximizando la experiencia del usuario
Al evitar el impacto en la usabilidad del dispositivo, la experiencia de navegación, el consumo de datos y la duración de la batería.

Asegurando privacidad por diseño
De dispositivos corporativos y BYOD.

EL VALOR DE LA CONSOLIDACIÓN DE LA SEGURIDAD

La implementación de las cinco protecciones imprescindibles para los usuarios remotos es un buen comienzo para asegurar el nuevo entorno híbrido de "trabajo desde cualquier lugar". Pero esto puede ser muy desafiante ya que requiere protecciones infinitas en dispositivos, redes, puntos de acceso y aplicaciones.

Algunas organizaciones intentan superar el desafío uniendo soluciones puntuales con API u optando por las mejores soluciones de su clase. Sin embargo, estos enfoques implican una gestión compleja y dejan muchas brechas de seguridad sin tratar, donde la organización tiene una visibilidad fragmentada en el mejor de los casos y sus opciones de escala son limitadas.
Para mantener seguras las redes corporativas y los datos confidenciales, las organizaciones no tienen otra opción que recalibrar el enfoque de seguridad en torno a los usuarios remotos y el acceso. La clave para superar el desafío es consolidar las diversas soluciones de seguridad en una solución unificada.

Descargue aquí el informe

NOTICIAS DEL SECTOR IT EN LATINOAMÉRICA

ITWARE
LATAM.COM

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

Manténgase informado suscribiendo a nuestros newsletter

@ITwareLatam @ITwareLatam ITware Latam

ITware Latam ITware Latam

10 AÑOS

Endpoints: lo que no se ve sí existe

By CrowdStrike

Cada día más empresas trasladan más aplicaciones, infraestructura y datos a la nube. El número de endpoints que accede a ellos se dispara. Un endpoint es cualquier dispositivo que se pueda conectar a una red, incluidos computadoras, portátiles, teléfonos móviles, tablets y servidores, así como cualquier otro dispositivo que se pueda conectar a Internet (Internet de las cosas o IoT).

Por eso, el endpoint se considera una de las mayores fuentes de riesgos para cualquier empresa. La falta de visibilidad y escalabilidad en este entorno expansivo plantea un serio desafío para los equipos de seguridad y TI encargados de la protección de los endpoints, y ahí, los sistemas de seguridad antiguos no sirven realmente de ayuda. Estas soluciones, desarrolladas en un principio para identificar archivos de malware conocido, no se diseñaron en ningún momento para escalarse y ofrecer el nivel de visibilidad necesario para proteger el entorno expansivo actual, objetivo de agresores que emplean malware sin archivos, aprovechan las vulnerabilidades de las plataformas y las aplicaciones, roban y utilizan ilícitamente identidades, e inyectan amenazas persistentes avanzadas.

La complejidad se alía con el agresor. Tener visibilidad y control de lo que está pasando en los endpoints es difícil, cuando no imposible, por muchos motivos, debido principalmente al creciente número de endpoints que cambian de ubicación con frecuencia. Los ciberdelincuentes aprovechan las lagunas de seguridad derivadas de una visibilidad insuficiente y una falta de control para sacar partido de la situación.

¿Qué hace falta para que los equipos de seguridad y TI protejan los endpoints con agilidad, eficiencia y eficacia?

La protección de endpoints moderna requiere una visibilidad total. Una protección de endpoints verdaderamente eficaz debe proporcionar el máximo nivel posible de seguridad, pero también ser fácil de utilizar. La complejidad sobrecarga a los equipos y los procesos, e introduce lagunas de seguridad que incrementan el riesgo de que disminuya la productividad y se dañe la reputación de una empresa.

Para conseguir tanto seguridad como simplicidad, la protección de los endpoints debe incluir cinco elementos clave:

1. Prevención para impedir la entrada del mayor número posible de agentes maliciosos.
2. Detección para buscar y eliminar ciberdelincuentes.
3. Threat hunting gestionado para llevar la detección más allá de las defensas automatizadas.
4. Inteligencia sobre amenazas para conocer a los atacantes y

anticiparse a sus movimientos.
5. Gestión de vulnerabilidades e higiene de TI para preparar y reforzar el entorno frente a amenazas y ataques.
Estas cinco capacidades solo se pueden implementar, integrar y ofrecer a través de una plataforma nativa de la nube que simplifique las operaciones de seguridad y cumpla los requisitos de velocidad, flexibilidad y escalabilidad necesarios para defenderse de las amenazas más sofisticadas de hoy en día.

Prevención: cierre la puerta a los ciberdelincuentes

La protección de endpoints tradicional centrada en el malware —como las soluciones antivirus— suele ser eficaz únicamente frente al malware conocido. Además, dado el aumento de las tácticas cada vez más sofisticadas sin archivos ni malware, resulta insuficiente ante el panorama de amenazas actual. Los equipos de seguridad y TI necesitan la inteligencia de una solución antivirus de nueva generación (NGAV) capaz de reconocer y evitar malware conocido y de día cero, ransomware, y ataques sin archivos y sin malware. Las soluciones NGAV avanzadas pueden emplear análisis de comportamiento para buscar automáticamente indicios de ataque y bloquearlos mientras suceden.
A diferencia de las soluciones de seguridad antiguas, que requieren actualizaciones diarias que dejan desprotegidos temporalmente los endpoints, las soluciones NGAV pueden utilizar aprendizaje automático para mantener la seguridad actualizada, sin sobrecargar a los equipos de seguridad y TI. Las mejores soluciones NGAV combinan estas y otras técnicas avanzadas que proporcionan la visibilidad y el contexto necesarios para evitar que las tácticas, técnicas y procedimientos (TTP) de ataque modernos logren su objetivo.
No obstante, como bien sabe todo equipo de seguridad experimentado, hasta la mejor estrategia de prevención es insuficiente frente a los ciberdelincuentes sofisticados y con amplios recursos económicos de hoy día. La solución más segura para una empresa pasa por combinar la prevención con una estrategia de detección sólida para identificar y bloquear cualquier ataque furtivo que consiga acceder.

