CYBERSECURITY
by itwarelatam.com

Edición - N°16

La revista de Cloud Security

INFORME ESPECIAL

Ransomware 2.0: el año en que vivimos en peligro

MÁS TEMAS

EDICIÓN N°16

NOTA DE TAPA

RANSOMWARE 2.0: EL AÑO EN QUE VIVIMOS EN PELIGRO

04

SUMARIO

La Ciberseguridad sigue en primera línea

Tienen ante sí un nuevo número, bajo nueva dirección editorial, pero manteniendo la calidad que han sabido apreciar ustedes lectores durante todo este tiempo.

En este caso la nota principal es sobre un tema muy candente y que está afectando desde individuos hasta empresas, causando pérdidas millonarias, exponiendo tus datos más sensibles, impactando en la operatoria de las compañías, y destrozando muchas vece la imagen de las mismas, con la influencia que esto tiene en la fidelidad de sus clientes y usuarios.

Sí, hablamos del ransomware. Pero no cualquiera, no el que tuvo sus orígenes décadas pasadas, sino el que resurgió con fuerza en los últimos tres o cuatro años, y ha pasado de ser una amenaza no tan distribuida, a ser un negocio de bandas profesionales que incluso venden herramientas para que hackers menos expertos también puedan vulnerar tus datos. El muy mentado Ransomware 2.0, o como muchos los denominan el Ransomware-as-a-service.

Pero eso no es todo, también hablamos sobre otros temas de actualidad, como es el de la falta de talentos en ciberseguridad, y cómo encontrarlos, capacitarlos y retenerlos. O los desafíos de los CISOs en un momento tan crucial de aumento de ciberataques. Y más.

Así que los invito a disfrutar de este número. Hasta la próxima.

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

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

RANSOMWARE 2.0: EL AÑO EN QUE VIVIMOS EN PELIGRO

Por Fernando Juliá

Transitamos en un mundo donde la digitalización profunda ha traído como consecuencia que también aumenten en la misma medida los ataques cibernéticos, muchas veces aprovechándose de faltas de medidas de seguridad, vulnerabilidades existentes, o hasta fallos humanos. Una de las amenazas más preocupantes es el Ransomware, e ITWare Latam consultó a varios expertos sobre el tema

El ransomware no es nuevo. Eddy Willems, un trabajador de una compañía de seguros de Bélgica, es una de las primeras víctimas del mismo en la historia de la informática. En 1989 su jefe le pidió que comprobara qué había en un disquete que había recibido de la OMS. Se esperaba una investigación médica sobre el SIDA, se encontró con un hackeo que le pedía 189 dólares.
Pero desde entonces este malware ha sufrido grandes cambios, se ha transformado en uno de los ataques que más preocupan a individuos, empresas y hasta gobiernos.
Según un informe de Check Point Software la media semanal global de organizaciones impactadas por ransomware alcanza ahora 1 de cada 40, lo que supone un aumento del 59% interanual (1 de cada 64 compañías en el segundo trimestre de 2021).

> “Hoy contamos con una gran evidencia sobre los ataques a las empresas. Es responsabilidad del profesional IT tomar las medidas básicas de seguridad para enfrentar de la mejor manera posible un ataque cuando suceda.
> **Leonardo Giordano, Cisco**”

Según el mismo reporte, América Latina experimentó el mayor aumento de los ataques, con 1 de cada 23 organizaciones impactadas semanalmente, lo que supone un aumento del 43% interanual, en comparación con 1 de cada 33 en el segundo trimestre de 2021.

Por su parte, WatchGuard Technologies. como resultados de su Informe de Seguridad en Internet trimestral, hallaron que las detecciones de ransomware en el primer trimestre de este año duplicaron el volumen total informado para 2021, la red de bots Emotet regresó a gran escala, la vulnerabilidad del Log4Shell triplicó sus esfuerzos de ataque, aumentando la actividad maliciosa de cryptomining y mucho más.

Asimismo, Fortinet revela que el crecimiento de variantes de ransomware muestra la evolución de los ecosistemas delictivos:

Leonardo Giordano

el ransomware sigue siendo una de las principales amenazas y los adversarios cibernéticos continúan invirtiendo recursos significativos en nuevas técnicas de ataque. En los últimos seis meses, FortiGuard Labs ha visto un total de 10.666 variantes de ransomware, en comparación con solo 5400 en el período de seis meses anterior. Eso es casi un 100% de crecimiento en variantes de ransomware en medio año.

En este constante cambio, ¿a qué se enfrentan las empresas hoy en día con respecto al ransomware?

La llegada del Ransomware 2.0

“Se denomina Ransomware 2.0 a la doble extorsión

que realizan últimamente los ciberdelincuentes, donde no solo piden rescate por la información secuestrada y cifrada, sino que también lo hacen para evitar que se distribuya esta información en la Clear, Deep y/o Dark web", comenta David López, vicepresidente de ventas para Latinoamérica de AppGate.

Los ciberdelincuentes han dado un paso más ofreciendo Ransomware como servicio o RaaS (del inglés Ransomware as a Service). En esta forma de explotación los cibercriminales crean un kit malicioso compacto capaz de lanzar un ataque de ransomware. Este kit lo venden/alquilan a los interesados bajo un programa de afiliación a otros cibercriminales que tienen la intención de lanzar un ataque. Además del software les proporcionan: conocimientos técnicos e información paso a paso sobre cómo lanzar un ataque.

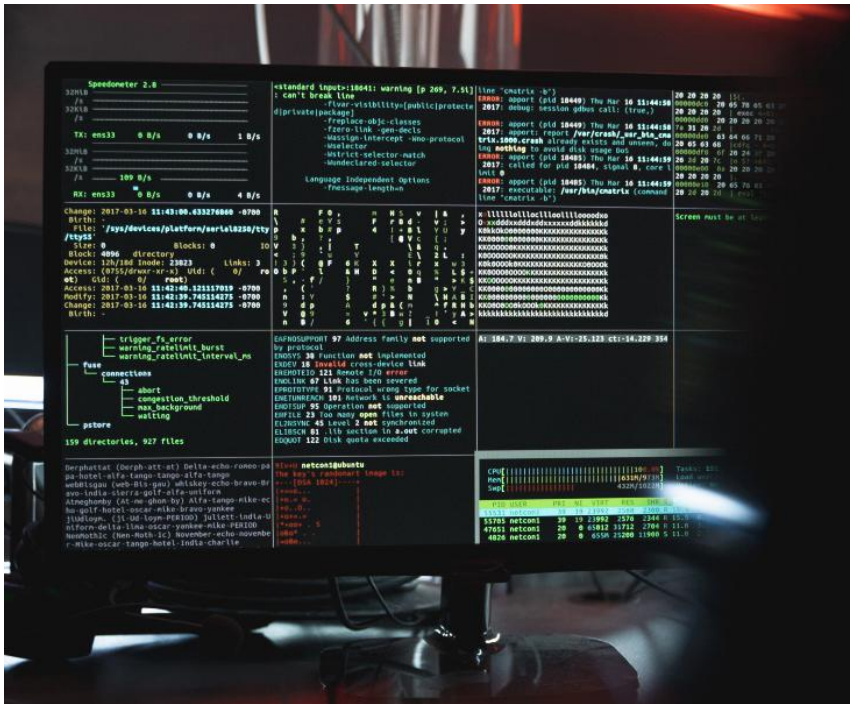
"Ransomware 2.0 es la inclusión de la extorsión y el chantaje como una nueva estrategia, donde los piratas informáticos amenazan con publicar en Internet los

Fabio Assolini

datos confidenciales robados si no se realiza el pago. Esta segunda etapa se caracteriza como una segunda extorsión o doble extorsión", sostiene Bruno Lobo, General Manager Commvault LATAM.

Por su parte, Fabio Assolini, Director del Equipo de Investigación y Análisis para América Latina de Kaspersky, declara que los ataques de ransomware como WannaCry normalmente solicitan un rescate para devolver el acceso a los datos cifrados por el malware, "pero en una reciente ola de ataques que ha empezado el 2020, los ciberdelincuentes hacen dos extorsiones: primero los ataques cifran los datos y después ellos también amenazan con publicar la información confidencial en línea. Otra diferencia es que los ataques ahora son más selectivos, es decir, los ciberdelincuentes eligen previamente cuáles son las empresas que van a atacar y hacer todo lo posible para tener éxito".

Como explica Martín Colombo, Country Manager en Veeam Argentina, esto requiere un análisis profundo sobre cómo se deben proteger los datos: "Así como las soluciones de seguridad, resguardo y backup de datos se perfeccionan, también los ciberdelincuentes encuentran nuevas formas de mejorar la forma en la que operan. El procedimiento más común de los ciberatacantes que utilizaban el ransomware era ingresar a los centros de datos, encriptarlos y pedir rescate. Hace un tiempo tomaron como regla la amenaza de publicar esos datos. Una de sus prácticas más utilizadas es destruir los repositorios de datos, para hacer creer a las organizaciones que no hay otra alternativa que pagar para recuperar la información".
Desde Fortinet, Arturo Torres, estratega de ciberseguridad de FortiGuard Labs



para América Latina y el Caribe, agrega que “Ransomware 2.0 es una modalidad evolucionada de ransomware, la cual consiste en realizar técnicas de doble o triple extorsión, el principal objetivo de los cibercriminales es presionar a las compañías no solo para devolver la información encriptada, si no para no filtrarla y/o venderla en foros. En esta modalidad los cibercriminales logran copiar toda la información contenida en los activos digitales de la empresa antes de encriptarla a diferencia del ransomware tradicional donde sólo buscaban secuestrarla, para después pedir dinero”.

A su vez, Leonardo Giordano, Country Manager de Cisco para Argentina, Uruguay y Paraguay, comenta sobre los cambios de esta amenaza: “En una evolución a los ransomware tradicionales y automáticos, en los que el ataque se generaba de una forma masiva y las víctimas variaba económicamente. Estos formatos, además de ser menos rentables, requieren un esfuerzo mayor hasta humano para poder concretar el ataque. La versión 2.0 trae consigo sofisticación y una combinación de diferentes técnicas mejoradas”.

La evolución de una amenaza: de simple ataque a negocio internacional

Una de las características más notables de la evolución del ransomware es cómo ha mutado de ser una amenaza puntual realizada por hackers individual es, a transformarse en un emprendimiento empresarial. con grupos conformados especialmente para realizar los ataques. Así lo explica Leonardo Giordano, de Cisco: “La mejora de la automatización de la industria organizada delictiva o “Gags”, sobre las rans, ya que previo a los ataques a grandes empresas, realizan estudios del negocio, infraestructura y rentabilidad de la misma para lograr una negociación favorable, para lograr una cadena de ataque profesional y efectivo”.

Desde Fortinet, Arturo Torres toma datos del último informe de FortiGuard Labs y suma que han visto que el ransomware es lo que más sigue creciendo, y que tan sólo en Latinoamérica este año se reportaron un total de 137 mil millones de intentos de ciberataques, de estos 52.000 corresponden a intento de ransomware. Pero no se queda allí y agrega,

“Además del mayor uso de Ransomware-as-a-Service (RaaS) donde los creadores de ransomware lo entregan a terceros a cambio de un pago mensual o una parte de las ganancias obtenidas, hemos observado que algunos actores de ransomware ofrecen a sus víctimas Servicio de soporte técnico 24/7 para agilizar el pago del rescate y la restauración de sistemas o datos encriptados. Los cibercriminales han convertido el ransomware en un modelo de negocio sumamente profesional y bien establecido”.

Esto tiene como consecuencia una ampliación del área de ataque y las fuentes del mismo. Como comenta Martín Colombo, de Veeam: “El ransomware ha dejado de ser una posible amenaza para las empresas y ha pasado a ser algo inevitable. El Informe de Tendencias de Ransomware 2022 de Veeam muestra que el 76% de las organizaciones sufrieron al menos un ciberataque en el 2021, lo que supone un aumento del 15% interanual. En promedio, sólo pudieron recuperar un 69% de sus datos. En nuestra región sufrieron un ataque el 47 % de los servidores de centros de datos, 49 % de

Bruno Lobo

las oficinas remotas y 46 % de las instancias en la nube. Un aspecto quizá más alarmante es la eficacia de los atacantes para destruir, de forma proactiva, los repositorios de backup de datos”. Pero esa masividad de ataques no significa que sean realizados al azar: cada día se ve más cómo los ciberdelincuentes seleccionan a sus víctimas. Así lo ejemplifica Fabio Assolini, de Kaspersky: “Tenemos que evaluar la evolución en dos puntos de vista: ataques totales y los ataques dirigidos. Los ciberdelincuentes están cambiando de ataques masivos para ataques donde eligen su víctima previamente, así lo confirman las estadísticas de ransomware de Kaspersky disminuyeron un 56% en 2021. Pero si evaluamos solamente a los grupos que trabajan de forma dirigida, hubo un incremento de más de un 200% en Latinoamérica. Entre las tendencias que hemos identificado, están la aparición de nuevos grupos como el BlackCat y el uso de herramientas legítimas (de Red Teaming) para hacer los ataques”.

Esta visión de ransomware como negocio y servicio es reforzada por Bruno Lobo, de Commvault: “El ransomware como servicio es un modelo basado en suscripción que permite a los afiliados utilizar herramientas ya desarrolladas para realizar ataques. Los afiliados ganan un porcentaje de cada pago de canje exitoso. Este es un caso de adopción del modelo de negocio de Software como Servicio (SaaS). En el pasado, la codificación era un requisito para todos los hackers exitosos, pero ahora, con la introducción del modelo RaaS, este requisito técnico se ha diluido por completo. Al igual que todas las soluciones SaaS, los usuarios no necesitan ser expertos o incluso experimentados para usar la herramienta con competencia. Estas soluciones, sin embargo, permiten incluso a los hackers más innovadores

ejecutar ataques cibernéticos altamente sofisticados".

Esta evolución ha tenido como consecuencia la aparición de grupos internacionales específicamente armados para realizar ataques de ransomware, tal como señala David López, de AppGate: "En los últimos años hemos visto cómo este tipo de ciberataques se ha posicionado en los primeros lugares de amenazas en ciberseguridad. Para el 2021 se calcularon unas 61 organizaciones impactadas por esta modalidad en todo el mundo. Además, sectores de ISP (Internet service provider) y MSP (managed service provider), junto al sector salud y de software fueron los más afectados por esta modalidad; ya que se ha popularizado un modelo de negocio basado en Ransomware as a service (RaaS), que busca millonarias recompensas por el rescate de los datos o sistemas secuestrados. Se espera que estas sumas lleguen en corto tiempo a los 100 millones de dólares como demanda de un solo rescate".

No se salva nadie

Una de las consecuencias de la transformación de este tipo de ataques es que se suma cada vez más gente que los realiza, y se diversifican los objetivos, ampliando la cantidad de empresas o individuos que pueden sufrirlos.
Es por eso que David López, de AppGate, asegura que todas las industrias y empresas pueden ser susceptibles a un ataque, pero unas pueden ser más fructíferas para los criminales: "Por ejemplo, los sectores asociados con productos o servicios de software e internet son bastante atractivos por la cantidad de actividades que se desarrollan digitalmente, y que pueden quedar paralizadas en un ataque de ransomware, afectando la compañía en cuestión, y a sus clientes".
"También se han popularizado los ataques al sector industrial, en los que secuestran los sistemas OT y IoT, y bloquean las operaciones productivas o de logística, como en el caso de Colonial Pipeline o de JBS. Además, es el sector financiero el principal objetivo del phishing con un 23,2% de los casos. Los cibercriminales aprovechan los mecanismos de autenticación anticuados como Usuario/Contraseña para acceder a las cuentas y generar pérdidas económicas a los usuarios e instituciones", agrega López.

> "La mejor protección contra el ransomware es la prevención y el bloqueo del intento de ataques.
> **Fabio Assolini, Kaspersky**"

No por nada Bruno Lobo, de Commvault, comenta que "Todos los segmentos o tamaños de empresas están sujetos a ataques, pero especialmente los sectores de educación, gobierno, comercio minorista, comercio electrónico y finanzas, donde los datos tienen un valor muy alto o tienen un impacto muy grande".

Fabio Assolini, de Kaspersky, es más rotundo en su comentario sobre qué tipo de empresas son las más afectadas, y responde con un "¡Todos!", a lo que agrega que "No hay un segmento específico para los ataques. Los ciberdelincuentes evalúan el potencial de ganancia de la víctima, o sea, si la empresa es rentable. Tomando esto como referencia, un análisis de Kaspers-

ky midió el porcentaje de solicitudes de respuesta a incidentes relacionadas con ransomware y el resultado fue que los sectores de gobierno, industrial y empresas de tecnología y finanzas tuvieron más solicitudes".

Martín Colombo, de Veeam, se hace eco de un informe de Statista, que dice que, durante el 2021, a nivel mundial, los ataques de ransomware fueron dirigidos principalmente a instituciones gubernamentales, educativas, al sector de salud, de servicios y tecnología, pero no deja de remarcar que igualmente "Actualmente, todos los sectores son vulnerables al ransomware".

> "Una Estrategia Moderna de Protección de Datos es hoy un diferencial de su negocio. Es la garantía de que la organización se preocupa por cuidar un activo vital como lo son los datos hoy en día.
> **Martín Colombo, Veeam**"

Aunque para Arturo Torres, de Fortinet, ninguna industria se salva de este tipo de ataques, en su experiencia "las más vulnerables tienden a ser las industrias críticas de un país: gobierno, minería, banca, e incluso salud. El ransomware se ha convertido en un modelo de negocio bien estructurado lo cual implica que cada grupo criminal tiene un objetivo diferente que puede ir desde desestabilizar la política o economía de un país, hasta simplemente un beneficio monetario propio".

Por su lado, Leonardo Giordano, de Cisco, pasa algo de la responsabilidad a las empresas, y que las que son objetivo de ataques son aquellas que no cuenten con seguridad informática, y por lo tanto son las más indefensas. Pero agrega que "Los sectores con más capital, siempre son los blancos de los estafadores, como los retail, bancos, centros médicos, etc. Pero a que su vez, se van preparando e invirtiendo en seguridad informática".

¿Hay forma de defenderse?