Detección: halle y elimine a los ciberdelincuentes que consigan colarse

Cuando los ciberdelincuentes consiguen un primer acceso sin que se disparen las alarmas, pueden permanecer silenciosamente en un entorno y provocar daños durante días, semanas o incluso meses, sin ser advertidos.
Las soluciones de detección y respuesta para endpoints (EDR) con funciones de prevención bien integradas proporcionan la visibilidad que necesitan los equipos de seguridad para descubrirlos lo más rápido posible. Para ello, una solución EDR debe registrar todas las actividades de interés de un endpoint para someterlas a

una inspección exhaustiva, tanto en tiempo real como a posteriori, y completar estos datos con inteligencia sobre amenazas, con el fin de suministrar el contexto necesario para el threat hunting y la investigación de las amenazas.
Los equipos de seguridad no deberían tener que dedicar tiempo a escribir y ajustar las reglas de detección. Una solución EDR eficaz cuenta con inteligencia para detectar automáticamente actividades maliciosas y presentar a los equipos ataques reales, sin distraerlos con falsos positivos y actividades lícitas. Mediante acciones de respuesta eficaces, los equipos pueden contener e investigar sistemas comprometidos, incluido el acceso remoto sobre la marcha, para tomar medidas inmediatas y detener la intrusión de raíz.
Aunque las soluciones EDR avanzadas pueden detectar ataques furtivos y descubrir amenazas que hayan conseguido eludir los sistemas de prevención, las empresas pueden dar un paso aún más proactivo para proteger los endpoints: incorporar threat hunters.

Threat hunting gestionado: eleve la detección más allá de las defensas automáticas

El threat hunting permite a las empresas aplicar un enfoque humano y proactivo para buscar activamente actividades sospechosas, en lugar de confiar únicamente en la tecnología, para detectar y avisar de manera automática de la actividad de un posible ciberdelincuente.
El threat hunting gestionado sirve de ayuda a empresas que carecen de recursos y expertos en seguridad para descubrir a los ciberdelincuentes e impedir que las amenazas avanzadas acechen silenciosamente su entorno. Un equipo de threat hunting experimentado puede monitorizar su entorno de manera ininterrumpida para detectar actividades furtivas maliciosas.
Los equipos de threat hunting gestionado analizan las amenazas y trabajan codo con codo con el personal interno para guiarle desde la detección hasta la respuesta. Esta interacción con expertos eleva el nivel de sofisticación de los equipos de seguridad y TI internos, no solo en ese preciso momento, sino también a la larga.
Los threat hunters adoptan un enfoque proactivo en cuanto a la protección de endpoints, gracias a sus años de experiencia. Al tener visibilidad del estado de los endpoints y acceso a la inteligencia adecuada sobre amenazas, no solo son capaces de entender lo que observan, sino que pueden también anticiparse a las ciberamenazas contra la empresa.
Inteligencia sobre amenazas: conozca y anticípese a los ataques
Los agresores se mueven con tanta rapidez y sigilo que a las tecnologías y los profesionales de la seguridad les resulta difícil seguir el ritmo de las últimas amenazas y protegerse de ellas con antelación. Para responder con la misma celeridad, las soluciones de seguridad de endpoints deben incorporar siempre inteligencia sobre amenazas o tener la capacidad de integrar inteligencia de terceros.

La inteligencia sobre amenazas debe cumplir los siguientes requisitos:

Proporcionar información práctica que permita a los equipos de seguridad y a las soluciones que ellos utilizan comprender, responder y solucionar incidentes de manera más rápida, para agilizar las investigaciones y la corrección de los incidentes.

Generar y priorizar alertas que ayuden a los equipos de seguridad a comprender mejor las tácticas y las campañas asociadas a determinados ciberdelincuentes.

Estar integrada a la perfección en la solución de protección de endpoints, de modo que esté al alcance de los equipos de seguridad y TI. Los equipos no deberían tener que cambiar manualmente entre las distintas soluciones de seguridad, sino que deben ser capaces de ver el contexto de una alerta y limitarse a hacer clic para desplazarse a otra pantalla con información más detallada.

La capacidad de entender y predecir ataques mediante la inteligencia sobre amenazas es un elemento clave de la preparación de una empresa a la hora de enfrentarse a ataques avanzados.

Además, la gestión de las vulnerabilidades y la higiene de TI refuerzan las defensas aún más.

Gestión de vulnerabilidades e higiene de TI: refuerce su entorno frente a los ataques

La gestión de vulnerabilidades y la higiene de TI ofrecen la visibilidad y la información práctica que los equipos de seguridad y TI necesitan para comprender qué sistemas y aplicaciones están en riesgo, así como qué y quiénes están activos en el entorno.

Para que la gestión de las vulnerabilidades sea eficaz, se requiere una monitorización continua de todos los endpoints a fin de identificar los puntos débiles de seguridad dondequiera que se encuentren, ya sea en las instalaciones o fuera de ellas.

Para garantizar que los sistemas de producción estén protegidos con parches actualizados, las empresas deben saber qué vulnerabilidades representan el nivel de riesgo más alto para la empresa y abordar las correcciones correspondientes.

A pesar de sus esfuerzos, inevitablemente, a las empresas les faltarán algunos parches y mitigaciones dado el constante aumento de las vulnerabilidades críticas. Dedicar a cada vulnerabilidad el tiempo necesario para mitigarla y responder para proteger el entorno es una tarea ingente, cuando no imposible. Las soluciones de higiene de TI monitorizan continuamente posibles cambios en los recursos, las aplicaciones y los usuarios, y ayudan a identificar los sistemas no gestionados o los que pueden comportar un riesgo para la red, como los dispositivos de terceros o los BYOD no protegidos.

Obtener visibilidad sobre las tendencias de inicio de sesión (por ejemplo, las actividades asociadas y la duración) en su entorno, dondequiera que se utilicen las credenciales y se creen las credenciales de administrador, permite a los equipos de seguridad detectar y mitigar el uso indebido de credenciales y los ataques basados en credenciales robadas.

La gestión de vulnerabilidades y la higiene de TI proporcionan a los equipos de seguridad la información que necesitan para adoptar una postura proactiva eficaz que mejore la estrategia de seguridad general y los coloque en una posición óptima para anticiparse a los adversarios y vencerles.

Dé el paso siguiente

Estas cinco capacidades esenciales de la seguridad de endpoints moderna solo se pueden implementar, integrar y ofrecer a través de una plataforma nativa de la nube que simplifique las operaciones de seguridad y se ajuste a la velocidad, la flexibilidad y la competencia necesarias para defenderse frente a los ciberdelincuentes modernos.

¿Está preparado para encontrar una solución que proporcione una protección de endpoints robusta que cuente con estas cinco capacidades esenciales?