Ante un panorama tan acuciante, es menester que las empresas se pregunten si están lo suficientemente preparadas para hacer frente a este tipo de ataques, o saber

Martín Colombo

qué medidas deben tener que tomar. Y los expertos que participan de este informe presentan varios puntos de vista al respecto.

Por ejemplo, para Leonardo Giordano, de Cisco, en general hay un consenso de términos tecnológicos y hay dos puntos que permiten a una empresa dar aviso previo al ataque: "Lo más importante es implementar un mecanismo de control de acceso a los recursos que utilicen (nubes, aplicaciones, etc.). El primer punto a tener en cuenta es contar con un MFA (Multifactor authentication). Podemos agregar un segundo punto que es la seguridad por DNS" .

Al respecto, Arturo Torres, de Fortinet, también señala que existen dos medidas básicas

a impulsar: “Por un lado, contar con soluciones que sean amplias, automatizadas, e integradas, que puedan crecer conforme las necesidades de cada empresa lo vayan requiriendo que abarquen todo el espectro de la red y ayuden a liberar las cargas de los equipos de TI. En segundo lugar y no menos importante, promover una cultura de ciber higiene en nuestros colaboradores, esto es igual de importante que la infraestructura de seguridad, casi todos los ataques que llegan a las empresas se derivan del error humano, ya sea por conexiones no seguras o correos de phishing, por eso es vital contar con campañas, y capacitaciones que enseñen a la fuerza laboral a detectar estas amenazas y reportarlas”.

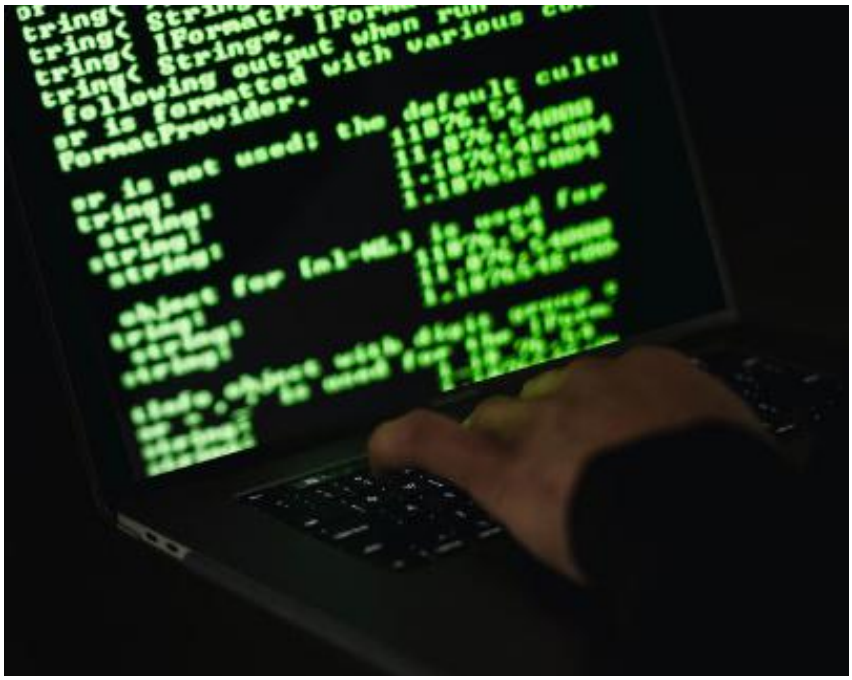
El trabajo y la supervisión continua son parte de las medidas de defensa, como comenta Martín Colombo, de Veeam: “Realizar monitoreos constantes en el entorno IT, implementar más encriptación «nearline», cifrando las copias de seguridad en cada etapa, y tener buenas prácticas de higiene digital entre los colaboradores son tres maneras de prevenir y detectar ataques a gran escala. Para el cuidado y resguardo de los datos, tener una estrategia moderna de protección es vital, para ello, sugerimos implementar la regla 3-2-1-1-0: siempre debe haber al menos tres backup de los datos importantes, en al menos dos tipos diferentes de medios, con al menos una fuera de las instalaciones, una en un medio offline, con cero copias de seguridad no verificadas o con errores”.

> “Esté siempre preparado para enfrentar las amenazas cibernéticas, sucederán, la diferencia será la preparación de las empresas y su rápida respuesta.
> **Bruno Lobo, Commvault**

Mientras, Bruno Lobo, de Commvault, es más directo: “Lamentablemente no existe una bala de plata, pero debemos aplicar múltiples capas de protección, siguiendo el Marco de Seguridad Cibernética del NIST (nist.gov), que define 5 puntos fundamentales: Identificación, Protección, Monitoreo, Respuesta y Recuperación. Podemos destacar las tecnologías basadas en Deception que pueden ayudar a evitar que los ataques se inicien y progresen dentro de la infraestructura del cliente”
.
Desde AppGate señalan que la solución más completa para las organizaciones empieza por la adopción de un paradigma preventivo a partir de una filosofía Zero Trust, en la que se evalúa constantemente a cada uno de los usuarios, dispositivos y conexiones como una potencial entrada de ciberataques. “El Zero Trust Network Access, articula un conjunto de tecnologías para un entorno seguro alrededor de los trabajadores e identidad, sin exponer los puertos a Internet. Además, las soluciones SDP permiten tener un control total sobre los ingresos, privilegios y alcances de cada uno de los colaboradores y clientes, para controlar sus acciones y disminuir al máximo la exposición al riesgo”.

“Lo ideal es acompañar estas estrategias con tecnologías de vanguardia que superen las anticuadas formas de autenticación, optando por modelos de Biometría, uso de Tokens, Push, códigos QR o Reconocimiento Facial. De esta forma,

se evita el robo de identidad y credenciales de acceso, que ponen en riesgo a los usuarios y a los sistemas", complementa David López, de la empresa.



Qué hacer si ya se realizó el ataque

Muchos expertos aseguran que el tema no es si una empresa va a ser víctima de un ataque de ransomware, sino cuándo. Teniendo eso en cuenta, si su empresa finalmente fue vulnerada, ¿qué pasos habría que tomar?

"Si una compañía ha sido infectada las medidas de contención y mitigación cobran importancia. Se debe reducir la superficie de ataque, evitar los movimientos laterales y tener dentro de los playbooks de respuesta a incidentes medidas automatizadas, que puedan aislar los puestos afectados en milisegundos. Desde Appgate creemos que es necesario prepararse de antemano para articular todo el ecosistema de ciberseguridad y responder automáticamente a este tipo de ataques al instante, y así, reducir la ventana de exposición", explica David López, de AppGate, que suma "Una solución es el perímetro definido por software, que permite coordinar toda esta respuesta, integrándose a través de APIs con el SIEM, SOAR, EDR y otros elementos del stack de ciberseguridad, para responder de manera rápida y automática con la redefinición de permisos o aislando puestos de trabajo/usuarios afectados. Esto es vital para evitar que los costos de este tipo de ataques crezcan exponencialmente a medida que transcurren las horas desde que sucede materialmente un primer comprometimiento".

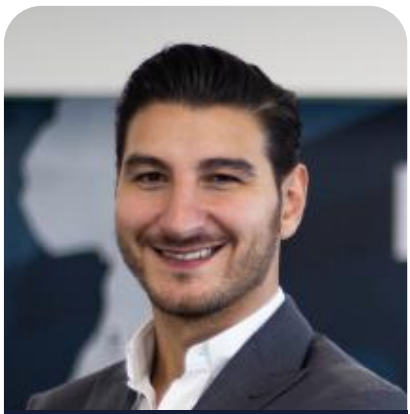
Por su parte, Bruno Lobo, de Commvault, señala que la respuesta ha sido vista históricamente como una cuestión del departamento de TI, y comenta que "Una planificación eficaz debe incorporar la coordinación en todas las funciones de la empresa. Por ejemplo: comunicación corporativa, acciones, regulación, legal, cumplimiento y auditoría, y operaciones comerciales. Una buena coordinación, combinada con un fácil acceso a la documentación del plan respuesta a Incidente, garantiza que todos los niveles de una organización puedan reaccionar más rápidamente durante un incidente".

Fabio Assolini, de Kaspersky, da otra mirada, tal vez más pesimista: “Desafortunadamente, no hay mucho que una empresa pueda hacer si los sistemas están infectados”, comenta, “El ransomware cifra los datos y sistemas, así la empresa no puede funcionar normalmente. Pero se puede decir “tengo copias de seguridad y puedo volver la operación de los sistemas con los mismos datos”. Hacer la recuperación con el backup es importante, pero aun los ciberdelincuentes tienen los datos y van a publicarlos en línea. La empresa tendrá pérdidas financieras y reputacionales con eso. No hay cómo mitigar las perdidas una vez que hay la infección”, por eso es que recomienda que la mejor protección contra el ransomware es la prevención y el bloqueo del intento de ataques.

Como se explicó, una de las características de este tipo de ataques es el pedido de dinero para liberar los datos encriptados y que lo robado no se publique en la web. Pero los expertos recomiendan no negocias con los ciberdelincuentes, tal como asegura Martín Colombo, de Veeam: “Nuestra recomendación siempre es no negociar con los ciberdelincuentes, no pagar el rescate de los datos, e iniciar un plan de recuperación de desastres, empezando por una fase de Detección y Análisis. La recuperación es casi siempre posible, en tanto y en cuanto, los repositorios de backup hayan sido recientemente actualizados y realizados correctamente. Es muy importante escanear el sistema restaurado para no introducir la amenaza que ha infectado nuestro sistema en el entorno nuevamente”.

Lo principal en mantener la calma si un ataque fue certero. Así lo recomienda Arturo Torres, de Fortinet: “Lo primero es no caer en pánico y poder contar con los medios para realizar la contención de la amenaza, es decir, evitar que esta se propague y cause más daño. Esto se logra teniendo una buena estrategia de protección de endpoints con soluciones como EDRs y contando con una estrategia sólida de segmentación de redes utilizando Firewalls de Segmentación interna que tengan la capacidad de detectar los movimientos laterales entre segmentos de la red. Por otro

lado, es de suma importancia que se cuenten con las herramientas de detección necesarias para medir el impacto de la amenaza y monitorear su actividad para poder responder correctamente".
"Cuando un sistema ya está comprometido, la respuesta es poco alentadora", indica Leonardo Giordano, de Cisco, "Es muy poco probable que se pueda recuperar la



Arturo Torres

información o desvanecer el daño ya hecho. Más allá de la prevención es muy importante siempre contar con un respaldo de datos, que es la práctica que más recomendamos. Una vez que ya están infectados y con mucha velocidad, es necesario cerrar puertas para evitar que esa infección se propague".

Las formas en que los proveedores de soluciones pueden ayudar a tu empresa

Desde Cisco ofrecen una solución completa a cada uno de sus clientes: "Realizamos un estudio previo de cada realidad de los sistemas y de sus requerimientos. Nos adaptamos a todas las industrias y presupuestos, ya que para nosotros lo más importante como líderes es aconsejar de una manera integral a la seguridad de la información y sistemas de las empresas, gastando lo realmente necesario", comparte Leonardo Giordano.

Por su lado, Arturo Torres, de Fortinet, explica que la empresa cuenta con un amplio portafolio de soluciones amplias, integradas y automatizadas, empezando con su Security Fabric que les permite dar respuesta de extremo a extremo, desde el endpoint hasta la Nube pasando por soluciones ZTNA, acceso seguro, SD-WAN, etcétera. Sus soluciones incluyen FortiDeceptor, FortiRecon, FortiSandbox, FortiEDR, y FortiNDR, entre otros.
Desde Veeam, Martín Colombo, define que la empresa proporciona una plataforma

> "Los CISO saben que sobrevivir a un ataque de ransomware requiere un plan de respuesta a incidentes, pero el desafío es el momento de documentar un plan completo y contar con los recursos adecuados para implementarlo cuando sea necesario.
> **Arturo Torres, Fortinet**"

única para entornos en la nube, virtuales, físicos, SaaS y Kubernetes, ofreciendo soluciones de respaldo, recuperación y administración de datos que ofrece protección de datos moderna para cada uno de sus clientes: "Nuestro objetivo es garantizar la disponibilidad de los datos en todos los entornos, eliminar la pérdida de datos y reducir al mínimo el tiempo de inactividad".
Para que las empresas se protejan de los ataques de ransomware, Fabio Assolini, de Kaspersky, recomienda mantener el software actualizado, capacitar a los empleados, elaborar una estrategia de defensa transversal, realizar copias de seguridad de

los datos, utilizar la inteligencia de amenazas más reciente, y recomienda entre su portfolio de soluciones Kaspersky Endpoint Detection and Response y Kaspersky Managed Detection and Response, que ayudan a identificar y prevenir ataques en las primeras etapas.

Para ayudar a las empresas, Commvault ofrece en su plataforma la integración del Framework NIST, cubriendo

> “Las empresas deben estar atentas a las nuevas formas en que actúan los cibercriminales, y ser capaces de entender e identificar cuáles son los riesgos a los que están expuestos, preparándose para abordar el tema.
> **David López, AppGate**”

los 5 puntos fundamentales, además de la Deception Solution denominada Metallic ThreatWise. Además, todas las funciones de Commvault y Metallic plataforma cuentan con la Arquitectura Zero-Trust, indica Bruno Lobo.

David López explica que Appgate puede ayudar con varias de sus soluciones, servicios y productos, pero principalmente lista dos: 1-SDP: Es una solución de perímetro definido por software que permite implementar ZTNA. Con Appgate SDP los puestos de trabajo afectados no pueden ver el resto de la infraestructura, ya que se lleva el perímetro a donde se encuentra el binomio usuario/dispositivo y se invisibilizan los activos de información que no son necesarios para el trabajo de los roles; 2- DTP: su Servicio de Protección contra Amenazas Digitales permite detectar, mitigar y desactivar sitios de Phishing, dominios similares, aplicaciones móviles maliciosas y perfiles falsos en redes sociales.

¿Qué se puede esperar?

Cómo bien definieron los expertos consultados, el ransomware sigue en evolución, acompañando la profundización de las estrategias y proyectos de digitalización y transformación digital de las empresas. Es por eso menester armar una fuerte línea de defensa, con soluciones que protejan los activos corporativos, sumado una profunda capacitación en seguridad de los empleados, que debe de ser acompañada con un fuerte apoyo de los directivos de las compañías.

David Lopez

Esto no termina acá: ciudades inteligentes, IoT, vehículos autónomos, migración a la multi-nube, infraestructura de base, salud, educación, etcétera, son campos que los ciberdelincuentes sumarán a sus ataques. Es por ello que la seguridad es un compromiso de todos, y debe de ser parte de los planes y estrategias de negocios de las empresas, gobiernos, e individuos.

Recuperación ante ransomware: lo que debe saber

Por Melissa Palmer, Senior Technologist on the Product Strategy Team at Veeam

Melissa Palmer

¿Sabía que solo 65 % de los datos se recuperan cuando sucede un ataque de ransomware según el estudio de Sophos sobre el estado del ransomware? Qué hacer para que esto no suceda

La recuperación de datos ante ransomware es el proceso que se sigue para volver a conectar los sistemas de TI luego de un ataque. La recuperación puede ser sencilla, puede copiar muchos de los procesos existentes de recuperación ante desastres con los que cuenta, siempre y cuando sus planes de recuperación ante desastres estén registrados correctamente y probados minuciosamente (de forma reciente).

En el entorno de la protección de datos hay un enfoque en la recuperación, en especial en recuperar VM cifradas desde un backup. Aunque esta sea una parte importante de la recuperación ante el ransomware, también existen otros impactos sobre el resto de su entorno de TI.

¿Cómo es la recuperación después de un ataque de ransomware?
El primer paso es alertar al equipo de seguridad de TI para que comience a ejecutar el proceso de respuesta ante incidentes. Este proceso puede llegar a ser un poco diferente de lo que están acostumbrados la mayoría de los administradores de backup cuando se trata de restaurar datos
.
Antes de poder recuperarse del ransomware, hay varias fases del plan de respuesta ante incidentes que deben completarse, como Detección y análisis, Contención y Erradicación y recuperación. El "cómo" de la recuperación ante ransomware dependerá de lo que se determine durante la fase de Detección y análisis, por lo que es importante tener múltiples estrategias de recuperación establecidas y probadas minuciosamente.

¿Cuál es la mejor solución para proteger sus archivos más importantes de un ataque de ransomware?
Aunque muchos quieren protegerse contra el ransomware, lo cierto es que deberían estar preparados para su impacto. Hay un número de grupos de ransomware que constantemente buscan nuevas maneras para explotar los entornos, con el fin de ingresar a ellos y poder implementar su ransomware. A pesar de que una estrategia sólida de seguridad de TI puede funcionar muy bien para protegerse contra el ransomware, nada puede prevenir con 100 % de efectividad que suceda un ataque.

La mejor solución es una estrategia sólida de backup, que incluya backups inmutables, para que los actores maliciosos no puedan cifrarlos ni eliminarlos.

¿Cuánto tiempo lleva recuperarse del ransomware?

La recuperación ante ransomware debe probarse regularmente, igual que los planes de recuperación ante desastres. De hecho, su plan de recuperación ante desastres es un buen lugar para comenzar cuando se trata de una recuperación ante ransomware, siempre y cuando esté actualizado y se haya probado minuciosamente.

Pagos de ransomware: ¿qué debe hacer?

Por Aamir Lakhani, Fortinet

Aamir Lakhani

Según una encuesta reciente, el 85 % de las organizaciones están más preocupadas por un ataque de ransomware que por cualquier otra ciberamenaza. Y aunque a menudo alguien puede sentirse desesperado y querer pagar el rescate o un arreglo de ransomware para recuperar el acceso a datos críticos, es una decisión que debe considerarse con mucho cuidado.

La supervivencia de una organización puede depender de obtener la clave de cifrado de los ciberdelincuentes para descifrar y recuperar los datos robados. Pero los dilemas parecen sorprendentemente similares para ambos grupos de víctimas.

¿Debe pagar ransomware?

Es difícil confiar en la buena voluntad de los acosadores o los ciberdelincuentes. En lugar de devolver sus cosas (información) que probablemente desee mantener en privado, simplemente podrían vaciar todo su contenido, incluidos los datos confidenciales, en Internet para que todos puedan acceder y utilizar.
O podrían darle sus datos a otro acosador o delincuente para que haga lo que quiera con ellos. En este caso, pagar no resuelve tu problema y te empobrece considerablemente. Y quizás, lo peor de todo, ahora tiene una reputación como un blanco fácil y un "pagador" que puede ser intimidado con facilidad y frecuencia.

Los problemas que crea el pago del rescate

Si bien aprecio que algunas organizaciones no tengan otra opción que pagar a los atacantes de ransomware, recomiendo no hacerlo a menos que sea absolutamente necesario correr el riesgo porque si no lo hace, su negocio está garantizado para fallar. Además de convertirse en una víctima recurrente, pagar el rescate envalentona a los malos y financia más ataques futuros contra usted y otros.

Qué hacer si eres víctima de un ataque de ransomware

Las organizaciones pueden limitar el impacto del ransomware tomando medidas rápidas. Primero debe aislar el ransomware. Esto puede evitar ataques horizontales , en los que el ransomware se propaga de un dispositivo a otro a través de conexiones de red.

A continuación, debe averiguar qué tipo de malware ha infectado su sistema con ransomware. Por lo general, no es solo un ataque de ransomware. El ransomware suele ser la última parte de un ataque mayor. Comprender qué tipo de malware está involucrado puede ayudar al equipo de respuesta a incidentes de seguridad a diseñar una solución o, en algunos casos, usar una clave de descifrado que ya está disponible para cierto malware.

Recuperándose de un ataque de ransomware

Para recuperar datos con éxito, su organización debe tener un programa de recuperación de datos configurado antes de un ataque. Si las copias de seguridad están programadas para varias veces al día, un ataque de ransomware podría costarle a su organización solo unas pocas horas.

El panorama de la ciberseguridad en 2022

Por David López Agudelo, VP Sales Latam de Appgate

David López Agudelo

Appgate, compañía de acceso seguro que ofrece soluciones de ciberseguridad para personas, dispositivos y sistemas, presentó su informe Fraud Beat 2022, una recopilación de las cifras, propias y de la industria, más relevantes de la ciberseguridad a nivel mundial, su impacto y estrategias para combatir el fraude.

"Las estrategias fraudulentas aprovechan el trabajo remoto y el aumento de usuarios como una superficie de ataque mucho más amplia, masiva y efectiva", comenta el vicepresidente de ventas para Latinoamérica de Appgate, David López Agudelo.

El 81% de las instituciones financieras percibe que el número de incidentes se ha mantenido igual o ha aumentado; mientras que el 78% indicó que los controles antifraude son una de las características más deseadas para el cliente en las plataformas digitales. Además, reveló los datos alrededor de los métodos más usados por los cibercriminales:

- Phishing: También conocido como Ingeniería social, representa el 80% de los incidentes reportados. En Latinoamérica se estima que más de 80.000 personas son objeto de estafas bajo la suplantación de identidad, exponiendo información personal y corporativa.
- Credenciales Robadas: Este tipo de información sigue siendo uno de los principales objetivos de búsqueda de los cibercriminales, ya que en el 100% de los casos se obtienen ganancias económicas. En el informe se reveló que el 61% de las fugas de datos tuvieron origen en las credenciales vulneradas y el 25% de las fugas provinieron de estos datos robados
- Ransomware: El secuestro de datos es uno de los ciberataques que más impacto genera en las organizaciones con 700 millones de ataques registrados en 2021. En el 20% de los casos comienzan por una fuga de datos y resulta prácticamente imposible recuperarse de este tipo de situaciones. En Latinoamérica genera pérdidas por unos u$s 2.56 millones de dólares, un 52% más a comparación del 2020
- Ataques Móviles: El 41% de las compañías de servicios móviles ha notado un incremento de incidentes en este tipo de canales, y el 23% registró un aumento en el número de cuentas falsas que se hacen pasar como clientes.

El 50% de las empresas consideran que se están quedando atrás ante las capacidades de los atacantes. Ante este creciente escenario de riesgo, el informe revela que las soluciones en las que más se espera invertir son: la Inteligencia Artificial y el Aprendizaje Automático (41%); la Autenticación Multifactor (31%); los Sistemas de detección y monitoreo de fraudes (27%); y el Monitoreo de transacciones (27%).

"La forma más eficiente de hacer frente al accionar de los cibercriminales es invertir en infraestructura tecnológica enfocada en la filosofía Zero Trust que cuente con soluciones Perímetro Definido por Software (SDP) y Protección contra Amenazas Digitales (DTP). Además, es indispensable que hoy en día las organizaciones cuenten con un enfoque estratégico, alineando sus capacidades de prevención de fraude y educación de los empleados, colaboradores y consumidores, para ofrecer mayor protección a sus clientes y operaciones", sostiene López Agudelo.

¿Preparado para el Ransomware?

Por Bruno Lobo, Gerente General Latam de Commvault.

Bruno Lobo

El ransomware es una amenaza real y persistente para empresas e individuos. ¿Qué hacer si se es víctima, cómo prevenirlo?

Cuando un ataque de ransomware exitoso lo golpea, necesita:

- Detectar: identificar todas las cepas de ransomware.
- Analizar: comprender el impacto de un ataque.
- Recuperar: restaurar lo antes posible.

Pasos a seguir luego de un ataque:

1) Ha determinado que ciertamente ha sufrido (o su red) un ataque de ransomware. Bloquee temporalmente el uso compartido de la red desde varias unidades y verifique los servidores de archivos para ver hasta qué punto se ha extendido el daño. Busque archivos con extensiones recién cifradas como .cry, .zepto o .locky (o cualquier nombre de extensión de archivo inusual) para averiguar cuántos archivos, servidores y unidades se han visto afectados.

2) Averigüe quién es el «paciente cero» (el primero en informar la infección) para posiblemente determinar el origen del ataque. Revise las propiedades de uno de los archivos infectados para ver quién aparece como propietario.

3) Elimine a todos los usuarios afectados de la red mientras implementa el control de daños. Por lo general, este es el momento en que determina la causa de la infección y, posteriormente, envía alertas a usuarios no infectados para mantenerse atento a cualquier tipo de cifrado de archivos ransomware que haya descubierto.

4) Si puede llegar al paciente cero y mitigar el ataque antes de que se propague, hágalo. Si tienes usuarios que reaccionan rápidamente e informan, puedes acceder al terminal del usuario final y realizar acciones que neutralicen el ataque.

5) Descargue e implemente una de las herramientas de descifrado gratuitas si hay una disponible para su variedad de ransomware. Si no las hay, su única otra opción es restaurar sus archivos de copia de seguridad.

Cómo prevenir estos tipos de ataques

«Commvault recomienda un enfoque de varios niveles, alineado con el marco de seguridad cibernética del NIST, que plantea seguir 5 pasos: Identificar amenazas, Proteger datos, Supervisar toda la actividad, Responder a amenazas e incidentes, Recuperar datos en caso de ataques».

En mi libro "¿Preparado para el Ransomware?" comparto información importante con nuestros clientes, canales y público en general para que puedan prepararse para enfrentar nuevas amenazas cibernéticas.

DESCARGA AQUÍ

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

El desafío de proteger tus emails

Por Noah Valle Gallo, Sales Director, Trustifi

Noah Valle Gallo

Siempre hay que estar un paso adelante de los ciberdelincuentes, y el correo electrónico sigue siendo una puerta de entrada a ataques, por lo que es imprescindible contar con una protección completa y adecuada.

Trustifi es una empresa de ciberseguridad que ofrece soluciones entregadas en una plataforma de software como servicio. El objetivo clave de la empresa es mantener los datos, la reputación y las marcas de los clientes a salvo de todas las amenazas relacionadas con el correo electrónico.

Trustifi fue reconocido por Gartner® como proveedor representante por su solución Outbound Shield, Inbound Shield y Email Account Compromise Detection en la Guía de mercado de Gartner 2021 para la seguridad del correo electrónico.

Encuentre Trustifi en IG Technologies, proveedor de ciberseguridad con presencia global en EE. UU., el Caribe y otros países de América Latina. Con más de diez años de experiencia, ofrecen servicios de consultoría en Seguridad de la Información y disponibilizan soluciones para enfrentar los desafíos que involucran la tecnología y la seguridad de los datos.

Qué ofrece Trustifi

El correo electrónico es similar a otras formas de comunicación. Es importante ser prudente a la hora de enviar información confidencial por correo electrónico. El correo electrónico viaja a través de numerosos sistemas antes de llegar a su destino, por lo que es posible que alguien lo intercepte y lo lea. Por lo tanto, convendrá que emplee medidas de seguridad para proteger la confidencialidad del correo electrónico.

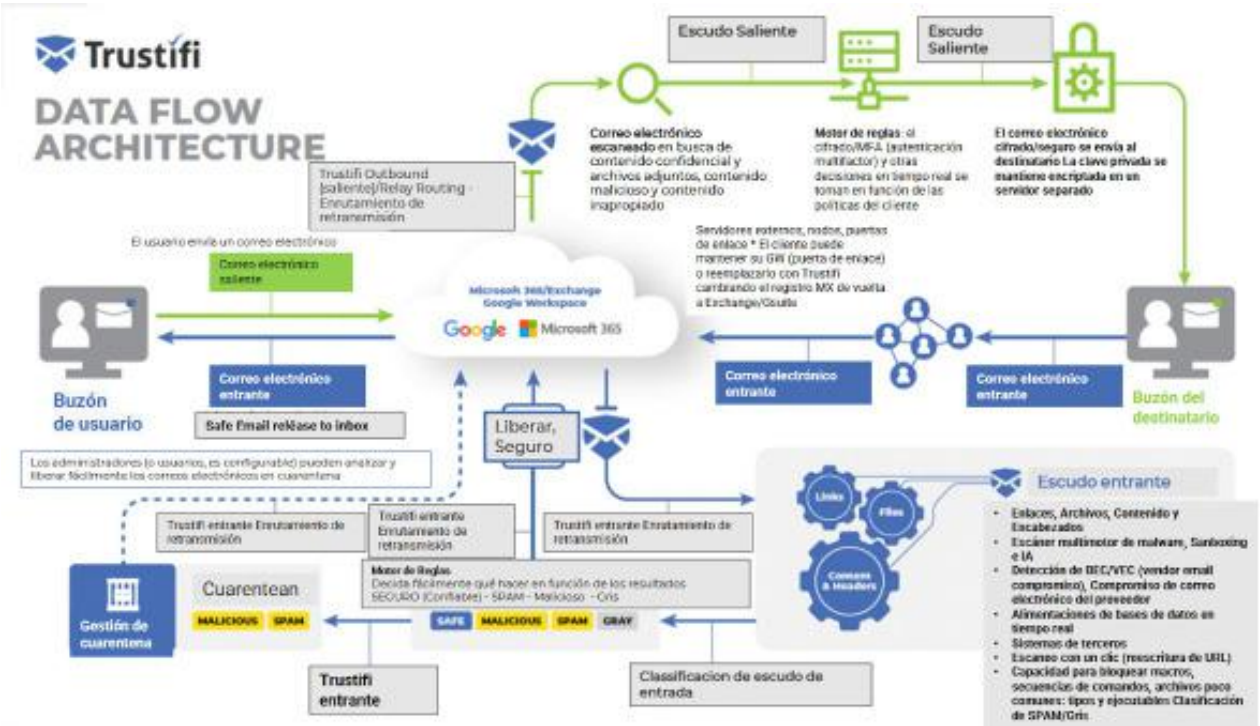
Con esta solución de punta a punta mantendrá seguros tres frentes básicos en su infraestructura de seguridad para email:

Outbound Shield (Salida), y la prevención de Pérdida de Datos:

- Cifrado AES de 256 bits.
- 100% compatible con HIPAA/HITECH, PII, GDPR, FSA, FINRA, LGPD, CCPA y más.
- Conocimiento en tiempo real sobre cuándo se han recibido, abierto y leído los correos electrónicos con entrega y seguimiento certificados.
- Autenticación de dos factores en el destinatario (incluso sin registrarse).
- Comunicación cifrada bidireccional.
- Un clic para descifrar -sin registro forzoso-.

Inbound Shield (Entrada):

- Detección de virus malware y ransomware (secuestros de datos), alertas y prevención de



ataques Business Email Compromise, BEC (Compromiso de correo electrónico comercial).
• Detección de suplantación de identidad, (Spoofing & Phishing), suplantación de identidad, detección de fraude y filtración de correo no deseado (SPAM).
• Opción de lista blanca y lista negra, reglas de prevención de amenazas personalizables
• Escaneo con un clic: reescritura de URL.
• Detección de correo gris.

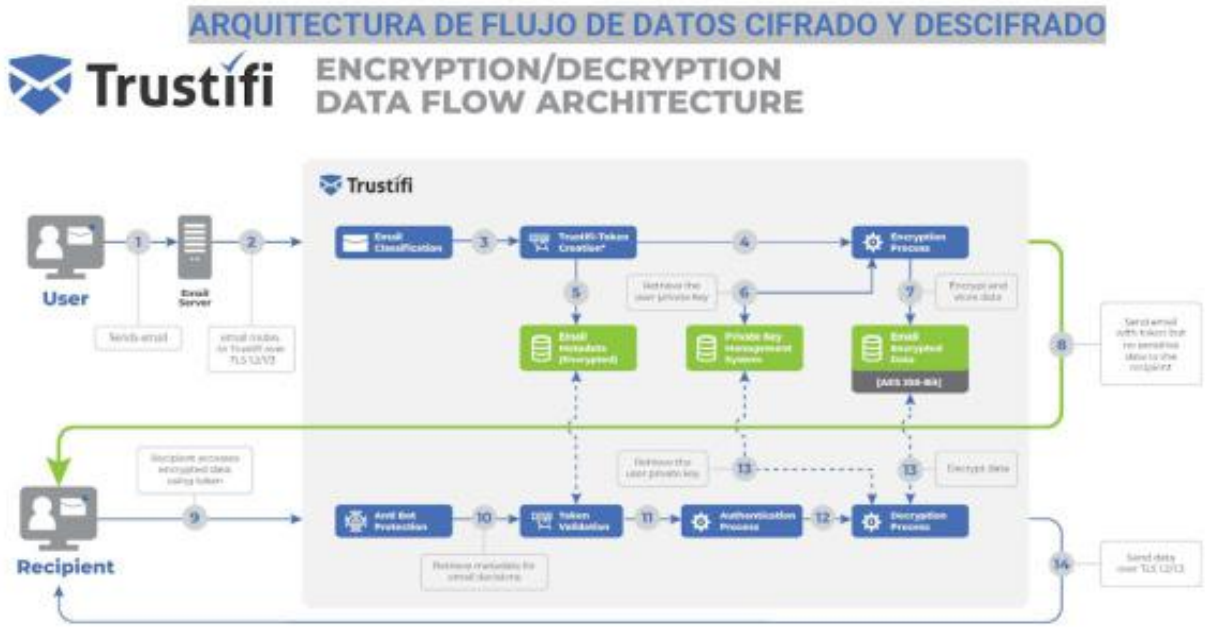
Indexación Inteligente Archivado en la Nube:

• Comparta fácilmente datos, casos y consultas con destinatarios específicos.
• Autenticación inteligente y acceso a monitoreo en tiempo real.

Otras características de Trustifi

El correo electrónico es una de las formas de comunicación empresarial más utilizadas en el planeta, pero lo cierto es que por sí solo no es completamente seguro para una comunicación privada. Además de sus problemas de privacidad, es uno de los principales medios que los atacantes usan para robar información e introducirse en las redes de las empresas.

Un estudio reciente estima que casi la mitad de los correos electrónicos que se envían son intentos de phishing, por otro lado, el trabajo remoto ha aumentado más del 55% en el último año y, como resultado, las amenazas a la seguridad cibernética también han aumentado específicamente a través de correos electrónicos a una tasa del 32% interanual.



Con tantos ataques, las empresas deben ir un paso por delante de los cibercriminales a fin de proteger sus datos y a sus clientes.

Es por ello que desde Trustifi también ofrecen la detección de Cuenta Comprometida (Detección de toma de posesión de cuenta), con las siguientes características:

• Geolocalizar el comportamiento de inicio de sesión del usuario.

• Detectar inicios de sesión desde nuevos dispositivos.

• Aprenda patrones en el volumen y la clasificación de datos de correos electrónicos salientes a través de AI/ML para determinar anomalías.

• Proporcione alertas en tiempo real al administrador del sistema para cerrar un posible ciberdelincuente o evento de pérdida de datos.

La seguridad del correo electrónico es multidimensional y puede requerir varias capas de protección diferentes, que Trustifi e IG Technologies le proveen.

emBlue

Hacemos que la **omnicanalidad sea simple**

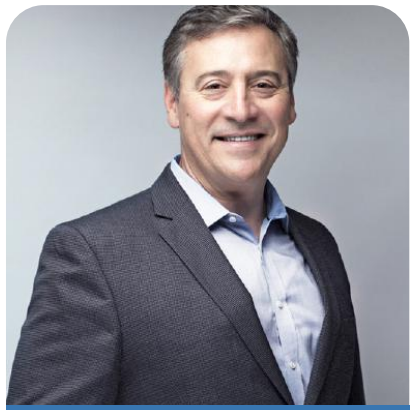
Marketing automation, email, sms, push notifications y más.

www.embluemail.com

/embluemail +506-4031-0300

Ransomware 2.0: cómo las empresas deben actuar antes de que sea demasiado tarde

Por: Miguel Llerena. Vicepresidente para Latinoamérica de Tanium



Miguel Llerena

El ransomware se ha convertido en una de las amenazas más comunes y de mayor impacto en el panorama de la ciberseguridad, con gran costo para todas las industrias que han sufrido incidentes de alto perfil. Por ello es necesario construir una defensa eficaz.

Sumado a ello, la nueva amenaza del ransomware 2.0 no da respiros a las empresas al no sólo cifran archivos y pedir rescate, sino que amenazan con filtrarlo y distribuirlo

Una de las técnicas más utilizada es el phishing, que es la puerta para descargar o instalar un software malicioso como es el ransomware. Entre las recomendaciones básicas está el realizar copias de seguridad de todos los datos críticos y comprobado si se puede acceder a ellos fácilmente, independientemente del tipo de industria a la que pertenezca su empresa.
Según un estudio de Tanium. 3 de 4 empresas invierten en ciberseguridad después de ser atacadas, el63% de los líderes están preocupados por la ciberseguridad después de un incidente, el 79% de los líderes aprueban un presupuesto de ciberseguridad después de una violación de datos, y el 55% no cuenta con suficientes empleados para adoptar medidas preventivas de seguridad.