Descargue aquí el informe

Qué esperar en ciberseguridad para 2023

Por FortiGuard Labs

2022 fue un año en que la ciberseguridad estuvo en la mira de todos, con un incremento en los ataques con resultados devastadores. FortiGuard Labs repasa las tendencias más preocupantes en el panorama cibernético para el año que se avecina.

Una mirada retrospectiva a sus predicciones para 2022

El año pasado, FortiGuard Labs hizo varias predicciones sobre cómo evolucionaría el panorama de amenazas, que van desde que los atacantes dedican más esfuerzo a las actividades previas al ataque hasta un número cada vez mayor de intentos de ataque que afectan la tecnología operativa (OT). Veamos cómo les fue a algunas de tales predicciones y cómo esperan que evolucionen estas amenazas a medida que planificamos para 2023.

El auge del ciberdelito persistente avanzado

Predijeron un aumento de nuevas vulnerabilidades y más actividad de "mano izquierda", o reconocimiento previo al ataque y armamento, entre los atacantes que allanarían el camino para escalar aún más el crecimiento de Crime-as-a-Service (CaaS). Y solo en la primera mitad de 2022, la cantidad de nuevas variantes de ransomware que identificaron aumentó casi un 100 % en comparación con el período de seis meses anterior.

Este crecimiento explosivo de nuevas variantes de ransomware se puede atribuir principalmente a la creciente popularidad de RaaS en la dark web.

Al igual que la transmisión de medios o las aplicaciones de entrega de alimentos, anticiparon que las organizaciones ciberdelincuentes utilizarán servicios de modelo de suscripción y comprarán ransomware plug-and-play. Para agregar más presión sobre las víctimas, los operadores de RaaS a menudo amenazan con filtrar datos robados en la web oscura si no se cumplen sus demandas.

Si bien la cantidad de variantes de ransomware que se están introduciendo se está disparando principalmente debido a RaaS, los pagos de ransomware también están aumentando. La Red de Ejecución de Delitos Financieros del Tesoro de EE. UU. (FinCEN) informó que las organizaciones pagaron casi u$s 600 millones en ransomware en la primera mitad de 2021. El 72 % de los encuestados afirma tener una política de rescate y el procedimiento para el 49 % de ellos es pagar el rescate directamente.

Ahora predicen que el mercado de CaaS se expandirá significativamente hasta 2023 y más allá, con nuevos exploits, servicios y programas estructurados que pronto se ofrecerán a los actores de amenazas a través de modelos de suscripción.

Los ataques perimetrales se generalizan

Los dispositivos perimetrales, como los sistemas OT y las redes de Internet satelitales, alguna vez se consideraron objetivos no tradicionales (y menos populares) para los atacantes astutos. Sin embargo, durante la última década, han observado un aumento en la sofisticación y el volumen de intentos de ciberataques contra estos objetivos.

La convergencia casi universal de las redes de TI y OT ha facilitado que los atacantes accedan a los sistemas OT. Según el Informe sobre el estado de la tecnología operativa y la ciberseguridad de Fortinet 2022, el 93 % de las organizaciones experimentó una intrusión dirigida a su infraestructura de OT en los últimos 12 meses, y el 83 % experimentó más de tres.

El año pasado, predijeron que los actores de amenazas usarían cada vez más los troyanos de acceso al borde (EAT) para atacar los entornos de borde, y vieron varios ejemplos de esto. Uno de esos ejemplos observado por FortiGuard Labs en marzo de 2022 fue un troyano genérico llamado StartPage que cambia la página de inicio de un navegador para mostrar publicidad, promover aplicaciones engañosas o maliciosas, o explotar el navegador para ejecutar amenazas. Impulsó un aumento global en la entrega de malware a dispositivos OT.

También predijeron que las redes de Internet satelitales se convertirían en un nuevo objetivo para los ciberdelincuentes. A medida que el tamaño y la escala de estas redes continúan creciendo, también lo hace la cantidad de intentos de compromiso.

Esperan que continúen estos tipos de ataques basados en satélites, siendo los principales objetivos las organizaciones que dependen de la conectividad basada en satélites para respaldar actividades de baja latencia, como cruceros y buques de carga, aerolíneas, plataformas y oleoductos de petróleo y gas, y servicios remotos. oficinas de campo.

La motivación de los ciberdelincuentes que buscan explotar los dispositivos perimetrales es simple: los objetivos como los sistemas OT y las redes satelitales ofrecen a los atacantes nuevos puntos de entrada al entorno de una organización. El aumento de los bordes de la red también significa que hay más lugares para ocultar las amenazas del tipo living-off-the-land, lo que permite a los atacantes hacer que sus operaciones maliciosas parezcan actividades normales de la red y pasen desapercibidas.

El ransomware y los wipers se potencian

El secuestro de datos es cada vez más desagradable y más caro. En una encuesta global sobre ransomware realizado por Fortinet, el 67 % de las organizaciones informaron haber sufrido un ataque de ransomware. Peor aún, casi la mitad dijo que había sido atacada más de una vez, y casi una de cada seis dijo que había sido atacada tres o más veces.

En 2021, comenzaron a ver los primeros indicios de que los atacantes estaban subiendo la apuesta al agregar malware wipers a sus ataques de ransomware. El malware Wiper, que se descubrió inicialmente hace una década, brinda a los ciberdelincuentes la capacidad de eliminar datos y paralizar la disponibilidad crítica del sistema, como OT o equipos y servidores, a menos que se cumpla una demanda de rescate. Dado el nivel de convergencia que han visto entre varios métodos de ataque y amenazas persistentes avanzadas (APT), anticipamos que un número creciente de ataques de ransomware se combinarían con capacidades más destructivas como el malware wipers.

Las tendencias del malware Wiper revelan una evolución inquietante de técnicas de ataque más destructivas y sofisticadas. La creciente prevalencia del malware wiper es un indicador de que estas cargas útiles armadas no se limitan a un objetivo o región y probablemente se usarán en combinación con otros libros de jugadas de ciberdelincuencia en el futuro. La combinación de malware de limpieza con ransomware re-

presenta una nueva combinación viciosa que sube la apuesta para los delincuentes que buscan extorsionar a sus víctimas.

Adaptando a la inteligencia artificial como arma

La IA ya se usa de manera defensiva para detectar comportamientos inusuales de Internet de las cosas (IoT) que pueden indicar un ataque, generalmente por botnets. Y como predijeron desde FortiGuard Labs, los ciberdelincuentes han comenzado a aprovechar cada vez más la IA para respaldar una multitud de actividades maliciosas, que van desde frustrar los algoritmos que detectan la actividad anormal de la red hasta imitar el comportamiento humano.