A eso se suma que el 92% de las empresas han sufrido un ataque o brecha de datos, sólo en el último año, y que más de dos tercios (69%) admitieron que las amenazas están aumentando y esperan que en este 2022 se registre la mayor cantidad de ataques de la historia.

Cómo las organizaciones pueden defenderse contra el ransomware

Antes del ataque: Establecer visibilidad continua de los endpoints, incluidas aplicaciones y la actividad en ellas; eliminar las vulnerabilidades conocidas en los activos constantemente parchados, actualizarlos y configurarlos; buscar proactivamente indicadores de riesgo como evidencia de los ataques en curso antes de que se desarrollen.

Durante el ataque: Investigar el ataque para identificar su origen, hacia donde se extendió y todo lo que tocaron los atacantes; cerrar las vulnerabilidades restantes en el entorno para contener la propagación del ataque; remediar el ataque, desalojar

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

a los atacantes y recuperar el control de los sistemas sin pérdida significativa de datos.

Después del ataque: Encontrar evidencias de cada vulnerabilidad que exploró el atacante y cerrarlas en los activos; encontrar cualquier punto de apoyo restante que los atacantes aún pudieran tener y desalojarlos; mejorar continuamente la higiene de TI y la seguridad general del entorno de endpoints para evitar nuevos ataques.

Una solución de seguridad moderna contra el ransomware

Tanium fue diseñado para ayudar a proteger los entornos modernos. La plataforma Tanium adopta un enfoque diferente en comparación con las estrategias actuales de la mayoría de las organizaciones ya que aborda los desafíos que enfrentan las organizaciones al utilizar su legado de herramientas para así asegurar y administrar sus entornos.

Tanium proporciona una plataforma unificada que ofrece la mayor parte del núcleo de capacidades requeridas para detectar, investigar y remediar amenazas de ransomware en una sola herramienta. Estas capacidades funcionan y operar a partir de los mismos datos e impulsan una colaboración de respuesta a las amenazas, eliminando al mismo tiempo, la complejidad de implementar múltiples herramientas.

Essential Solutions de Tanium como defensa contra ransomware

Responsables de seguridad de diferentes organizaciones han adoptado una amplia gama de capacidades de Tanium para aumentar sus defensas contra ransomware y otras amenazas modernas, también encontraron las siguientes soluciones de la plataforma para hacerlas más efectivas:

Asset Discovery and Inventory

Para saber qué terminales y aplicaciones hay en el entorno, incluso cuando cambia rápidamente.

Risk and Compliance Management

Para evaluar el riesgo e impacto de las vulnerabilidades en tiempo real, incluido el movimiento lateral.

Threat Hunting

Para tener la confianza de informar con certeza sobre cualquier endpoint ubicado en cualquier lugar, para solucionar en segundos incidentes y evitar que vuelvan a ocurrir.

Las organizaciones pueden poner en marcha estas soluciones rápidamente aprovechando la ligera arquitectura de un solo agente y basada en su oferta en la nube: Tanium Cloud.

Con Tanium Cloud, las organizaciones pueden lanzar nuevas capacidades de seguridad en horas o días, no semanas o meses, para rápidamente asegurar los “huecos” frente a su estrategia de seguridad existente o crear una nueva defensa integral contra el ransomware desde una única solución.

Finalmente, es importante tener en cuenta la importancia de implementar herramientas de seguridad modernas. Las herramientas heredadas no pueden proteger los entornos modernos contra amenazas rápidas y complejas como el secuestro de datos. Se deben adoptar herramientas diseñadas para igualar la velocidad y la escala del entorno de activos modernos.

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

Por qué simular el Ransomware

Por Smartfense

Hay muchas formas de prevenir o gestionar un ataque de Ransomware: tener al día la estrategia de backup, definir una clara política de actualizaciones de seguridad, armar una defensa del perímetro incluyendo protección de casillas de email, e invertir en el factor humano mediante programas de awareness.

Una de las primeras medidas es saber cómo ingresa el ransomware en una organización

En casos muy populares como Wannacry, todavía no se sabe a ciencia cierta qué pasó, pero las 3 especulaciones más fuertes son:
• Una campaña clásica de ingeniería social vía email
• Equipos expuestos por SMB (puerto 445) a Internet directamente
• USB o ejecución directa de un binario malicioso

No se puede asegurar que los ataques remotos a vulnerabilidades sean el método principal de ingreso de ransomware en la organización. Los otros dos métodos son ataques directos al usuario final, sea por un email o un USB infectado.

¿Para qué simular Ransomware?

Muchos responsables de ciberseguridad buscan plataformas de simulación de ransomware con el objetivo principal de medir el comportamiento de los usuarios frente a posibles ataques. Debemos asegurarnos que las trampas simuladas se comporten como si fueran verdaderas.

¿Cómo es un ataque de Ransomware simulado?

Una simulación de ataque de Ransomware, a diferencia del Phishing, no busca medir la negligencia de un usuario al entregar información sensible, sino si este tendría un comportamiento riesgoso a la hora de descargar y abrir archivos.

Ambos tipos de simulación comienzan por un ataque de ingeniería social, complementado con herramientas que permitan confundir al usuario (spoofing y certificados SSL válidos). La diferencia radica en si el usuario podría haber sido el vector de ataque que permite ingresar al ransomware en la organización.

En una simulación sólo se miden los hábitos de los usuarios. El usuario recibe un mensaje educativo que le permite saber el peligro que ha sorteado.

¿Por qué simular Ransomware?

• Porque es el ataque más popular por los ciberdelincuentes
• Porque están creciendo enormemente los ataques de ransomware
• Porque el usuario es uno de los vectores de ataque preferidos
• Porque no sabes por dónde entrará el próximo Ransomware

Plataformas de concientización en Seguridad de la Información como SMARTFENSE ofrecen simulaciones integradas de ransomware listas para usar. Los partners especializados en ciberseguridad pueden acompañar estos procesos con herramientas, reportes y servicios especializados, facilitando la tarea de los CISO y responsables de área.

Otras empresas ya invierten en concienciación.

Los ciberdelincuentes prefieren “pescar” en la tuya.

SMARTFENSE

www.smartfense.com
info@smartfense.com

Grupos de ransomware funcionan como startups de Silicon Valley

Según su estudio, la industria autosustentable del ransomware obtuvo u$s 692 millones provenientes de ataques colectivos en 2020, siendo México el país con mayor actividad de ransomware en Latinoamérica. Por Tenable

Netflix y Spotify han cambiado a una variante cada vez más utilizada, que es la economía de las suscripciones. En un mundo cada vez más orientado a los servicios, como muestra una investigación de Tenable®, la compañía de Cyber Exposure, los ciberdelincuentes hacen los mismo, y es cada día más común ver ofertas de "Ransomware as a Service" (RaaS).

Grupos delictivos ya casi se asimilan a startups

En 2020, grupos de ransomware obtuvieron u$s 692 millones por rescates, un aumento del 380 % con respecto a los seis años anteriores combinados.

"El ransomware se ha convertido en su propia industria autosostenible, que funciona como las empresas tradicionales, con un increíble modelo de negocio que implica a múltiples actores, estrategias de marketing y servicio al cliente", dijo Satnam Narang, ingeniero de investigación senior de Tenable.

Inaugurado por el grupo de ransomware Maze, para Tenable uno de los puntos que incentivó este crecimiento fue la aparición de una técnica conocida como "doble extorsión", que aparte de pedir rescate, amenaza con publicar los archivos robados, y se combina con ataques DDoS, contactar a los clientes de sus víctimas, u ofrecer millones a empleados para obtener el acceso.

"La postura de riesgo es más relevante que nunca para minimizar el riesgo ante las crecientes amenazas que no discriminan los activos que tenemos conectados en las organizaciones" Omar Alcala, Director de Ciberseguridad para Tenable América Latina.

Todo un ecosistema a favor del delito

Los propagadores son los conductores responsables de impulsar los ataques de ransomware: traen los leads, encuentran e infectan a las víctimas y las traen a los grupos de ransomware para "cerrar el trato". A cambio, ganan entre 70 % y 90 % del pago del ransomware. Los afiliados están multiplicando los esfuerzos de un "negocio" en auge y los grupos de ransomware no podrían hacerlo más fácil: hasta ofrecen un manual con recomendaciones sobre cómo vulnerar las organizaciones. En algunos casos, los afiliados también pueden trabajar con IABs, que son individuos o grupos que ya han obtenido acceso a las redes y venden el acceso

CONVIERTA LOS ATAQUES DE RANSOMWARE EN SOLO INTENTOS

6 PASOS SENCILLOS PARA **PREVENIR EL RANSOMWARE**

INICIAR

tenable

al mejor postor. Sus tarifas oscilan, por término medio, entre los 303 dólares por el acceso al panel de control y los 9.874 dólares por el acceso al RDP.

"Mientras que los grupos de ransomware obtienen la mayor notoriedad y atención por los ataques, estos grupos van y vienen. A pesar de la rotación, los propagadores y los IAB siguen siendo elementos destacados en este espacio y debería prestarse más atención a estos dos grupos en el ecosistema en general", añadió Narang.

Cómo hay que defenderse de los ataques

El informe proporciona varias tácticas defensivas para las empresas, entre ellas:

- **Utilizar la autenticación multifactor para todas las cuentas de su organización:**

Los grupos de ransomware compran el acceso a las organizaciones a través de los IAB que proporcionan credenciales o explotan vulnerabilidades que revelan las credenciales de inicio de sesión. Al añadir la autenticación multifactor como requisito, se añade otra capa adicional que los atacantes de ransomware tienen que superar.

- **Requerir el uso de contraseñas fuertes para las cuentas**

El uso de contraseñas débiles o predeterminadas facilita a los grupos de ransomware el acceso a las cuentas. Dificulta a los atacantes la entrada por fuerza bruta asegurándose de que los requisitos de las contraseñas incluyan palabras largas y sin diccionario, así como marcando las contraseñas que ya han sido expuestas como parte de una violación de datos.

- **Identificar y aplicar parches a los activos vulnerables de su red en el momento oportuno**

Sabemos que los grupos de ransomware son expertos en aprovechar las vulnerabilidades conocidas sin parches, por lo que es importante que las organizaciones identifiquen los activos vulnerables dentro de sus redes y apliquen los parches disponibles.

- **Concientizar a empleados sobre seguridad y vectores de ataque más comunes**

Los ataques de ingeniería social, incluido el spearphishing a través del correo electrónico o de las redes sociales, son otra forma en que los ciberdelincuentes introducen el malware en los sistemas de su red. Mediante la formación de concienciación de los usuarios, sus empleados y personal pueden ayudar a orientar sobre cómo identificar los vectores de ataque más comunes utilizados por los ciberdelincuentes, lo que desempeñará un papel importante en la protección de sus redes.

"Mientras el ecosistema del ransomware siga prosperando, también lo harán los ataques contra organizaciones y gobiernos. Es imperativo que estas entidades se preparen con antelación para estar en la mejor posición posible para defenderse y responder a los ataques de ransomware", finaliza Satnam.

Cómo utilizar la última filtración de datos para justificar el gasto en seguridad

Por Neil Thacker, CISO EMEA y LATAM de Netskope

Neil Thacker

Una filtración de datos puede considerarse una pesadilla o, simplemente, un episodio inevitable para una organización, no obstante, en ambos casos, es importante saber cómo responder cuando esto ocurre y evitar que dicho incidente pueda convertirse en una bola de nieve. Para lograrlo, es aconsejable analizar el episodio de filtración de datos, plasmar los resultados en un caso de estudio y aprovechar la experiencia para obtener una respuesta adecuada a posibles nuevos incidentes. Esto, sin duda, ayudará a desbloquear el presupuesto en el futuro.

Para ello, es importante considerar los distintos enfoques a adoptar para analizar el costo de una brecha con el fin de solicitar un gasto preventivo adecuado.

¿Cálculos únicos?

Aunque, a menudo, los departamentos de seguridad intentan estimar el costo hipotético de una filtración de datos, es sumamente difícil calcular de forma convincente los complejos factores de este incidente porque cada organización requerirá una fórmula única basada en su modelo de negocio, las condiciones del mercado y los datos que posee.

Además, no todos los datos son iguales, e incluso dentro de un mismo conjunto, el valor y el riesgo asociado pueden fluctuar drásticamente con el tiempo. Los cálculos, sin embargo, no dejan de ser hipotéticos y aunque se alcance una cifra defendible, hay que prever la probable reticencia a reconocer que el suceso se ha producido.

Una vez admitida la incidencia, ya es posible demostrar no solo que este tipo de ataques ocurren, sino que, además, tienen costos reales. Así que, tras una filtración de datos identificada como un incidente de pérdida de datos, ¿por dónde empezar a evaluar los costos reales?
Pérdida de productividad

Esta categoría de costos debería reflejar cualquier alteración en la capacidad de la organización para generar valor sobre su negocio principal, durante y después de la filtración.

Es necesario reflejar esta variación utilizando métricas que el comité de dirección reconozca y con las que esté de acuerdo. El tiempo es el elemento clave aquí: ¿cuánto tiempo se vio afectado el negocio? Hay que emplear los informes financieros para determinar los ingresos que normalmente se obtendrían en ese periodo, utilizando los sistemas o las fuentes de datos que no estuvieron disponibles o se perdieron durante la brecha.

Costos de la respuesta

En este apartado se deben detallar todos los gastos acumulados en la gestión de la filtración de datos, incluyendo los asociados a los recursos internos (tiempo y equipo humano) así como los honorarios de los proveedores. Es esencial no ceñirse únicamente a los costos del equipo de TI, sino incluir también el presupuesto destinado a costear el trabajo de abogados, personal de apoyo a las comunicaciones y

cualquier otra persona que se haya visto involucrada en dicho proceso, tanto de forma interna como externa.

3. Costo de sustitución

Mientras que los "costos de respuesta" cubren los activos que se han podido reparar o reconstruir, habrá otros que se pierdan o dañen en una filtración de datos y que deban ser sustituidos—incluidos los propios datos. Este valor variará mucho en función de la naturaleza y el alcance de la pérdida de datos, y de si se produce desde la organización o se pierden para la organización (es decir, si la empresa sigue teniendo los datos o si es necesario sustituirlos). La lista de precios puede proporcionar presupuestos sobre los activos de infraestructura o hardware de sustitución. Aquí deben incluirse los costos de los seguros (tanto de terceros como de las pólizas de garantía) con los proveedores.

4. Multas y tasas judiciales

Puede llevar algún tiempo tener una idea clara de la inversión necesaria para cubrir esta categoría, pero en el momento en que se conoce que se es potencialmente responsable o que se ha presentado una denuncia relacionada con la filtración de datos acaecida en la empresa, ya es posible incluirlos en el cálculo de costos. Cada vez más países establecen regulaciones al respecto, por lo que el costo de multas o demandas deber tenerse en cuenta. Si por ejemplo, en

relación con el RGPD/GDPR, se solicita un presupuesto significativamente menor para subsanar el problema, vale la pena señalar que existe un precedente para que las autoridades reduzcan la multa impuesta como resultado de la respuesta demostrada, incluso después del episodio.

5. Pérdida de ventaja competitiva

Tras una infracción, las organizaciones pueden ver disminuido el valor de los activos que las diferencian competitivamente. Esto no es fácil de identificar, pero el valor de los conjuntos de datos individuales dentro de las grandes organizaciones es algo que debe ser evaluado y medido por los propietarios de los datos individuales dentro de cada equipo (ingeniería, producto, marketing, recursos humanos, etc.). Estos propietarios de datos entienden el ciclo de vida, el valor y el uso de sus datos específicos y es una conversación valiosa para ver si pueden poner un número más preciso en el impacto de cualquier pérdida de datos.

6. Daños a la reputación

La escala del daño a la reputación y a la marca depende del modelo de negocio de la organización y de los detalles de la filtración de datos, siendo los costos relacionados con la reputación menores, moderados o sustanciales. El daño a la reputación puede predecirse basándose en el porcentaje de clientes perdidos o de usuarios que reducen el uso de sus servicios durante un periodo después de una filtración de datos. A menudo, esto puede suponer la mayor alteración para la organización y puede alargarse meses, años o indefinidamente hasta que se restablezca la reputación, por lo que deben incluirse los factores temporales junto con el posible impacto en la cadena de suministro a través de contratos rescindidos.

Para los departamentos de seguridad que luchan por conseguir los fondos adecuados para garantizar una seguridad apropiada, una filtración de datos suele despejar el camino para alcanzar el presupuesto correcto. Una vez resuelto el problema inmediato, se obtiene un caso de estudio a medida y el argumento de negocio perfecto para revisar el gasto en seguridad y aumentar potencialmente la inversión en áreas vulnerables.

Mejores prácticas para contratar y desarrollar profesionales de seguridad

La ciberseguridad es una profesión de gran demanda y alto perfil con una grave escasez de personal. Al enfrentarse a un entorno de reclutamiento feroz, los gerentes de contratación exitosos han aprendido a ser más creativos y flexibles a medida que se esfuerzan por construir equipos de seguridad sostenibles y resistentes.

Una investigación realizada por (ISC)² encuentra que los gerentes de contratación buscan candidatos de nivel inicial y junior para llenar vacantes, asumir tareas diarias y agregar valor y nuevas perspectivas frescas que ayuden a fortalecer las operaciones de seguridad.

El primer paso para contratar miembros prometedores del equipo es averiguar dónde encontrarlos. El método más popular, citado por el 52 % de los participantes del estudio, es trabajar con organizaciones de contratación y dotación de personal. Este enfoque es seguido por la búsqueda de organizaciones de certificación (46 %) y colegios y universidades (46 %).
Los gerentes también confían en las publicaciones de trabajo estándar (45 %) para encontrar candidatos; aprendizajes y pasantías dentro de sus propias organizaciones (43%); y alianzas con programas de fuerza laboral del gobierno (33%)

Cómo debe de ser la descripción de trabajo

La temida descripción de trabajo de nivel de entrada poco realista, todo incluido continúa siendo ridiculizada como una de las principales causas de los desafíos de dotación de personal de seguridad cibernética de las organizaciones. La investigación sugiere que una mayor colaboración entre los gerentes de contratación y Recursos Humanos es la solución.