Uno de esos ejemplos de atacantes que utilizan la IA como arma es el desarrollo de Deep fakes. El término "deepfake" se utilizó por primera vez hace cinco años. Este vector de ataque presenta una causa creciente de preocupación. Existen varios métodos para crear deepfakes y las tecnologías están mejorando rápidamente. Uno de los más populares es el uso de la red adversarial generativa (GAN), que se entrena para reconocer patrones mediante algoritmos que también se pueden usar para crear imágenes falsas.

Otro método es a través de algoritmos de inteligencia artificial llamados codificadores, que se utilizan en la tecnología de reemplazo e intercambio de rostros. El decodificador recupera e intercambia imágenes de caras, lo que permite superponer una cara a un cuerpo completamente diferente.

Los deepfakes ciertamente representan otro vector de amenaza potencial que los equipos de seguridad y sus organizaciones deben considerar. Ya están viendo algunos casos de piratas informáticos que utilizan estas tácticas para apoyar actividades delictivas.

Atracos a billeteras criptográficas

Las transacciones bancarias y las transferencias electrónicas solían ser los principales objetivos de los ciberdelincuentes. Sin embargo, a medida que los bancos mejoran cada vez más sus medidas de seguridad, encriptando transacciones y requiriendo autenticación de múltiples factores (MFA), ahora es más difícil para los piratas informáticos interceptar estas transacciones. Pero como dice el dicho, "Cuando una puerta se cierra, otra se abre". Como se predijo, observan más instancias de malware diseñado para apuntar a las credenciales criptográficas almacenadas y drenar las billeteras digitales. Las billeteras digitales son objetivos fáciles para los piratas informáticos, ya que tienden a ser menos seguras.

Nuevas tendencias de ataque a tener en cuenta en 2023

No es ningún secreto que los piratas informáticos seguirán confiando en ciertas tácticas de ataque probadas y verdaderas, particularmente aquellas que son fáciles de ejecutar y les ayudan a lograr ganancias rápido. Sin embargo, el equipo de FortiGuard Labs predice que surgirán varias tendencias de ataques nuevas y distintas en 2023. Estos son algunos de los desarrollos únicos de ataques de seguridad para los que hay que estar atentos el próximo año.

Nuevas ofertas de crimen como servicio

Dado el éxito de los ciberdelincuentes con RaaS, predicen desde FortiGuard Labs que un número creciente de vectores de ataque adicionales estarán disponibles como servicio a través de la dark web. Además de la venta de ransomware y otras ofertas de Malware-as-a-Service (MaaS), también se comenzarán a ver nuevas soluciones criminales y un aumento en la venta de acceso a objetivos previamente comprometidos.

CaaS podría ser un modelo comercial atractivo para los actores de amenazas. Esperan ver más ofertas llave en mano basadas en suscripción disponibles para los actores de amenazas. Este modelo emergente permitiría a los ciberdelincuentes de todos los niveles implementar ataques más sofisticados sin invertir el tiempo y los recursos por adelantado para elaborar su propio plan único. Y para los ciberdelincuentes experimentados, la creación y venta de carteras de ataques "como servicio" ofrece un día de pago simple, rápido y repetible.

Como resultado, prepárense para que surja una cartera de CaaS ampliada en 2023 y más allá.

También anticipan que los actores de amenazas comenzarán a aprovechar los vectores de ataque emergentes, como los deepfakes, ofreciendo estos videos y grabaciones de audio y algoritmos relacionados de manera más amplia para su compra. Más allá de apuntar a celebridades de alto perfil y funcionarios públicos, esperan que los actores de amenazas amplíen su alcance para incluir personas influyentes, particularmente aquellos con una fuerte presencia digital.

Además de los deepfakes, predicen que el reconocimiento como servicio aumentará en popularidad. A medida que los ataques se vuelven más específicos, es probable que los actores de amenazas contraten "detectives" en la web oscura para recopilar información sobre un objetivo en particular antes de lanzar el ataque. Al igual que los conocimientos que se pueden obtener al contratar a un investigador privado, las ofertas de Reconocimiento como servicio pueden ofrecer planes de ataque, para incluir el esquema de seguridad de una organización, el personal de seguridad clave, la cantidad de servidores que tienen, las vulnerabilidades externas conocidas e incluso credenciales comprometidas para la venta, y más, para ayudar a un ciberdelincuente a llevar a cabo un ataque altamente dirigido y efectivo.

El lavado de dinero recibe un impulso con la automatización

Para ayudar a hacer crecer una organización criminal, los líderes y los programas de afiliados suelen emplear mulas de dinero, personas que, a sabiendas o sin saberlo, se utilizan para ayudar a lavar dinero

en nombre de un sindicato del crimen. Las mulas de dinero a menudo se reclutan a través de anuncios y se utilizan para mover dinero de forma anónima de un país o cuenta bancaria a otro.
Esta mezcla de dinero generalmente se realiza a través de servicios de transferencia bancaria anónimos o mediante intercambios de cifrado para evitar la detección. El uso de mulas desconocidas para las transacciones y la reubicación física del dinero ayuda a evitar dejar un rastro digital y sigue siendo común. Los fondos a menudo se fragmentan en lotes más pequeños y luego se transfieren a través de múltiples canales para evitar activar las alertas exigidas por las leyes contra el lavado de dinero.

Anticipan que los ciberdelincuentes comenzarán a usar el aprendizaje automático (ML) para la selección de objetivos, ayudándolos a identificar mejor a las mulas potenciales y reduciendo el tiempo que lleva encontrar a estos reclutas.
También esperan que las campañas manuales de mulas sean reemplazadas por servicios automatizados que mueven dinero a través de capas de intercambios criptográficos, lo que hace que el proceso sea más rápido y más difícil de rastrear.
El lavado de dinero como servicio está claramente en el horizonte. Esto podría convertirse rápidamente en parte de la creciente cartera de CaaS. Y para las organizaciones y personas que son víctimas de este tipo de ciberdelincuencia, el paso a la automatización significa que el lavado de dinero será más difícil de rastrear, lo que reduce las posibilidades de recuperar los fondos robados.

Las ciudades virtuales dan la bienvenida a una nueva ola de ciberdelincuencia

El metaverso está dando lugar a nuevas experiencias totalmente inmersivas en el mundo en línea, y las ciudades son algunas de las primeras en incursionar en esta nueva versión de Internet impulsada por la realidad aumentada (AR), la realidad virtual (VR) y la realidad mixta (MR).
Estas ciudades virtuales prometen replicar experiencias y lugares de la vida real: las personas pueden crear avatares que luego pueden trabajar, jugar, comprar y más en un espacio virtual. Los minoristas incluso están lanzando productos digitales disponibles para su compra en estos mundos virtuales.
Sin embargo, si bien estos nuevos destinos en línea abren un mundo de posibilidades, también abren la puerta a un aumento sin precedentes de la ciberdelincuencia. Considere que el avatar de un individuo es esencialmente una puerta de entrada a su información de identificación personal (PII), lo que los convierte en objetivos principales para los atacantes.
Debido a que las personas pueden comprar bienes y servicios en ciudades virtuales, billeteras digitales, intercambios de cifrado, NFT y cualquier moneda utilizada para realizar transacciones, ofrecen a los actores de amenazas otra superficie de ataque. Estos bienes y activos virtuales también se pueden robar y revender. La piratería biométrica también podría convertirse en una posibilidad real debido a los componentes impulsados por AR y VR de las ciudades virtuales, lo que facilita que un ciberdelincuente robe el mapeo de huellas dactilares, los datos de reconocimiento facial y los escaneos de retina y luego los use con fines maliciosos.

Jugando el (ataque) juego largo

Desde FortiGuard Labs predicen que ciertas nuevas tecnologías ofrecerán a los ciberdelincuentes nuevas oportunidades de compromiso. Según lo que se sabe hoy sobre las tecnologías emergentes, como Web3, así como aquellas que parecen ser más desenfrenadas y destructivas que nunca, aquí hay varias predicciones a largo plazo sobre cómo podemos esperar que evolucione el panorama de amenazas, no solo en los próximos 12 meses, sino en los próximos años.

Wipeout

El malware Wiper ha tenido una rea-

parición espectacular este año, con atacantes que introducen nuevas variantes de este método de ataque de hace una década. Si bien el crecimiento en la prevalencia del malware de borrado en sí mismo es alarmante, anticipan que los actores de amenazas combinarán cada vez más varias amenazas para maximizar el nivel de destrucción continua que pueden causar.

Por ejemplo, un ciberdelincuente podría combinar fácilmente un gusano informático con malware de limpieza, lo que facilita que el malware se replique rápidamente y se propague más ampliamente. Dada la vulnerabilidad adecuada, dicho exploit podría causar una destrucción masiva en un corto período de tiempo. Esto hace que el tiempo de detección y la velocidad a la que los equipos de seguridad puedan remediar sean primordiales.

De cara al futuro, el uso de wipers en combinación con otros vectores de ataque es una de las mayores amenazas emergentes a las que nos enfrentamos como comunidad de seguridad. Los wipers pueden tomar potencialmente el ciberespacio por asalto, impactando las redes de TI en los sectores público y privado en todo el mundo.

El Salvaje Oeste de la Web3

Web3 es una nueva iteración de Internet basada en blockchain que tiene como objetivo descentralizar la propiedad de la economía digital. Se está convirtiendo rápidamente en la corriente principal, con un número cada vez mayor de corporaciones que comienzan a experimentar con las herramientas Web3. Y es fácil ver por qué: Web3 ofrece a las organizaciones muchos beneficios potenciales, como facilitar que los equipos de desarrollo implementen aplicaciones sin administrar y mantener una nueva infraestructura para respaldar ese proceso.

Pero al igual que cualquier nueva tecnología, Web3 no está exenta de riesgos de seguridad. Web3 se trata de que el usuario controle sus propios datos. Y si hay algo que hemos aprendido de los incidentes de seguridad anteriores, es que los usuarios suelen ser el eslabón más débil. Y aunque el aspecto irrever-

sible de blockchain ofrece algunos beneficios, también presenta desafíos. Por ejemplo, las billeteras Web3 de hoy no usan MFA, dependen solo de contraseñas y son difíciles de recuperar si se pierden.

Anticipamos que antes de que Web3 se generalice, veremos algunas regulaciones introducidas sobre cómo los nodos de red, los nodos que son responsables de mantener el estado de la red, abordan las actividades fraudulentas y los datos robados. Deben existir protocolos para que cuando se cometa un fraude, la actividad se pueda rastrear y contener de la misma manera que lo hacen los bancos cuando se comete un fraude no autorizado.

Señalice los preparativos del Q-Day

La computación cuántica comenzó hace más de cuatro décadas, pero en los últimos años, tanto las organizaciones del sector público como privado han incrementado sus inversiones en esta tecnología. Un reciente informe de McKinsey and Company afirma: "Si bien la computación cuántica promete ayudar a las empresas a resolver problemas que están más allá del alcance y la velocidad de las computadoras convencionales de alto rendimiento, los casos de uso son en gran parte experimentales e hipotéticos en esta etapa temprana". La computación cuántica ya está proporcionando un gran avance en cosas como romper algoritmos criptográficos previamente irrompibles.

Aunque ciertas capacidades de computación cuántica podrían no ser ampliamente aplicables o estar disponibles en la actualidad, algunos expertos advierten que el día cuántico (también llamado Q-Day), el punto en el que las computadoras cuánticas se vuelven lo suficientemente poderosas como para romper los mecanismos de encriptación actuales, se acerca rápidamente. Y mientras la comunidad de seguridad está trabajando para crear nuevos algoritmos de encriptación diseñados para hacer frente a las computadoras cuánticas, este esfuerzo aún es un trabajo en progreso.

Por ejemplo, hace solo unos meses, el NIST anunció los ganadores de un concurso de varios años en el que se pidió a los participantes que diseñaran nuevos estándares de cifrado que pudieran defenderse contra las computadoras cuánticas. Uno de estos algoritmos de encriptación poscuántica, Supersingular Isogeny Key Encapsulation, o "SIKE", para abreviar, sufrió rápidamente un ataque cibernético de una computadora de un solo núcleo que rompió con éxito la encriptación.

Sin duda, la computación cuántica evolucionará y se volverá más poderosa en el futuro, incluso más allá de su eventual capacidad para descifrar el algoritmo de cifrado. Debido a que la computación cuántica eleva las capacidades de procesamiento en una cantidad insondable, es posible que eventualmente los ciberdelincuentes las utilicen para actividades adicionales. Un ejemplo potencial son los malos actores que utilizan la computación cuántica para armar la IA y luego aplicarla a la aplicación fuzzing en la búsqueda de nuevas vulnerabilidades de día cero.