Por otro lado, el estudio descubrió una extensa lista de tareas y responsabilidades de los gerentes de contratación evaluadas en todos los niveles de experiencia. Esto puede ayudar a guiar a los gerentes de contratación a medida que identifican las tareas y responsabilidades clave por tipo de trabajo y nivel de experiencia que se espera que los recién llegados aprendan y realicen.

Principales tareas para nivel junior:

- 35% Monitoreo de Alertas y Eventos
- 35% Documentación de Procesos y Procedimientos
- 29% Uso de lenguajes de secuencias de comandos
- 28% Respuesta a incidentes
- 26% Informes (Desarrollo y producción de informes)

Cuando se preguntó qué certificaciones ayudan a identificar a los candidatos ideales de nivel inicial y junior, los gerentes de contratación mencionaron certificaciones que requieren varios años de experiencia.

Qué se valora a la hora de contratar

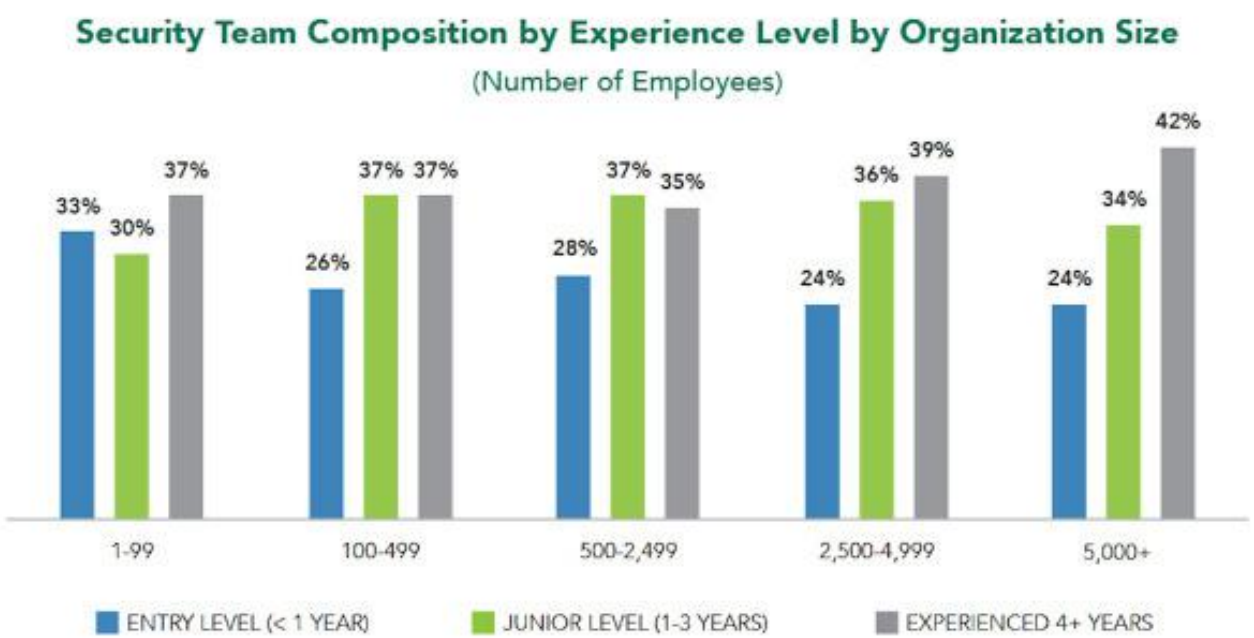
La tendencia de muchas organizaciones es buscar candidatos con las calificaciones técnicas más altas y certificaciones relevantes, pero esperar esas calificaciones no es realista para los candidatos de nivel inicial y junior.

Las habilidades técnicas no son los únicos atributos importantes que un candidato puede ofrecer. Entre otros talentos, son importantes el pensamiento creativo y analítico, el trabajo en equipo y la capacidad de trabajar de forma independiente y en equipo.
A eso se suman rasgos tales como fuertes habilidades para resolver problemas, curiosidad y entusiasmo por aprender, sólidas habilidades de comunicación y pensamiento estratégico son igual o más importantes que las certificaciones y la experiencia relevante en ciberseguridad.

Capacitación in-house

La capacitación en el trabajo es fundamental para el personal de nivel inicial y subalterno, y la investigación reveló que es más probable que se asignen tareas a cada nivel de experiencia.

Las diferencias en la asignación de tareas según el tamaño de la organización también fueron reveladoras. Es más probable que los gerentes de contratación en organizaciones con 2500 empleados o más asignen responsabilidades de seguridad en la nube a los miembros del equipo de seguridad cibernética más experimentados



que sus contrapartes dentro de las pequeñas y medianas empresas.
Sin embargo, casi una cuarta parte (23 %) de los gerentes de empresas medianas (entre 500 y 2499 empleados) creen que el personal de nivel inicial está equipado para manejar la seguridad en la nube.

Las pequeñas empresas y las grandes empresas están de acuerdo en que la remediación de endpoints debe estar a cargo de profesionales más experimentados. Cuando se trata de análisis forense, cuanto más grande es la organización, más gerentes sienten que los miembros del equipo con más experiencia deberían manejar la tarea. Mientras tanto, el 38 % de los gerentes de organizaciones pequeñas (aquellas con menos de 100 empleados) creen que los miembros del equipo de nivel de entrada pueden manejar el análisis forense.

El desarrollo profesional

Una de las ideas más prometedoras de la investigación es la revelación de que los participantes valoran invertir tiempo y dinero para capacitar al personal de nivel inicial y junior. Reconocen el valor de dar a los empleados tiempo para desarrollarse, lo que en última instancia genera valor para sus equipos y organizaciones. Además, proporciona un punto de referencia para que otras organizaciones y gerentes de contratación entiendan cuánto tiempo les puede tomar a los recién llegados estar listos para operar de manera independiente y cuánto cuesta normalmente.

El 91% de los gerentes de contratación dicen que les permiten a los miembros del equipo de seguridad cibernética de nivel inicial y junior tiempo de desarrollo profe-

Who Takes the Lead?

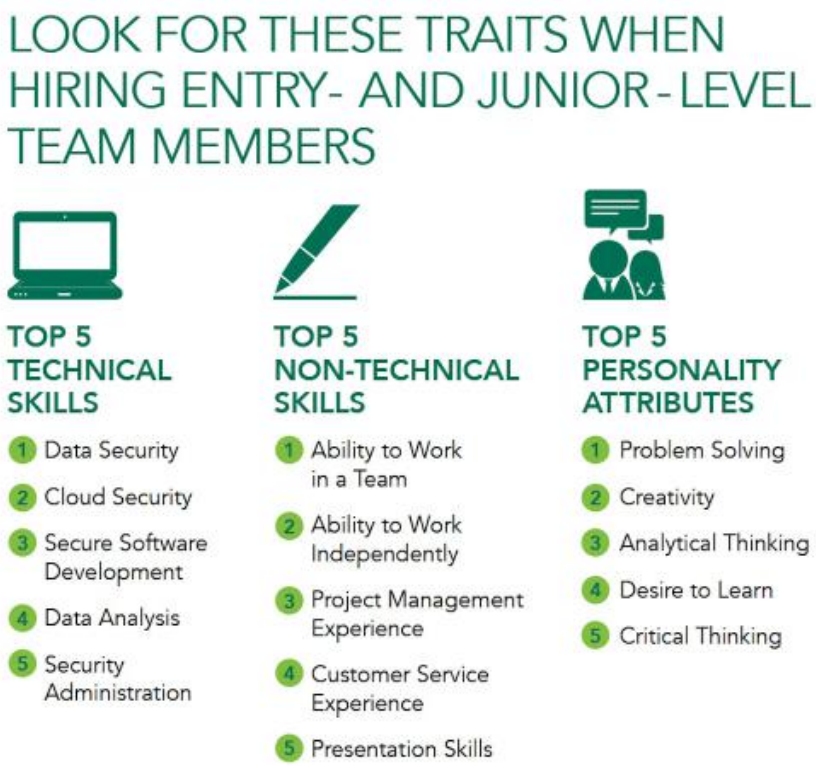
	Human Resources	Cybersecurity Managers	Cybersecurity Teams
Critical and Required Technical Skills	36%	67%	46%
Nice to Have Technical Skills	37%	62%	50%
Non-Technical Skills and Personality Attributes	51%	52%	45%
Education Requirements	46%	64%	46%
Certification Requirements	35%	63%	51%
Professional Experience Requirements	36%	66%	52%
Security Clearance and Compliance Requirements	32%	62%	54%

sional durante las horas de trabajo. La práctica es solo un poco menos común en los EE. UU., donde el 87 % de los gerentes de contratación la ofrecen, en comparación con Canadá (93 %), el Reino Unido (94 %) y la India (93 %).

Las certificaciones se clasificaron como el método más eficaz de desarrollo de talento para los profesionales de nivel inicial y junior (27 %), seguidas de la capacitación interna (20 %), las conferencias (19 %), la capacitación externa (13 %) y la tutoría (11%). Sin embargo, la capacitación interna encabezó la lista en las empresas más pequeñas, mientras que las organizaciones medianas prefieren las conferencias y las grandes empresas prefieren los seminarios web.

El 37% de los participantes estima que los profesionales de nivel inicial se consideran "al día" después de seis meses o menos en el trabajo. La mitad dijo que lleva hasta un año. Otro 14% sitúa la estimación en más de un año.

El 65% de los participantes del estudio dice que el personal de nivel de entrada está

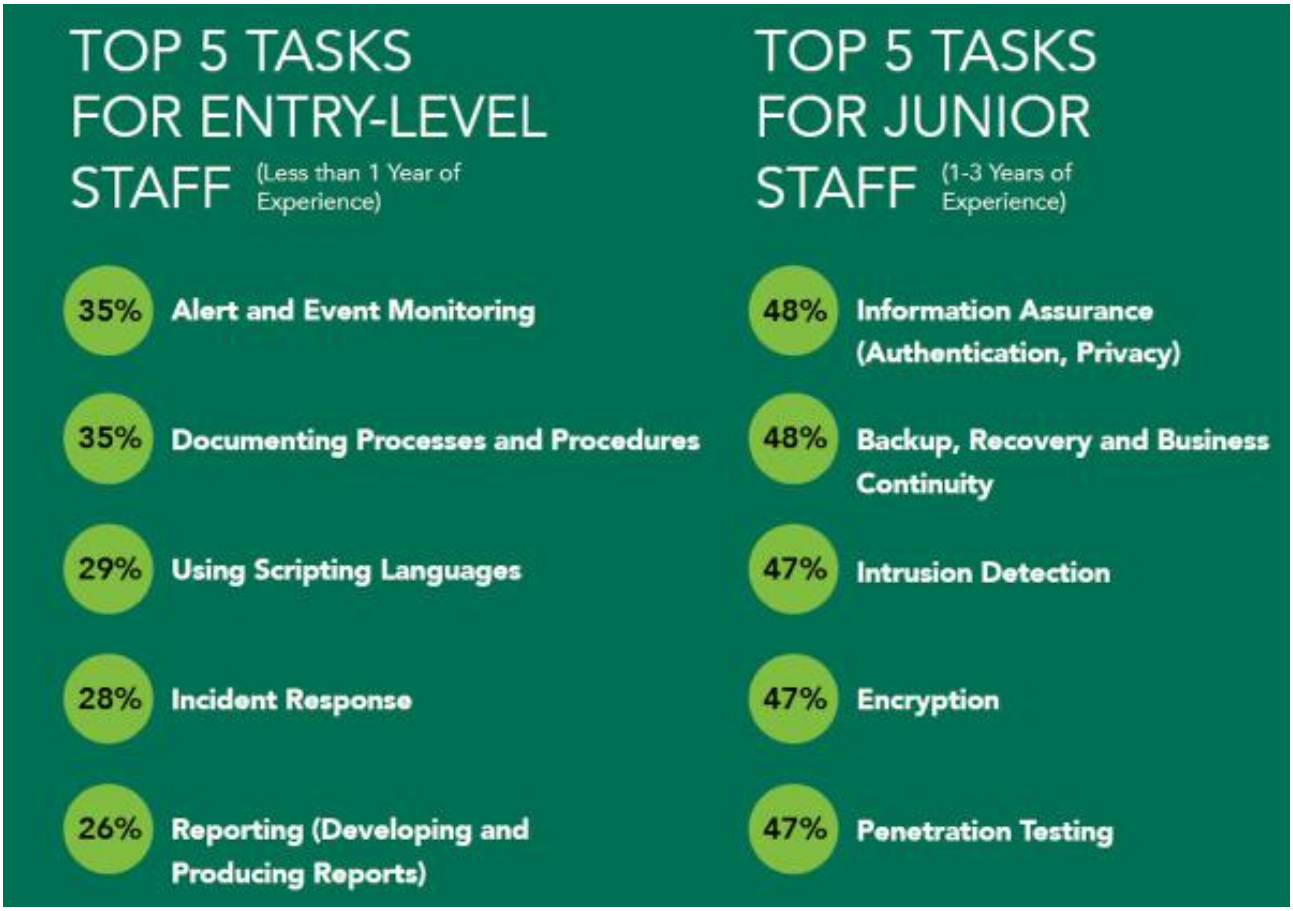


listo para trabajar de forma independiente dentro de los nueve meses, y el 37% dice que lleva seis meses o menos. Estas ideas deberían ser alentadoras para cualquier gerente de contratación de seguridad cibernética preocupado de que capacitar a los recién llegados requiera demasiado tiempo y recursos.

Beneficio de contratar empleados junior

Los resultados del estudio reafirman los beneficios que obtienen las organizaciones cuando contratan personal de seguridad cibernética de nivel inicial y junior. Cuando se les preguntó cómo estos profesionales han ayudado a su organización, los participantes dijeron que aportan nuevas perspectivas, ideas, creatividad, habilidades críticas en nuevas tecnologías, entusiasmo y energía revitalizante.

Un participante señaló: "Tener miembros del equipo de



seguridad cibernética de nivel junior es muy importante para ayudar a una organización a crecer. Traen nuevas ideas a la mesa. El hecho de que tengan menos experiencia significa que también son más flexibles a las nuevas ideas, y creo que es un factor muy importante a tener en una empresa y un mercado en constante crecimiento".

Los participantes también señalaron que contar con practicantes de nivel inicial y junior en su equipo de seguridad cibernética permite que los miembros del equipo senior se concentren en el trabajo avanzado, ya que "se encargan de gran parte del trabajo diario para liberar a los senior para el trabajo más técnico"

Las cinco mejores prácticas al crear equipos de ciberseguridad:

1-Abrace a los profesionales de nivel inicial y junior: los gerentes de contratación dicen que su inversión de tiempo y recursos tiene retornos significativos con la nueva energía, pasión y perspectivas que obtie-

nen al reclutar miembros del equipo de nivel inicial y junior.

2-Mire más allá de TI: a medida que el campo de la seguridad cibernética atrae a talentos más jóvenes y diversos, los gerentes de contratación deben considerar cuidadosamente las habilidades y rasgos no técnicos que indican candidatos fuertes para el éxito profesional a largo plazo.

3-Asóciese con Recursos Humanos para obtener descripciones de puestos ganadoras: las descripciones de puestos deben ser una responsabilidad compartida. Trabaje en estrecha colaboración con Recursos Humanos para crear descripciones de trabajo realistas para roles de nivel inicial y junior que establezcan expectativas claras para los nuevos empleados y empleadores.

4-Asigne tareas cuidadosamente a los recién llegados: considere la tarea y las responsabilidades que los encuestados mencionaron como apropiadas para los empleados con diferentes niveles de experiencia. Asigne tareas a los recién llegados que les permitan aprender y crecer en el trabajo, pero también libere a los miembros del equipo senior para que se concentren en tareas de alta prioridad.

5-Invertir en desarrollo profesional: las mejores prácticas indican que hacer tiempo para aprender durante las horas de trabajo, los programas de tutoría, la obtención de certificaciones, la capacitación y las trayectorias profesionales claras son clave para desarrollar y retener el talento junior.

*Con información de (ISC)², asociación internacional de miembros sin fines de lucro enfocada en inspirar un mundo cibernético seguro y protegido.

Un paso necesario: el uso de inteligencia artificial en ciberseguridad

La Inteligencia Artificial es cada vez más importante en el área de la seguridad de la información, y se vuelve un desarrollo necesario para asegurar el funcionamiento sin interrupción de una empresa.

Los sistemas de inteligencia artificial (IA) están constantemente mejorando y aprendiendo problemas complejos, basándose en datos de ataques cibernéticos anteriores y actuales para identificar nuevos tipos de ataques que podrían ocurrir en el futuro

Desde la verificación de vulnerabilidades hasta la defensa, la combinación de las capacidades de la Inteligencia Artificial en la ciberseguridad con la experiencia de los expertos en seguridad se convierte en un éxito excepcional.

Las organizaciones se benefician de conocimientos inmediatos y, como resultado, tienen un tiempo de reacción más rápido. Los sistemas de inteligencia artificial (IA) se pueden entrenar para crear advertencias de peligro, descubrir nuevas formas de malware y asegurar datos críticos para las empresas si se usan adecuadamente.

Beneficios de Incorporar Inteligencia Artificial en Ciberseguridad

Con los ataques cibernéticos de rápida evolución en el mundo en línea de hoy y el rápido uso de dispositivos electrónicos modernos, la inteligencia artificial puede ayudar a vigilar a los ciberdelincuentes que intentan comprometer los sistemas de red, automatizando la detección de amenazas cibernéticas y respondiendo de manera más eficiente y precisa
.
A continuación, se detallan algunos de los beneficios y usos de la Inteligencia Artificial en el campo de la ciberseguridad.

1-Detección de nuevas amenazas

Las máquinas de inteligencia artificial están siendo entrenadas para identificar y detectar el reconocimiento de patrones de virus malware o ransomware antes de que lleguen a las redes de una organización utilizando algoritmos complejos y creando un nuevo firewall para ello.