Defenderse contra el panorama de amenazas en evolución

Los actores de amenazas pueden estar ampliando sus respectivas bolsas de trucos, pero la buena noticia es que se están realizando numerosos esfuerzos para hacer retroceder el ecosistema del delito cibernético. El Departamento de Justicia (DOJ) vio victorias clave contra los operadores de ransomware este año. En enero, 14 miembros de la notoria pandilla de ciberseguridad REvil fueron arrestados en Rusia a petición de las autoridades estadounidenses.

Un mes después, dos personas fueron arrestadas en la ciudad de Nueva York. por conspirar para lavar las ganancias de 119.754 bitcoins que fueron robados de un cambio de moneda virtual e iniciaron más de 2.000 transacciones no autorizadas. Las fuerzas del orden han incautado más de 3600 millones de dólares en criptomonedas

vinculadas a ese hackeo hasta el momento.

Las asociaciones que se extienden a través de países y proveedores también están ayudando a identificar sindicatos de delitos cibernéticos. Como uno de los miembros fundadores de la Asociación contra el Cibercrimen (PAC) del Foro Económico Mundial (WEF), Fortinet se esfuerza por hacer esto con el proyecto Cybercrime ATLAS, una misión dedicada a mapear los ecosistemas cibercriminales para comprender mejor su plan y luego interrumpir. FortiGuard Labs comparte inteligencia y trabaja con varias organizaciones adicionales, que incluyen: Microsoft Active Protections Program (MAPP), Forum of Incident Response and Security Teams (FIRST), Cyber Threat Alliance (CTA), INTERPOL Global Crime Expert Group (GCEG) y Proyecto Gateway, Asociación Cibernética de la Industria de la OTAN (NICP), Centro de Ciberseguridad del Foro Económico Mundial y Centro de Ingenio MITRE para la Defensa Informada contra las Amenazas.

En lugar de centrarse únicamente en los operadores, se están realizando más investigaciones sobre los afiliados, lo que envía el mensaje de que no son inmunes al enjuiciamiento.

Comprender el ciclo de vida de un ciberataque

Para defender eficazmente su organización, debe comprender mejor a los ciberdelincuentes, sus motivaciones, sus tácticas y cómo actúan. El marco MITRE ATT&CK puede ayudar con esto, ya que documenta tácticas, técnicas y procedimientos comunes (TTP) que las amenazas persistentes avanzadas usan contra las redes empresariales. ATT&CK se puede usar de varias maneras para respaldar las operaciones de seguridad, la inteligencia de amenazas y la arquitectura de seguridad

Adopte una plataforma de malla de ciberseguridad

Una plataforma mallada de ciberseguridad amplia, integrada y automatizada es esencial para reducir la complejidad y aumentar la eficacia de la seguridad, especialmente a medida que las redes se expanden y los malhechores encuentran cada vez más nuevas formas de llevar a cabo sus ataques.

Tradicionalmente, las defensas de ciberseguridad se han implementado una solución a la vez, generalmente en respuesta a un desafío emergente. Pero una colección de soluciones puntuales no es efectiva en el panorama actual. La consolidación y la convergencia en una sola plataforma de ciberseguridad son cruciales, ya que permiten una integración mucho más estrecha, una mayor automatización y una protección y respuesta más rápida, coordinada y efectiva a las amenazas en toda la red.

Para permitir una respuesta rápida y coordinada, las soluciones de seguridad deben mejorarse con IA para que puedan detectar patrones de ataque y detener las amenazas en tiempo real. Las soluciones también deberían poder escalar para abordar el aumento de los ataques

Implementar segmentación y microsegmentación de red

La segmentación de la red ofrece muchos beneficios para las empresas. La segmentación mejora la seguridad al evitar que los ataques se propaguen por una red y se infiltren en dispositivos desprotegidos. En caso de un ataque, la segmentación también garantiza que el malware no pueda propagarse a otros sistemas empresariales.

La microsegmentación es una técnica de seguridad de red que permite a los arquitectos de seguridad segmentar aún más un entorno para una visibilidad lateral de todos los activos en el mismo dominio de transmisión. La granularidad se logra dividiendo lógicamente el entorno de red en distintos segmentos de seguridad hasta el nivel de carga de trabajo individual. Dado que las políticas se aplican a cargas de trabajo individuales, la microsegmentación ofrece una mayor resistencia a los ataques. Y si ocurre una infracción, limita la capacidad de un pirata informático para moverse entre las aplicaciones comprometidas.

Descargue aquí el informe

Amenazas de seguridad en entornos de Nube

By Huawei

Los entornos de datos y computación en la nube son cada vez más versátiles, flexibles, accesibles y móviles. De esta manera, debemos asegurarnos de que las personas, las empresas, las organizaciones y los gobiernos sean conscientes de las amenazas a la seguridad que existen en estos entornos. En pocas palabras, ningún entorno es completamente seguro.

1 - Entornos de Nube: ¿Una puerta abierta a las amenazas de seguridad?

En los últimos años, los dispositivos y las personas se han vuelto más conectados a Internet, compartiendo información y recursos computacionales, colaborando, generando o consumiendo una gran cantidad de datos. Particularmente en estos dos últimos años, la transición al trabajo, el juego y la educación a distancia se ha acelerado, allanando aún más la era del "mundo hiperconectado". Como una forma de apoyar el procesamiento y almacenamiento necesarios, la nueva era de Internet también cuenta con el soporte de la tecnología de computación en la nube (o, del inglés, Cloud Computing). En la última década, la computación en la nube ha evolucionado desde servicios esencialmente de almacenamiento a servicios más complejos, como Software como Servicio (SaaS), Plataforma como Servicio (PaaS), Infraestructura como Servicio (IaaS.

Sin embargo, el potencial que ofrece la computación en la nube y sus máquinas virtuales rara vez se utiliza hoy en día para la ciberseguridad. Además, los desafíos para mantener seguros los entornos en la nube son enormes y difieren de la seguridad en entornos convencionales, ya que un entorno en la nube tiene diferentes niveles de responsabilidad con respecto a la seguridad cibernética.

Amenazas Crecientes

Resultados del Ponemon Institute, que desde el año 2002 ha llevado a cabo de forma independiente investigaciones y educación relacionadas con la información y la privacidad, indican que las amenazas a la seguridad interna han aumentado en número y frecuencia y que desde el año 2020 dichas amenazas casi se han duplicado.