El procesamiento del lenguaje natural de la Inteligencia Artificial proporcionará una mayor inteligencia predictiva al seleccionar rápidamente todos los artículos relacionados y las noticias para investigar los riesgos cibernéticos.

Esto puede proporcionar información sobre virus y ataques cibernéticos recientemente lanzados y proporcionar contramedidas adecuadas para implementar. Después de todo, los piratas informáticos siguen las mismas tendencias que el resto de nosotros, por lo que lo que está de moda con ellos cambia todo el tiempo.

2-Robots en combate

No menos del 20 % del tráfico actual de Internet a sitios web/blogs recibe tráfico creado artificialmente, llamado tráfico de bots, y son potencialmente dañinos.

Los bots pueden ser una amenaza grave, desde hacerse cargo de las cuentas de administrador mediante ataques de fuerza bruta mediante el envío de contraseñas hasta que tengan éxito.

La inteligencia artificial nos ahorra mucho tiempo al evaluar grandes cantidades de datos en el menor tiempo posible y permite a los profesionales de la ciberseguridad encontrar soluciones adecuadas para un entorno de amenazas cambiante .

“Al analizar los patrones de comportamiento, las empresas pueden aprender a responder preguntas como ‘¿cómo es el viaje de un usuario promedio?’ y ‘¿cómo es un viaje atípico peligroso?’” Desde aquí, podemos descifrar el propósito del tráfico de su sitio web y adelantarnos a los bots maliciosos”, dice Mark Greenwood, arquitecto técnico jefe y jefe de ciencia de datos de Netacea

3-Garantizar una seguridad libre de riesgos de vulneración

Las máquinas de inteligencia artificial ayudan a la gestión de una organización a determinar el inventario de activos, como la cantidad de dispositivos/sistemas, recursos humanos de varios departamentos y aplicaciones con diferentes niveles de acceso a diferentes sistemas de red.

También pueden predecir y anticipar la magnitud del ataque cibernético y cómo y dónde es más probable que lo pirateen, lo que le permite ejecutar el plan de acción para contrarrestarlo en situaciones de vulnerabilidad.

Al implementar los datos recibidos del análisis basado en IA, puede diseñar y optimizar los procedimientos operativos estándar (SOP) para aumentar la resiliencia cibernética de su organización.

4-Seguridad de endpoint mejorada

La cantidad de dispositivos electrónicos utilizados para el trabajo virtual está creciendo rápidamente y la inteligencia artificial desempeñará un papel vital en la prevención de cualquier ataque cibernético en todos esos puntos finales.

Los servicios de software antivirus tradicionales protegerán los sistemas de red y el software como servicio (SaaS) contra la inyección de

ataques de malware y ransomware al confiar en las firmas existentes.

Esto implica que deben mantenerse actualizados sobre las nuevas firmas de virus para eliminarlos de manera proactiva y proteger los datos en la nube contra las nuevas amenazas.

5-La IA se aprende por sí misma con el tiempo

La tecnología de inteligencia artificial actual incluye aprendizaje automático, sistemas expertos, redes neuronales y aprendizaje profundo, por nombrar algunas instancias o subconjuntos.

ML emplea enfoques estadísticos para permitir que las computadoras "aprendan" (por ejemplo, aumenten el rendimiento con el tiempo) de los datos en lugar de programarse explícitamente. El aprendizaje automático funciona mejor cuando se enfoca en un solo trabajo en lugar de un propósito amplio.

El aprendizaje profundo es un tipo de aprendizaje automático que se centra en el aprendizaje de representaciones de datos en lugar de algoritmos específicos de tareas. La identificación de imágenes basada en el aprendizaje profundo ahora suele ser superior a los humanos en una serie de aplicaciones, incluidos automóviles autónomos, análisis de escaneo y diagnósticos médicos.

El aprendizaje automático ahora se usa en prácticamente todos los servicios de la empresa, particularmente en el aprendizaje profundo, que permite que los algoritmos realicen cambios más autónomos y autorregulados a medida que se entrenan y crecen.

Los ciberdelincuentes, por otro lado, pueden usar los mismos sistemas de inteligencia artificial por razones nefastas. Según Accenture, la IA adversaria "hace que los modelos de aprendizaje automático malinterpreten las entradas al sistema y actúen de una manera que sea beneficiosa para el atacante".

Lo que los ejecutivos de ciberseguridad piensan sobre la IA

El Instituto de Investigación Capgemini analizó el papel de la IA en la ciberseguridad y su informe titulado Reinventar la ciberseguridad con inteligencia artificial sugiere fuertemente que fortalecer las defensas de la ciberseguridad con IA es urgente para las empresas modernas.

Los encuestados (850 ejecutivos de seguridad cibernética, seguridad de la información de TI y operaciones de TI en 10 países) creen que la respuesta habilitada por IA es necesaria porque los cyberpunks ya están aprovechando la tecnología de IA para ejecutar ataques cibernéticos.

Algunas de las conclusiones clave del informe incluyen:
• Tres de cada cuatro ejecutivos encuestados dicen que la IA permite que su organización responda más rápido a las infracciones.
• El 69 % de las organizaciones cree que la IA es necesaria para responder a los ciberataques.
• Tres de cada cinco empresas dicen que el uso de IA mejora la precisión y la eficiencia de los ciberanalistas.

Desventajas de la IA en Ciberseguridad

Las ventajas discutidas anteriormente son solo una pequeña parte del potencial de la IA para mejorar la ciberseguridad.

Sin embargo, como con cualquier cosa, también hay algunas desventajas en el uso de IA en este campo. Para construir y mantener un sistema de IA, las organizaciones necesitarían muchos más recursos e inversiones financieras.
Además, dado que los sistemas

de IA se entrenan con conjuntos de datos, debe adquirir muchos conjuntos distintos de códigos de malware, códigos no maliciosos y anomalías. La adquisición de todos estos conjuntos de datos lleva mucho tiempo y requiere inversiones que la mayoría de las organizaciones no pueden permitirse.

Otro inconveniente importante es que los ciberdelincuentes también pueden utilizar la IA para analizar su malware y lanzar ataques más avanzados, lo que nos lleva al siguiente punto...

Conclusión

La IA está emergiendo rápidamente como una tecnología imprescindible para mejorar el rendimiento de los equipos de seguridad de TI. Los humanos ya no pueden escalar para asegurar lo suficiente una superficie de ataque de nivel empresarial, y la IA brinda el análisis y la identificación de amenazas que tanto necesitan los profesionales de seguridad para minimizar el riesgo de brechas y mejorar la postura de seguridad. Además, la IA puede ayudar a descubrir y priorizar riesgos, dirigir la respuesta a incidentes e identificar ataques de malware antes de que entren en escena.

Por lo tanto, incluso con las posibles desventajas, la IA servirá para impulsar la ciberseguridad y ayudar a las organizaciones a crear una postura de seguridad más sólida.

*Con información de Cybersecurity for Me, e IEEE Computer Society

Líderes en ciberseguridad están perdiendo el control en un ecosistema distribuido

La ciberseguridad se está convirtiendo en un fenómeno social. El interés de los inversionistas, la presión pública, las demandas de los empleados y las regulaciones gubernamentales están fortaleciendo los incentivos para que las organizaciones rastreen e informen los objetivos y métricas de seguridad cibernética dentro de sus esfuerzos ambientales, sociales y de gobierno como un requisito comercial

Esta investigación de Gartner muestra que el 88 % de los directorios consideran la seguridad cibernética como un riesgo comercial y no solo como un problema técnico de TI. El trece por ciento de las juntas han respondido a esto instituyendo comités de junta específicos de seguridad cibernética supervisados por un director dedicado

Qué recomienda Gartner a los líderes de seguridad y gestión de riesgos (SRM)

- Incentive a los ejecutivos de negocios para que consideren la seguridad cibernética como uno de sus objetivos comerciales estratégicos asegurándose de que la junta esté revisando los informes de desempeño de seguridad cibernética basados en resultados
- Refuerce el comportamiento de riesgo de ciberseguridad ejecutivo deseado trabajando con el equipo de recursos humanos (HR) para insertar objetivos de desempeño de ciberseguridad en los acuerdos de empleo de ejecutivos de negocios.
- Reduzca el potencial de impacto social negativo de su organización mediante el desarrollo de objetivos ambientales, sociales y de gobernanza (ESG) como parte de su planificación estratégica anual de ciberseguridad.
- Defina el alcance y objetivos de sus terceros. Para algunos, esto podría ser solo los proveedores de TI críticos, mientras que para otros podría incluir todo el ecosistema, como clientes/ciudadanos individuales o subsidiarias.
- Asegúrese de que la cuantificación del riesgo cibernético se base en los resultados. Aclare la decisión comercial específica en la que desea influir y haga que los resultados de la cuantificación sean directamente procesables para los tomadores de decisiones.

Qué tener en cuenta para una planificación estratégica

Según Gartner, para 2026, al menos el 50 % de los ejecutivos de nivel C tendrán requisitos de desempeño relacionados con el riesgo de ciberseguridad incorporados en sus contratos de trabajo.

Por otro lado, para 2025, el 60 % de las organizaciones utilizarán el riesgo de ciberseguridad como un factor determinante significativo en la realización de transacciones y compromisos comerciales con terceros.

Para el mismo año, el 50 % de los líderes en ciberseguridad habrán intentado, sin éxito, utilizar la cuantificación del riesgo cibernético para impulsar la toma de decisiones empresariales.

Para 2026, el 30 % de las grandes organizaciones tendrán objetivos ambientales, sociales y de gobernanza (ESG) compartidos públicamente centrados en la ciberseguridad, frente a menos del 2 % en 2021.
Para 2025, el 40 % de los programas implementarán principios de

comportamiento social para influir en la cultura de seguridad en toda la organización, frente a menos del 5 % en 2021.

Los líderes de seguridad cibernética de hoy están agotados, con exceso de trabajo y practican un modo "siempre activo". Este es un reflejo directo de cuán elástico ha sido el rol durante la última década debido a la creciente desalineación de las expectativas de las partes interesadas dentro de sus organizaciones.

En una nota similar, han surgido nuevos conceptos como:

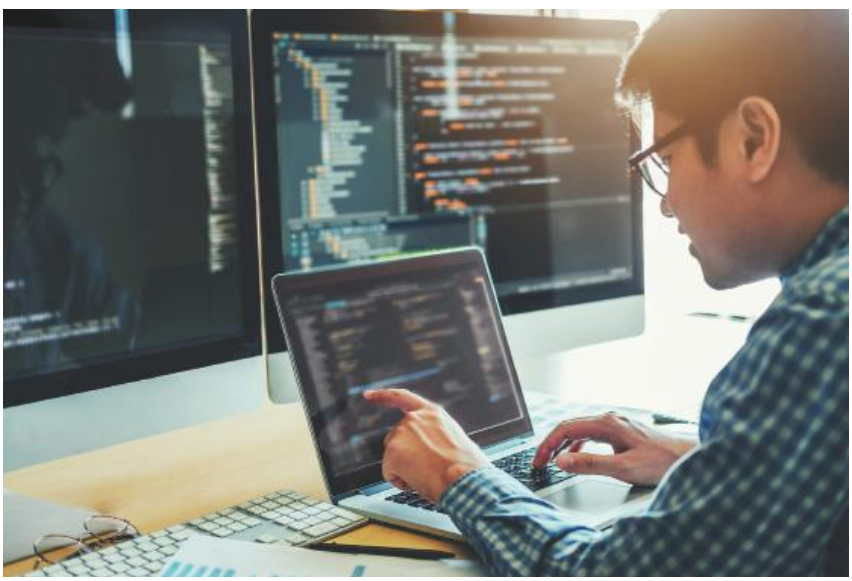
Resiliencia y cuantificación de riesgos

Mayores niveles de conexiones digitales que obligan a la organización a poner niveles significativamente más altos de esfuerzo para controlar (evaluar, influir) la salud cibernética de partes externas

Los empleados ahora toman decisiones con implicaciones de riesgo cibernético sin consultar a los líderes de gestión de riesgos y seguridad

Se establecen comités ejecutivos fuera del alcance/competencia del líder de seguridad cibernética

Estos factores conducirán a un entorno en el que el líder de seguridad cibernética tendrá menos control directo sobre muchas de las decisiones que normalmente estarían bajo su alcance en la actualidad. Por lo tanto, Gartner recomienda que los líderes monitoreen estas predicciones y actúen en consecuencia a medida que vean surgir señales en sus respectivos entornos. Además, es posible que un número cada vez mayor de líderes en seguridad cibernética deba reformular sus roles para tener éxito.



Riesgo comercial

La investigación de Gartner muestra que el 88 % de los directorios ahora consideran la ciberseguridad como un riesgo comercial en lugar de un problema técnico de TI. Además, durante la pandemia de COVID-19, los líderes de SRM aumentaron su tiempo enfocado en las siguientes prioridades:

- Educar al CIO/CEO y otras partes interesadas sénior sobre el valor de la seguridad y la gestión de riesgos.
- Medir y articular el valor de la función de seguridad y gestión de riesgos.
- Aumentar su compromiso y fortalecer sus relaciones con el CEO y el equipo de liderazgo senior.

Este mayor enfoque en educar a los líderes empresariales sobre ciberseguridad se atribuye en

parte al mayor interés de la junta. Además, los principales líderes de SRM están respondiendo de manera proactiva a una tendencia predominante en la que ven más personas que no son de TI o de seguridad dentro de una organización que toman decisiones de riesgo de la información.

Sin embargo, aún queda claro a partir de cientos de interacciones relacionadas con el gobierno de la seguridad con clientes de Gartner que:

- La responsabilidad por el tratamiento de los riesgos cibernéticos generalmente no se asigna formalmente a la empresa.
- Los líderes de SRM continúan luchando para articular por qué la responsabilidad por el riesgo de seguridad cibernética debe residir en el negocio (y no en TI o la función de seguridad).
- Esto afecta la puntualidad y la calidad de las decisiones de riesgo de la información que cada vez más toman las partes interesadas fuera de la línea de visión de TI o seguridad.

Sin embargo, Gartner espera ver un cambio inexorable en la responsabilidad formal por el tratamiento de los riesgos cibernéticos del líder de seguridad a los líderes empresariales senior. Específicamente, esta responsabilidad recaerá cada vez más y, en última instancia, en los líderes empresariales que:

- Son responsables ante el CEO de la entrega de objetivos estratégicos (p. ej., ingresos, satisfacción del cliente).
- Los propietarios de cualquier proceso de negocio asociado, aplicaciones y/o datos que permitan el logro de esos objetivos estratégicos.
- Empoderado (formal o informalmente) y dispuesto a realizar adquisiciones de tecnología independientes en la búsqueda de esos objetivos.
- Responsable de garantizar que cualquier otro riesgo operativo para esos objetivos (y los indicadores clave de rendimiento asociados) se gestionen a niveles aceptables.

Sin embargo, a medida que la transferencia formal de responsabilidad por el riesgo de seguridad cibernética se traslada al negocio, el rol del líder de SRM también debe redefinirse. El rol del líder de SRM deberá evolucionar de ser la persona responsable “de facto” para tratar los riesgos cibernéticos a ser responsable de garantizar que los líderes comerciales tengan las capacidades y el conocimiento necesarios para tomar decisiones de riesgo de información independientes, informadas y de alta calidad.

Para ello Gartner recomienda:

- Incentive a los ejecutivos de negocios para que consideren la seguridad cibernética como uno de sus objetivos comerciales estratégicos asegurándose de que la junta esté revisando los informes de desempeño de seguridad cibernética basados en resultados.
- Defina una responsabilidad clara por el riesgo de seguridad cibernética con la empresa mediante la creación de un estatuto de seguridad empresarial firmado por la junta, el director ejecutivo y los ejecutivos comerciales que indiquen su acuerdo de que no tomarán decisiones unilaterales que expongan a la organización a niveles inaceptables de riesgo cibernético.
- Establezca acceso a un servicio de asesoramiento de seguridad que brinde asesoramiento oportuno sobre seguridad y riesgos, y otro material de orientación de autoservicio, lo que permite a los líderes empresariales tomar decisiones de riesgo de información independientes y de alta calidad.
- Refuerce el comportamiento de riesgo de ciberseguridad ejecutivo deseado trabajando con el equipo de recursos humanos para insertar objetivos de desempeño de ciberseguridad pragmáticos y medibles en los acuerdos de empleo de ejecutivos de negocios.

Identificación de riesgos de terceros

Los ciberataques relacionados con terceros van en aumento. Sin embargo, la mayoría de las organizaciones no cuentan con medidas estrictas para identificar estos riesgos. Según los datos más recientes de Gartner's IT Score for Security and Risk Management (SRM), sólo el 23 % de los líderes de SRM realmente monitorean a sus terceros en tiempo real para detectar la exposición a la ciberseguridad. Además, las organizaciones suelen limitar su cobertura de terceros solo a sus vendedores y proveedores inmediatos, sin tener en cuenta a otros actores del ecosistema, como clientes, socios comerciales, inversores, reguladores, etc

La preocupación por el riesgo cibernético en el ecosistema digital se está volviendo crítica. Por ejemplo, el 56 % de los clientes (B2B y B2C) ahora expresan interés y preocupación frecuentes en la postura de seguridad cibernética de las organizaciones con las que hacen negocios. De manera similar, los reguladores (en particular, la Comisión de Bolsa y Valores de EE. UU.) exigen que las empresas divulguen al público los factores de riesgo en sus aventuras para apoyar a los inversores en un intento de aumentar la transparencia.

Como resultado, Gartner cree que las organizaciones comenzarán a exigir y utilizar el riesgo de ciberseguridad como un factor determinante significativo al realizar negocios con todos los terceros, en todo el ecosistema digital. Estos compromisos pueden ser tan simples como monitorear a un proveedor de tecnología crítica, o más complicados, como invertir en una nueva adquisición y/o asegurar la experiencia/satisfacción del cliente.

Los líderes de ciberseguridad ahora deben enfrentar este problema desde dos ángulos: las ramificaciones internas de la exposición al riesgo cibernético de terceros, así como la demanda continua de transparencia y debida diligencia cibernética del resto de los actores del ecosistema. Esto conducirá a numerosas implicaciones de mercado, en particular:

- Demanda de soluciones tecnológicas adicionales que impulsen la transparencia en la gestión general de riesgos de terceros.
- La introducción de nuevas partes interesadas internas, como relaciones con inversores, profesionales de marketing y finanzas que pueden aumentar los requisitos/expectativas del equipo de liderazgo de ciberseguridad.
- El cambio a un entorno centrado en el cliente que se centra en equilibrar el riesgo de ciberseguridad con la experiencia del usuario y la experiencia del cliente. Las organizaciones sobreprotegidas pueden sufrir interrupciones comerciales de la misma manera que las organizaciones vulnerables en la actualidad.

Cuantificación del riesgo cibernético

La Encuesta de Cuantificación de Riesgo Cibernético de Gartner de 2021 muestra que mientras el 80 % de los encuestados miden el riesgo con escalas ordinales, el 20 % usa técnicas de modelado estadístico (p. ej., simulaciones de Monte Carlo) y el 43 % planea adoptar la cuantificación de riesgo basada en estadísticas dentro de los próximos dos años.

Los casos de uso populares para la cuantificación del riesgo cibernético (CRQ) incluyen priorizar los riesgos cibernéticos y mejorar la comunicación con los propietarios del riesgo, la gerencia ejecutiva y las juntas. En particular, tres de los cinco casos de uso principales se centran en la comunicación con socios empresariales. Los adoptantes de CRQ creen que expresar el riesgo en unidades financieras y relevantes para el negocio justificará las inversiones en seguridad, impulsará la urgencia en torno a la mitigación del riesgo

y ayudará a los líderes empresariales a tomar decisiones críticas de compensación, por ejemplo, entre los riesgos cibernéticos y otros riesgos empresariales o entre el riesgo cibernético y generación de valor.

Hasta ahora, los resultados son mixtos. La mayoría (62 %) de los adoptantes de CRQ cita ganancias leves en credibilidad y conciencia del riesgo cibernético, pero solo el 36 % ha logrado resultados basados en acciones, incluida la reducción del riesgo, el ahorro de dinero o la influencia real en las decisiones .

Dado que la mayoría de los experimentadores se encuentran en la curva de aprendizaje, es inevitable que abunden las ineficiencias e incluso los fracasos absolutos. Como era de esperar, la falta de datos de calidad es el principal desafío al que se enfrentan los usuarios de CRQ, aunque el 46 % de los encuestados de Gartner mencionan que la conexión de CRQ con decisiones comerciales y resultados claros es un obstáculo serio.

Mientras los líderes empresariales y las juntas sigan exigiendo traducciones financieras del riesgo cibernético y una justificación respaldada por datos para los controles y las inversiones en seguridad, los líderes de seguridad cibernética se sentirán obligados a invertir en CRQ. A la vanguardia están aquellos en las industrias financieras , tecnológicas o altamente reguladas, así como organizaciones con programas sólidos de gestión de riesgos de ciberseguridad que buscan dar el siguiente salto de madurez. Las organizaciones con programas de seguridad cibernética menos maduros estarán demasiado enfocados en construir y consolidar procesos de gestión de riesgos para perseguir CRQ de manera significativa.

Para lograrlo:

• Concentre su potencia de fuego en la cuantificación que solicitan los tomadores de decisiones en lugar de producir análisis autodirigidos que luego debe persuadir a la empresa para que se preocupe.
-Considere los activos comerciales en lugar de CRQ basado en escenarios para maximizar el uso de los datos empresariales existentes. El CRQ basado en escenarios requiere estimaciones subjetivas de probabilidad basadas en incidentes históricos o eventos raros. Modelar el valor de los activos y la exposición a la interrupción del negocio le permitirá utilizar datos objetivos del análisis de impacto comercial (BIA) existente y las capacidades de monitoreo.
• Sea muy escéptico acerca de las promesas de los proveedores. Un CRQ eficaz requiere una comprensión profunda de sus datos, la arquitectura tecnológica y las prioridades de la empresa, que

los proveedores no tienen y que sus soluciones no pueden proporcionar sin un ajuste exhaustivo.

Objetivos ambientales, sociales y de gobernanza (ESG)

Han aumentado las expectativas de que las organizaciones deberían ser más transparentes sobre sus riesgos de seguridad. Esto ha resultado en la demanda pública de una mayor transparencia en torno a los objetivos ambientales, sociales y de gobernanza (ESG). Los informes ESG están pasando rápidamente de una actividad discrecional a un requisito empresarial. El interés de los inversionistas, la presión pública, las demandas de los empleados, el comportamiento de los pares y las regulaciones gubernamentales están fortaleciendo el incentivo para que las organizaciones rastreen e informen sus esfuerzos ESG.

Las organizaciones están de acuerdo en que la ciberseguridad ya no es únicamente un riesgo para la organización, sino un riesgo para la sociedad . Aunque la ciberseguridad rara vez se incluye en las divulgaciones actuales de ESG generalizado:

Una serie de marcos desarrollados por terceros establecidos para comparar los esfuerzos de ESG (p. ej., Global Reporting Initiative [GRI], Sustainability Accounting Standards Board) incluyen seguridad de datos o violaciones de datos (como un subconjunto de la privacidad) dentro de sus marcos .

A medida que estos marcos y la inclusión de objetivos y métricas de seguridad cibernética se conviertan en normas de la industria, los líderes de SRM tendrán que demostrar cada vez más un compromiso organizacional para reducir los problemas sociales que pueden surgir de los incidentes de seguridad cibernética.

Los líderes de SRM ya tienen un papel clave que desempeñar en el apoyo a otras métricas de ESG; como aumentar la equidad y la inclusión dentro de la función de seguridad cibernética, y garantizar que los incidentes de seguridad se consideren dentro de la compensación ejecutiva.

Se les pedirá a los líderes de SRM que desarrollen objetivos y métricas para demostrar su compromiso organizacional para reducir los problemas sociales que pueden surgir de los incidentes de seguridad cibernética. Esto podría incluir la estrategia de la organización para reducir el impacto social o social de incidentes tales como, entre otros:

- Violaciones de datos de la información personal del cliente.
- Preocupaciones potenciales de seguridad por el uso de sistemas ciberfísicos.
- El potencial de mal uso y abuso dentro de sus productos.
- Ciberactividad maliciosa (incluido el ransomware) contra la infraestructura crítica (CI).

Al igual que con otras métricas de ESG, en ausencia de información y métricas transparentes, las partes interesadas externas (en particular, los inversores institucionales) confiarán en la información disponible públicamente y, en particular, en los servicios de calificación de seguridad (SRS) para informar su evaluación de la postura de ciberseguridad de una organización. ya no puedes espere mantener en secreto los fracasos y los éxitos de su función de ciberseguridad.

Cómo lograrlo:

- Trabaje con los líderes de sustentabilidad y riesgo empresarial para garantizar que los requisitos de informes ESG existentes y emergentes y las implicaciones a corto y largo plazo para la estrategia de seguridad cibernética se identifiquen de manera proactiva .
- Desarrolle métricas para evaluar de manera proactiva el impacto social o social de los incidentes de ciberseguridad y aumente la transparencia en el desempeño

actual de la organización y las estrategias para reducir este impacto. Estas métricas y estrategias formarán la base de los futuros objetivos ESG de ciberseguridad.

- Supervise de forma proactiva las posibles fuentes de datos, incluidos los servicios de calificación de seguridad que podrían utilizar las partes interesadas externas (en particular, los inversores institucionales) para informar su evaluación de la postura de ciberseguridad de una organización.
- Trabaje en estrecha colaboración con la junta y los altos ejecutivos para garantizar que las comunicaciones corporativas (incluidas las divulgaciones formales de ESG) demuestren compromiso y progreso para reducir el impacto social de los incidentes de ciberseguridad.

Principios de comportamiento social para influir en la cultura de seguridad en toda la organización

Fomentar una cultura consciente del riesgo cibernético es un habilitador clave de un programa de seguridad cibernética efectivo. Cambiar la cultura requiere una combinación de intervención de liderazgo activo y técnicas basadas en una comprensión de cómo las personas se comportan como individuos y en grupos. Los líderes de SRM utilizarán cada vez más el conocimiento de las ciencias sociales de la psicología, la sociología y la economía del comportamiento para obtener información sobre cómo influir en su cultura de seguridad

Los usuarios de tecnología y sus líderes son bombardeados con información desde todas las direcciones. Los mensajes a menudo son contradictorios, por ejemplo, la presión para compartir información con clientes o socios comerciales frente a las demandas de protección de datos, lo que genera disonancia y falta de claridad sobre lo que se debe hacer. Los esfuerzos de concientización tradicionales se basan erróneamente en la suposición errónea de que proporcionar a las personas información sobre el riesgo cambiará su comportamiento de riesgo.

La conciencia y la información no dan como resultado automáticamente un comportamiento más seguro: la conciencia no debe confundirse con la gestión de riesgos real. Las decisiones que toman las personas como parte de su comportamiento, si bien están un poco influenciadas por los esfuerzos tradicionales de concientización, están mucho más influenciadas por las normas y señales inherentes al entorno en el que se encuentran .

Algunas recomendaciones de Gartner

- Cambie el objetivo principal de su programa de concientización sobre seguridad lejos de la mera concientización hacia el establecimiento y fomento de una cultura consciente de los riesgos cibernéticos.
- Designe a alguien con experiencia en ciencias sociales para aplicar la sociología o la economía del comportamiento para mejorar la cultura de seguridad de su organización.
- Busque herramientas que aprovechen de manera efectiva las técnicas de las ciencias sociales para influir en el comportamiento de ciberseguridad.

Conclusión

El riesgo relacionado con la ciberseguridad se considera en gran medida como un riesgo comercial.

La encuesta View from the Board of Directors Survey 2022 encontró que el 88 % de los encuestados veían el riesgo relacionado con la ciberseguridad como un riesgo comercial, no solo como un riesgo tecnológico. Además, el 51% de los encuestados había experimentado un incidente de riesgo de ciberseguridad en los últimos dos años.

El informe completo de Gartner puede ser bajado aqui

Los frameworks de seguridad que marcarán tendencia en 2022

Los frameworks han sido desarrollados por miles de expertos en seguridad cibernética para garantizar una estrategia cohesiva para construir un programa para proteger cualquier negocio.

Un marco de ciberseguridad es una serie de procesos documentados que definen políticas y procedimientos en torno a la implementación y la gestión continua de los controles de seguridad de la información. Estos marcos son un modelo para gestionar el riesgo y reducir las vulnerabilidades.

Los profesionales de la seguridad de la información utilizan marcos para definir y priorizar las tareas necesarias para gestionar la seguridad empresarial. Los marcos también se utilizan para ayudar a prepararse para el cumplimiento y otras auditorías de TI. Por lo tanto, el marco debe soportar requisitos específicos definidos en la norma o reglamento

.

Las organizaciones pueden personalizar los marcos para resolver problemas específicos de seguridad de la información, como requisitos específicos de la industria o diferentes objetivos de cumplimiento normativo.

Los marcos también vienen en diversos grados de complejidad y escala. Los marcos actuales a menudo se superponen, por lo que es importante seleccionar un marco que admita de manera efectiva los requisitos operativos, de cumplimiento y de auditoría.

¿Por qué son importantes los frameworks?

En el mundo digital actual, la ciberseguridad es más importante que nunca. Las empresas de todos los tamaños deben tomar medidas para proteger sus datos de las ciberamenazas. Una forma de hacerlo es implementar un marco de ciberseguridad. Un marco de ciberseguridad es un conjunto de directrices y mejores prácticas para gestionar los riesgos de ciberseguridad. Puede ayudar a las organizaciones a identificar y evaluar riesgos, desarrollar e implementar controles y medir su desempeño.

Al seguir un marco de seguridad cibernética, las empresas pueden beneficiarse de una seguridad mejorada, costos reducidos y una mayor confianza del cliente. Además, el uso de un marco puede ayudar a las empresas a cumplir con los requisitos reglamentarios y mejorar sus posibilidades de aprobar las auditorías. Como resultado, implementar un marco de seguridad cibernética debería ser una prioridad para cualquier organización que quiera proteger sus datos y garantizar su éxito a largo plazo.

Cómo elegir un marco de seguridad de TI

No existe una respuesta única para todos a la pregunta de cómo elegir un marco de seguridad de TI. El mejor enfoque para su organización dependerá de una serie de factores, incluidos su sector, el tamaño de la empresa y la tolerancia al riesgo. Sin embargo, hay algunas consideraciones generales que pueden ayudarlo a reducir sus opciones.

Primero, piense en los beneficios que espera obtener al implementar un marco de seguridad. ¿Quiere mejorar su postura de cumplimiento? ¿Fortalecer sus capacidades de respuesta a incidentes? ¿Reducir costos? Una vez que tenga una idea clara de sus objetivos,

puede comenzar a evaluar diferentes marcos para ver cuáles se adaptan mejor a sus necesidades. Otra consideración importante es si el marco es lo suficientemente flexible para adaptarse a cambios futuros en su entorno empresarial. Después de todo, un marco de seguridad inflexible es de poca utilidad si no puede mantenerse al día con las amenazas en evolución que enfrenta. Con estos factores en mente, debería poder reducir sus opciones y elegir un marco de seguridad de TI que lo ayude a minimizar el riesgo y proteger su negocio.

El tipo de industria o los requisitos de cumplimiento podrían ser factores decisivos. Las empresas que cotizan en bolsa, por ejemplo, pueden querer usar COBIT para cumplir con Sarbanes-Oxley, mientras que el sector de la salud puede considerar HITRUST. La serie ISO 27000 de marcos de seguridad de la información, por otro lado, es aplicable en los sectores público y privado.

Si bien la implementación de los estándares ISO suele llevar mucho tiempo, son útiles cuando una organización necesita demostrar sus capacidades de seguridad de la información a través de la certificación ISO 27000. Si bien la Publicación especial (SP) 800-53 del NIST es el estándar requerido por las agencias federales de EE. UU., cualquier organización puede utilizarla para crear un plan de seguridad de la información específico de la tecnología.

Estándares de seguridad de TI que más se pueden utilizar en 2022

1. ISO/CEI 27001

ISO/IEC 27001 es el estándar internacional que especifica los requisitos para un sistema de gestión de seguridad de la información (SGSI). Un SGSI es un marco de políticas y procesos que ayuda a las organizaciones a mantener segura su información confidencial. ISO/IEC 27001 se publicó por primera vez en 2013 y se basa en el estándar anterior, ISO/IEC 17799. El estándar está diseñado para adaptarse a cualquier organización, independientemente de su tamaño o sector. Puede ser utilizado por empresas de todo tipo, incluidos fabricantes, minoristas, bancos y agencias gubernamentales.

Para obtener la certificación ISO/IEC 27001, las organizaciones deben someterse a una auditoría por parte de un organismo de certificación acreditado. Una vez certificados, deben mantener su cumplimiento con la norma a través de auditorías periódicas. Al implementar ISO/IEC 27001, las organizaciones pueden beneficiarse de una seguridad mejorada y un menor riesgo de filtraciones de datos. Además, la certificación puede ayudar a demostrar el cumplimiento de las leyes y reglamentos, además de proporcionar una ventaja competitiva.

Los beneficios de la certificación ISO/IEC 27001 incluyen seguridad de la información mejorada, mayor confianza del cliente, menor riesgo de filtraciones de datos y mayor eficiencia. El estándar proporciona un marco para que las empresas lo sigan al implementar y mantener su sistema de gestión de seguridad de la información (SGSI). La revisión de 2013 actualizó el estándar para reflejar los últimos cambios en tecnología y seguridad de datos. La certificación ISO/IEC 27001 puede ayudar a las empresas a mejorar la seguridad de su información y proteger sus datos de infracciones. También puede dar confianza a los clientes en el negocio, así como reducir el riesgo de filtraciones de datos y hacer que el negocio sea más eficiente.

La implementación de ISO/IEC 27001 puede ayudar a las organizaciones a proteger sus datos y sistemas del acceso, uso o divulgación no autorizados. El estándar también puede ayudar a las

organizaciones a cumplir con sus obligaciones de cumplimiento. Al implementar los controles y procedimientos detallados en ISO/IEC 27001, las organizaciones pueden beneficiarse de una postura de seguridad mejorada y un riesgo reducido de filtraciones de datos.

2. Marco de ciberseguridad del NIST (NIST CSF)

El Marco de Seguridad Cibernética del Instituto Nacional de Estándares y Tecnología (NIST CSF) es un conjunto de pautas voluntarias que proporciona una taxonomía de alto nivel de los resultados de seguridad cibernética y una metodología para evaluar y gestionar esos resultados. Su objetivo es ayudar a las organizaciones del sector privado que brindan infraestructura crítica con orientación sobre cómo protegerla, junto con protecciones relevantes para la privacidad y las libertades civiles

El NIST CSF tiene muchos beneficios, incluido el hecho de que es independiente de la tecnología, lo que significa que puede implementarse independientemente de las opciones tecnológicas de una organización; también es escalable, por lo que se puede adaptar para satisfacer las necesidades específicas de cualquier organización; y, quizás lo más importante, proporciona un lenguaje común para discutir la seguridad cibernética, lo que puede ayudar a facilitar la comunicación y la colaboración entre diferentes organizaciones.

Incluye tres componentes principales: identificar, proteger y detectar. El primer paso, identificar, ayuda a las empresas a identificar sus activos y vulnerabilidades. El segundo paso, proteger, ayuda a las empresas a implementar controles de seguridad para proteger sus activos. Finalmente, el tercer paso, detectar, ayuda a las empresas a detectar y responder a los incidentes cibernéticos. Al seguir el marco de seguridad cibernética del NIST, las empresas pueden mejorar su postura de seguridad cibernética y defenderse mejor contra los ataques.

3. PCI DSS

El estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) es uno de seguridad de la información para organizaciones que manejan tarjetas de crédito de marca de los principales esquemas de tarjetas. El Estándar PCI es obligatorio para las marcas de tarjetas, pero lo administra el Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago. El estándar se creó para aumentar los controles sobre los datos del titular de la tarjeta para reducir el fraude con tarjetas de crédito.