Los principales ciberataques están relacionados con el ataque de secuestro de datos, más conocido como ataque de ransomware. A modo de ejemplo, Sophos publicó en su informe de investigación "The State of Ransomware 2021". De las respuestas, el 37% de las organizaciones fueron afectadas por el ransomware en 2021, el 54% de las empresas afectadas

dijo que los cibercriminales fueron capaces de cifrar sus datos más significativos en el ataque y el 96% de aquellos cuyos datos fueron cifrados recuperaron sus datos, no necesariamente después de que pagar el rescate.
Vemos un aumento en el número y la diversidad de las violaciones de seguridad, pero lo más preocupante es la falta de comprensión de las muchas formas en que pueden ocurrir las violaciones de seguridad y, lo que es más importante, el escaso conocimiento de cómo se pueden seguir pasos simples para evitar la pérdida de datos personales o empresariales.

Nueva Forma de Trabajar y su Impacto en la Seguridad

Las prácticas de trabajo flexibles también se están consolidando en las instituciones. El "hot desking", en el que las personas se mueven por la oficina y usan el espacio cuando y donde lo necesitan, desafía la organización tradicional de la oficina y crea posibles problemas de ciberseguridad donde los empleados tienen diferentes niveles de autorización de seguridad o antigüedad.
Este entorno permite a los empleados acceder a datos, infraestructura, software y otros recursos informáticos que ofrece la empresa a través de computadoras, portátiles, tabletas o teléfonos inteligentes, siempre y cuando estén conectados a Internet. El entorno de nube se considera más seguro para la institución que la administración de los recursos informáticos por parte de la propia institución.

2. Computación en la Nube

Hoy en día, existen varios proveedores de servicios de computación en la nube (PSCC), por Ej, instituciones que ofrecen servicios en la nube. Un ejemplo de ellos es Huawei Cloud. Sin embargo, hay otras empresas tecnológicas ofrecen este tipo de servicios desde las más conocidas hasta las menos conocidas. Los principales servicios en la nube que se ofrecen son: Software como Servicio (SaaS), Plataforma como Servicio (PaaS) e Infraestructura como Servicio (Iaas).
Los entornos de nube pueden ser de tres tipos principales: públicos, privados e híbridos. El entorno de nube privada es el modelo que proporciona mayor seguridad y flexibilidad. El acceso a este entorno es a través de una sola institución, lo que hace que ésta pueda operarlo con mayor control y privacidad.

3. Amenazas de Seguridad en el Entorno de Nube

Teniendo en cuenta el funcionamiento y la arquitectura de los entornos de nube, es importante destacar que existen riesgos para la seguridad (confidencialidad, integridad y disponibilidad) y para la privacidad de los sistemas e información, tales como:
- Fuga y acceso no autorizado a datos entre máquinas virtuales que operan en el mismo servidor
- Falla de un proveedor de entorno de nube de proteger y gestionar información y datos confidenciales

- Divulgación de datos confidenciales o críticos a las autoridades y agencias gubernamentales sin la aprobación/conocimiento del usuario
- Fallas del sistema que pueden hacer que el servicio en la nube no esté disponible durante un largo período de tiempo
- Compromiso de las aplicaciones del cliente alojadas en el entorno de nube
- Acceso a información confidencial y propagación de software malicioso

El entorno de nube aumenta el potencial de amenaza debido a su complejidad y a la ausencia de una visión y control holísticos por parte del cliente/usuario. En este contexto, cuando nos referimos a las ciberamenazas en entornos cloud, las amenazas que más destacan por estas características se engloban brevemente en: Ataque de denegación de servicio; Amenazas internas; Menor visibilidad de la infraestructura; Uso no autorizado de la carga de trabajo del entorno de nube; APIs inseguras; Ransomware y fuga de datos; Configuración incorrecta del entorno de nube; Temas Relacionados con el Cumplimiento y las Regulaciones.

Otro factor que potencia las botnets y los ataques DDoS son los servicios ofrecidos en Internet para generar estos ataques, también conocidos como DDoS como servicio o Malware como servicio. Es importante identificar y definir, como referencia, el comportamiento del tráfico normal para poder detectar cualquier comportamiento anormal. En este último punto sobre la detección de anomalías, las técnicas avanzadas de Ciencias de Datos, Inteligencia Artificial y Machine Learning pueden ayudar significativamente.

Amenazas Internas

Hasta el 43% de las violaciones de seguridad se originan dentro de la organización. Los ataques internos pueden ser maliciosos (como en el caso de empleados insatisfechos) o no intencionales. La formación y la concienciación adecuadas son la clave para mitigar los ataques de información privilegiada, junto con un estricto control y políticas de acceso y uso. Seguir los principios de mínimo privilegio y confianza cero es una buena práctica a la hora de diseñar controles de acceso al entorno de nube para limitar el daño que los empleados pueden causar.

Menor Visibilidad de la Infraestructura

La naturaleza del uso de un proveedor externo para la computación significa ceder el control parcial de la infraestructura al proveedor de servicios en la nube. En este caso, la institución no es propietaria de la infraestructura física, por lo que es difícil tener una visibilidad completa de su infraestructura y uso de recursos, especialmente sin los conocimientos técnicos adecuados. El entorno de nube opera bajo un modelo de responsabilidad compartida entre el cliente y el proveedor de servicios en la nube. Si bien esto significa que el proveedor realiza la gestión de la infraestructura física, sigue siendo responsabilidad

de la empresa garantizar que la carga de trabajo de los datos y las aplicaciones en la nube permanezca segura.

Uso no Autorizado de la Carga de Trabajo en la Nube

La mayoría de los grandes proveedores operan en un modelo de autoservicio. Esto facilita que los usuarios aprovisionen y desprovisionen cargas de trabajo en tiempo real en función de sus necesidades. Por otro lado, esta facilidad de uso también conlleva lo que se denomina Shadow IT, o recursos de TI que los usuarios crean y utilizan sin el conocimiento del personal de TI. Shadow IT conlleva su propio conjunto de riesgos, que incluyen (pero no se limitan a): Mayor riesgo de pérdida y fuga de datos; Costos inesperados; Infracciones de cumplimiento.

Para evitar esta amenaza, es esencial asegurarse de cumplir con el principio de mínimo privilegio y autorizar la creación de cargas de trabajo sólo a los usuarios que lo necesiten como parte de su trabajo.

APIs Inseguras

Incluso con controles estrictos en la infraestructura, las API de aplicaciones inseguras pueden traspasar las defensas del entorno de nube y crear una puerta de entrada para los atacantes. Muchas API tienen sus propias vulnerabilidades de seguridad que, cuando se explotan, pueden poner en riesgo el entorno en la nube. Para mitigar esta amenaza, es necesario que el personal de TI revise todas las aplicaciones externas que cualquier equipo planea usar y esté al tanto de cualquier riesgo antes de la implementación.

Ransomware

El entorno de nube ha sido objeto de gran interés para los ciberdelincuentes relacionados con este tipo de secuestros. Ya existen diferentes variantes de ransomware que han demostrado ser capaces de atacar datos en la nube y utilizar tecnologías basadas en ella. Ejemplos de estas variantes son Jigsaw, Petya, RANSOM_CERBER.cad y Ransomcloud.

Configuración Incorrecta del Entorno de Nube

La infraestructura en la nube requiere una serie de configuraciones. Una parte de la responsabilidad de estos ajustes es del proveedor de entorno de nube y la otra parte en del cliente/usuario. Dependiendo del tipo de servicio (SaaS, PaaS e IaaS), el grado de responsabilidad de la configuración recae más en el proveedor que en el cliente/usuario.

En todos los casos, tanto el cliente/usuario como el proveedor tienen un porcentaje de responsabilidad en los ajustes y éstos deben realizarse correctamente. A continuación, se muestran algunos de los problemas de configuración más comunes que se encuentran en la infraestructura de nube.

- Almacenamientos de acceso público.
- Controles de acceso a recursos inseguros.
- Credenciales expuestas en repositorios públicos.

Temas Relacionados con el Cumplimiento y las Regulaciones

Con la aparición de nuevas normativas y la actualización de las más antiguas a medida que cambia el escenario, puede ser un desafío para las organizaciones mantenerse al día. El cumplimiento continuo de las normas en la nube demuestra ser la principal solución a los problemas normativos. Esto significa monitorear constantemente la postura de cumplimiento en la nube, en lugar de trabajar sólo durante la temporada de auditorías.

4. Responsabilidades de Seguridad en el Entorno de Nube

En general, la responsabilidad de seguridad asigna el grado de control que cualquier actor tiene sobre la pila de arquitectura:

- Software como Servicio: El proveedor de servicios de computación en la nube es responsable de

casi toda la seguridad, ya que el usuario de la nube puede acceder y gestionar el uso de la aplicación, pero no puede cambiar su funcionamiento.

- Plataforma como Servicio: El proveedor de servicios en la nube es responsable de la seguridad de la plataforma, mientras que el cliente es responsable de todo lo que implementa en la plataforma, incluyendo cómo configura las características de seguridad ofrecidas.
- Infraestructura como Servicio: Al igual que PaaS, el proveedor es responsable de la seguridad fundamental, mientras que el usuario de la nube es responsable de todo lo que desarrolla sobre la infraestructura. A diferencia de la PaaS, pone mucha más responsabilidad en el cliente.

La comprensión del modelo de responsabilidades y estas pautas se pueden correlacionar y resumir en dos recomendaciones principales:

- El proveedor debe documentar claramente el control de seguridad interna y los atributos de seguridad del cliente. Los proveedores deben diseñar e implementar estos controles de seguridad.
- Los usuarios del entorno de nube deben tener un mapeo de las responsabilidades y documentar quién está implementando los controles de seguridad y cuáles. Este mapeo debe tener en cuenta las regulaciones y normas de cumplimiento vigentes.

5. Mejores Prácticas

Conocer en detalle la organización, sus políticas y cómo actúa es fundamental para construir un plan e innovar en este ámbito. ¿Qué es lo que realmente pretende proteger? ¿Qué es importante proteger?

Un primer paso para responder a estas preguntas es crear un inventario de los activos de la organización. Es necesario saber dónde se aloja el activo, conocer los acuerdos de nivel de servicio y las garantías que ofrece el proveedor en la nube donde se aloja el activo, saber qué ofrece el proveedor en términos de protección y seguridad y cuáles son las responsabilidades del cliente.

Una segunda mejor práctica para garantizar el entorno de nube es automatizar el proceso de descubrimiento de aplicaciones y servicios. Este descubrimiento ayuda a crear la lista de aplicaciones, servicios y sus datos.

Definir un equipo de ciberseguridad es una tercera buena práctica. El equipo necesita realizar un seguimiento de este inventario, conocer los servicios, definir e implementar protecciones contra las amenazas de seguridad en el entorno de nube.

La cuarta mejor práctica es definir un plan de gestión de riesgos. Es el resultado de acciones tales como la identificación de datos sensibles, la clasificación de datos y servicios, la definición de niveles de acceso permitidos a los usuarios y las formas de implementar la política de acceso, la supervisión de accesos, la gestión de accesos remotos, la protección con contraseñas y la identificación de los requisitos de seguridad y privacidad por aplicación y servicios.

La quinta mejor práctica es tener una política que defina los niveles de privilegios para los usuarios de la nube basándose en el principio de confianza cero.

6. Conclusiones

Cabe señalar que ninguna de las amenazas enumeradas en el presente informe es nueva desde el punto de vista de la ciberseguridad. Sin embargo, el panorama cambiante y la transición a la nube requieren diferentes enfoques en comparación con las cargas de trabajo locales más antiguas. Ser proactivo no sólo evita que surjan problemas más grandes y costosos, sino que también ayuda a construir la reputación de la organización y permite que ésta se centre en las tareas que añaden valor a su actividad final.

Descargue aquí el informe

channeltalks

23 eventos en toda Latinoamérica y Centroamérica

LINEUP 2023

Uruguay
MONTEVIDEO

Chile
SANTIAGO

CONCEPCIÓN

Argentina
ROSARIO

NEUQUÉN

MAR DEL PLATA

TUCUMÁN

SANTA FE

CORRIENTES

CÓRDOBA

MENDOZA

BUENOS AIRES

Bolivia
COCHABAMBA

LA PAZ

SANTA CRUZ

Paraguay
ASUNCIÓN

CIUDAD DEL ESTE

Costa Rica
SAN JOSE

Perú
LIMA

AREQUIPA

Ecuador
QUITO

Colombia
BOGOTA

Jamaica
KINGSTON

SitioSimple

Crear tu página web es tan rápido como leer esta publicidad

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

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

ESCANEÁ
Y EMPEZÁ GRATIS

DonWeb.com