La implementación de PCI DSS puede ser un beneficio para las organizaciones al disminuir la posibilidad de una violación de datos y, por lo tanto, reducir la cantidad de daños que podrían estar asociados con tal incidente. Además, cumplir con PCI DSS también puede ayudar a mejorar la reputación de una organización

Además, el cumplimiento de PCI DSS puede ayudar a desarrollar la confianza del cliente en una empresa, lo que lleva a un aumento de las ventas y la repetición de negocios. Por estas razones, las empresas que manejan tarjetas de crédito deben asegurarse de que cumplan con PCI DSS.

4. COBIT

COBIT originalmente se centró en reducir los riesgos de TI. COBIT 5, lanzado en 2012, incluía nuevas tecnologías y tendencias comerciales para ayudar a las organizaciones a equilibrar los objetivos comerciales y de TI. La versión actual es COBIT 2019. Es el marco más utilizado para lograr el cumplimiento de Sarbanes-Oxley. Numerosas publicaciones y certificaciones profesionales abordan los requisitos de COBIT.

El marco COBIT proporciona un

lenguaje común para que las organizaciones discutan y midan el beneficio de las inversiones en TI. También proporciona un enfoque integral para abordar los objetivos de control, los procesos de apoyo y las prácticas. En resumen, COBIT es una herramienta que las organizaciones pueden utilizar para mejorar su gobierno de TI. Como tal, se considera una parte esencial de cualquier programa efectivo de gobierno de TI.

Está diseñado para ayudar a las organizaciones a administrar sus recursos de TI de una manera que se alinee con sus objetivos comerciales. Uno de los beneficios de usar COBIT es que puede ayudar a las organizaciones a garantizar el cumplimiento de regulaciones como Sarbanes-Oxley e HIPAA. Además, COBIT puede ayudar a las organizaciones a mejorar su desempeño general al proporcionar un conjunto de pautas claras y concisas para administrar los recursos de TI.

5. CIS 18

Los controles críticos de seguridad del Centro para la seguridad de Internet (CIS), versión 8, anteriormente SANS Top 20, enumera los controles operativos y de seguridad técnica que se pueden aplicar a cualquier entorno. No aborda el análisis de riesgos o la gestión de riesgos como NIST CSF; más bien, se centra únicamente en reducir el riesgo y aumentar la resiliencia de las infraestructuras técnicas
.
Hay 18 controles CIS en total, divididos en tres categorías: básicos, fundacionales y organizativos. Los controles básicos son los más esenciales y deben implementarse primero. Los controles fundamentales se basan en los controles básicos y deben implementarse a continuación. Los controles organizacionales son los más completos y deben implementarse según lo permitan los recursos.

Los controles CIS pueden beneficiar a cualquier organización, pero son especialmente adecuados para las pequeñas empresas que pueden no tener los mismos recursos que las organizaciones más grandes. La implementación de los controles CIS puede ayudar a las pequeñas empresas a proteger sus datos y sistemas de los ataques cibernéticos.

Los controles están diseñados para implementarse en un enfoque por etapas, y cada etapa sucesiva brinda protección adicional. Los beneficios de implementar los Controles de Seguridad Críticos de CIS incluyen una postura de seguridad mejorada, menor riesgo de filtraciones de datos y cumplimiento de los requisitos reglamentarios. Además, los controles pueden ayudar a las organizaciones a identificar y responder rápidamente a los incidentes de seguridad. Como resultado, los controles críticos de seguridad de CIS son una parte esencial de cualquier programa de seguridad.

6. Marco común de seguridad de HITRUST

El marco de seguridad común (CSF) de HITRUST es un marco de seguridad ampliamente adoptado que brinda a las organizaciones un enfoque integral para administrar el riesgo. El MCA incluye un marco de análisis y gestión de riesgos, así como requisitos operativos. Esto lo convierte en una herramienta ideal para organizaciones de todos los tamaños que buscan mejorar su postura de seguridad. Uno de los beneficios del CSF es que ayuda a las organizaciones a administrar el riesgo de manera integral. Al identificar y evaluar los riesgos en todos los departamentos y funciones, el CSF proporciona una visión integral de los riesgos de una organización.

Esto ayuda a las organizaciones a desarrollar estrategias de gestión de riesgos más eficaces y eficientes. Además, los requisitos operativos de la CSF brindan orientación sobre cómo implementar controles y procedimientos de seguridad. Esto ayuda a las organizaciones a garantizar que sus controles de seguridad sean efectivos y cumplan con las mejores prácticas de la industria. En general, HITRUST CSF es una herramienta valiosa para cualquier organización que busque mejorar su postura de seguridad.

El CSF también incluye requisitos operativos diseñados para ayudar a las organizaciones a reducir sus riesgos de ciberseguridad. El CSF de HITRUST ha sido reconocido por el Departamento de Seguridad Nacional de EE. UU. como un beneficio para la postura de seguridad cibernética del país. El CSF también está siendo utilizado por organizaciones de atención médica de todo el mundo para mejorar sus programas de ciberseguridad. La implementación del CSF puede ayudar a las organizaciones de cualquier industria a reducir sus riesgos de ciberseguridad y mejorar su postura de seguridad general.

7. Los 10 mejores de OWASP

OWASP es una organización sin fines de lucro que publica regularmente los 10 principales problemas de seguridad de la aplicación web, dispositivos móviles, servicios web, etc. La mayoría de las organizaciones de auditoría de seguridad siguen estos 10 principales problemas de seguridad para categorizar las vulnerabilidades de seguridad.

Cada pocos años, OWASP publica una lista actualizada de los 10 principales riesgos de seguridad, que ayuda a las organizaciones de auditoría de seguridad a categorizar y priorizar las vulnerabilidades de seguridad. El beneficio de usar la lista Top 10 de OWASP es que proporciona un lenguaje común para discutir y clasificar los riesgos de seguridad. Además, ayuda a concienciar sobre estos riesgos a los desarrolladores y propietarios de aplicaciones. Como resultado, la lista Top 10 es una herramienta

importante para cualquier organización que desee mejorar la seguridad de sus aplicaciones web.

8. SOC 2

El Instituto Estadounidense de Contadores Públicos Certificados (AICPA) desarrolló el marco SOC 2. El propósito del marco es permitir que las organizaciones que recopilan y almacenan información personal de los clientes en servicios en la nube mantengan la seguridad adecuada.

El marco también proporciona a las empresas de SaaS pautas y requisitos para mitigar los riesgos de filtración de datos y fortalecer sus posturas de ciberseguridad. Además, el marco SOC 2 detalla los requisitos de seguridad que deben cumplir los proveedores y terceros. Los requisitos los guían en la realización de análisis de amenazas externas e internas para identificar posibles amenazas a la ciberseguridad.

SOC 2 contiene 61 requisitos de cumplimiento, lo que lo convierte en uno de los marcos más difíciles de implementar. Los requisitos incluyen lineamientos para la destrucción de información confidencial, sistemas de monitoreo de anomalías de seguridad, procedimientos para responder a eventos de seguridad, lineamientos de comunicación interna, entre otros.

El beneficio del marco SOC 2 es que permite a las organizaciones mantener la seguridad adecuada de la información personal del cliente en los servicios en la nube. El marco proporciona a las empresas de SaaS pautas y requisitos para mitigar los riesgos de filtración de datos y fortalecer sus posturas de ciberseguridad. Como resultado, las organizaciones que adoptan el marco SOC 2 pueden beneficiarse de una mayor seguridad de los datos de sus clientes.

9. FedRAMPl

FedRAMP (Programa federal de gestión de riesgos y autorizaciones) es un marco diseñado para agencias gubernamentales. El marco proporciona pautas estandarizadas que pueden permitir que las agencias federales evalúen las ciberamenazas y los riesgos para las diferentes plataformas de infraestructura y los servicios y soluciones de software basados en la nube.
El marco también se basa en el monitoreo continuo de la infraestructura de TI y los productos en la nube para facilitar un programa de ciberseguridad en tiempo real. Más importante aún, FedRAMP se enfoca en pasar de una TI tediosa, atada e insegura a una TI móvil más segura y rápida. El objetivo es garantizar que las agencias federales tengan acceso a tecnologías modernas y confiables sin comprometer su seguridad.

Para lograr los niveles de seguridad deseados, FedRAMP colabora con expertos en ciberseguridad y en la nube para mantener otros marcos de seguridad. Estos incluyen NSA, DoD, NIST, GSA, OMB y otros grupos del sector privado.

Los objetivos principales de FedRAMP son acelerar las migraciones a la nube mediante la reutilización de autorizaciones y evaluaciones, mejorar la confianza en la seguridad de la nube, garantizar que las agencias federales apliquen sistemáticamente las prácticas de seguridad recomendadas y aumentar la automatización para el monitoreo continuo.
El beneficio del Programa Federal de Administración de Riesgos y Autorizaciones (FedRAMP) es que proporciona un enfoque estandarizado para la evaluación y autorización de seguridad para productos y servicios en la nube. Este programa agiliza el proceso para las agencias que buscan utilizar servicios en la nube al proporcionar un conjunto único de requisitos de seguridad que son válidos en todas las agencias federales. Además, el programa requiere un monitoreo continuo de los proveedores de servicios

en la nube, lo que ayuda a garantizar que los riesgos de seguridad se identifiquen y aborden de manera oportuna. Como resultado, FedRAMP proporciona una forma más eficiente y efectiva para que las agencias usen los servicios en la nube mientras mantienen sólidos estándares de seguridad.

10. Suplemento de regulación de adquisiciones federales de defensa (DFARS)

El Suplemento del Reglamento Federal de Adquisiciones de Defensa (DFARS) es un conjunto de reglamentos que rigen la adquisición de bienes y servicios por parte del Departamento de Defensa de los Estados Unidos (DOD). Los reglamentos son promulgados por el DOD y están codificados en el Código de Reglamentos Federales en el Título 48, Capítulo 1. Implementan las disposiciones del Reglamento Federal de Adquisiciones (FAR), que es el reglamento principal que rige la adquisición de bienes y servicios por parte de todos organismos del poder ejecutivo. El DFARS proporciona requisitos específicos para la adquisición de bienes y servicios por parte del DOD, incluidos los requisitos para la contratación con pequeñas empresas y para el uso de artículos comerciales. El DFARS también prescribe métodos para adquirir suministros y servicios que apoyen la defensa nacional.

El DFARS también establece estándares mínimos de seguridad, salud y seguridad. Además, el DFARS requiere que los contratistas cumplan con las leyes y reglamentos federales, incluidos los relacionados con las leyes laborales y de empleo. El DFARS es aplicado por el Sistema de Regulaciones de Adquisición (DARS) del DOD. Los contratistas que no cumplan con el DFARS pueden

estar sujetos a sanciones civiles o penales
.
Los beneficios de DFARS incluyen el hecho de que ayuda a mejorar la seguridad de la información y los sistemas de defensa. Lo hace estableciendo estándares para contratistas y otras entidades que acceden o manejan información de defensa. El DFARS también requiere que los contratistas informen cualquier incidente cibernético, para que el gobierno pueda investigarlos y abordarlos adecuadamente. Además, DFARS prohíbe el uso de ciertos tipos de software en los sistemas de defensa, lo que puede ayudar a prevenir infecciones de malware. En general, los beneficios cibernéticos de DFARS ayudan a mejorar la seguridad de la información y los sistemas de defensa.

¿Cómo elegir un buen framework de ciberseguridad?

Cuando se les pregunta cómo auditar o medir su nivel de seguridad, hay muchas opciones. Hay más de 50 estándares y marcos de ciberseguridad. Entonces, ¿cómo elige un marco sólido y reconocido que satisfaga sus necesidades sin ser demasiado complicado?

Aquí se explica cómo establecer una lista de medidas de seguridad que se puede utilizar como referencia. Descubra el resultado de años de experiencia adquirida en diferentes jurisdicciones, contextos y sectores de actividad.

Criterios de selección

Elija siempre una línea de base que pueda usarse para medir y realizar un seguimiento de la postura de seguridad. La precisión y la objetividad son importantes. Sobre todo, un marco de seguridad es una herramienta que se puede usar todos los días.

Para ayudarlo a tomar una decisión, se revisaron docenas de pautas y estándares de seguridad de la información.

Antes de elegir un marco de referencia de ciberseguridad, es importante tener en cuenta su sector empresarial y los requisitos normativos aplicables. Si este es tu caso, debes utilizar el framework adecuado. Sin embargo, para la mayoría de las organizaciones, se recomienda el marco de seguridad cibernética (CSF) del NIST. Es completo, comprensible y muy bien alineado con otros estándares y requisitos de cumplimiento.

-El enfoque de 5 áreas tiene mucho sentido:

- Entender qué proteger (Identificar)
- Implementar medidas de protección (Proteger)
- Monitorear y anticipar (Detectar)
- Gestionar incidentes de seguridad (Responder)
- Saber qué hacer si las cosas salieran mal (Recuperar).

Conclusión

Aplicar un marco de ciberseguridad es el siguiente paso para su organización. Para mejorar su postura de seguridad cibernética, deberá adoptar un enfoque integral que abarque personas, procesos y tecnología. Al identificar los riesgos cibernéticos e implementar controles para mitigarlos, puede hacer que su organización sea más resistente a los ataques.

Los beneficios de usar un marco de seguridad cibernética incluyen detección y respuesta de amenazas mejoradas, exposición reducida a vulnerabilidades y protección de datos mejorada. Al considerar qué marco es el adecuado para su organización, tenga en cuenta sus necesidades y objetivos específicos. Con el marco adecuado, puede construir una base sólida para proteger sus datos y salvaguardar su negocio.

*Con información de Framework Security y Coresilium

El ABC del ransomware: qué es, cómo detectarlo, prevención y respuesta a ataques

Comprender qué es el ransomware, qué riesgo presenta para su organización y cómo crear un plan de respuesta y recuperación efectivo es crucial para implementar un programa sólido de inteligencia de amenazas y mantener seguros sus activos, infraestructura y personal, indican desde Flashpoint

El ransomware utiliza el cifrado de datos para bloquear el acceso de las organizaciones a sus propios datos confidenciales, exigiendo que se pague un rescate para desbloquearlos de forma segura.

Aunque se ha discutido cada vez más en la última década, los ataques de ransomware existen desde hace casi 40 años. Uno de los primeros ataques de ransomware registrados, que tuvo lugar en 1989 y se lanzó a través de un disquete, fue el troyano AIDS, también llamado PC Cyborg Virus.

Hasta la década de 2000, era difícil recibir pagos de rescate de manera eficiente, lo que hacía que los ataques de ransomware fueran relativamente raros en comparación con la actualidad. Con la llegada de las criptomonedas, se ha vuelto mucho más fácil para los actores de amenazas recibir pagos y obtener ganancias rápidamente, lo que ha llevado a que este tipo de ataque se generalice.

El avance del ransomware

La evolución del ransomware ha visto un cambio en la forma en que los actores de amenazas eligen sus objetivos y adaptan sus ataques. En el pasado, los ataques de ransomware "generales" eran más comunes y se dirigían a grupos más amplios de víctimas a la vez para aprovechar un mayor volumen de pagos de menor valor. Eran bastante aleatorios y se aprovechaban de quienquiera que descargara el malware que los obligaría a pagar.

Sin embargo, los sitios extorsionadores, como el asociado con los delincuentes detrás del ransomware Maze, han brindado a los actores de amenazas la capacidad de apuntar de manera efectiva a entidades específicas que están dispuestas a pagar rescates más altos en un solo ataque.

A medida que los ataques de ransomware se vuelven más avanzados, muchos actores de amenazas también han comenzado a aprovechar otras tácticas además de mantener como rehenes los datos confidenciales para alentar aún más a las organizaciones a pagar rápidamente. Una de las amenazas secundarias más comunes es divulgar la información privada que han capturado, ya sea al público en general o al directorio de una empresa, lo que daña aún más la reputación de una organización después de un ataque.

¿Cómo funciona el ransomware?

Hay varias formas en que los actores de amenazas logran estos pasos, pero la mayoría de las veces se dividen en los siguientes componentes:

Tácticas de distribución e infección

• Correos electrónicos de phishing: los miembros de una organización reciben correos electrónicos desde fuera de la empresa que contienen enlaces con malware dañino adjunto. El correo electrónico incluye un mensaje que alienta al destinatario a hacer clic en el enlace adjunto, normalmente con el pretexto de tener un propósito legítimo, y el ransomware puede infectar el sistema.

• Descarga oculta: los miembros de una organización visitan sin saberlo sitios web que contienen malware, que luego puede propagarse a su dispositivo local e infiltrarse en la infraestructura de la empresa, lo que permite que el ransomware cifre sus datos.

• Compromiso del protocolo de escritorio remoto (RDP): un actor de amenazas que puede obtener las credenciales de inicio de sesión de un usuario para su dispositivo puede autenticarse e iniciar sesión de forma remota en una computadora dentro de la red de una organización. Desde allí, pueden controlar el dispositivo y descargar malware para ejecutar un ataque de ransomware.

• Infiltración directa: algunos ataques de ransomware involucran a los actores de amenazas que piratean directamente la red de una organización, lo que les permite infectar la infraestructura de la empresa ellos mismos. Se dirigen específicamente a los sistemas sin parches que dejan a una organización expuesta a vulnerabilidades que facilitan a los atacantes la distribución del malware necesario para ejecutar un ataque de ransomware.

Cifrado de archivos y datos

Después de que se bloquea el acceso de una organización a sus sistemas, se exige un rescate a través del ransomware para que las organizaciones paguen lo más rápido posible. Esto normalmente se comunica a la víctima a través de una nota de rescate, que está programada para configurarse como fondo de pantalla del dispositivo desde el que las víctimas intentan acceder a sus archivos.

Cómo ataca el ransomware

Ransomware viene en muchas formas, incluyendo:

1-Encriptadores: como sugiere el nombre, los encriptadores encriptan los datos de un sistema y los hacen inaccesibles para cualquier persona sin una clave de descifrado. Uno de los tipos más comunes de ransomware, este daño del ransomware de cifrado puede ser generalizado y devastador.

2-Doxware/leakware: Doxware o leakware roban información confidencial y amenazan con hacerla pública si la organización no paga el rescate. Este tipo de ransomware suele ser eficaz debido a la respuesta de pánico que provoca en el personal que no quiere que la reputación de su organización se vea dañada tras un ataque.

3-Scareware: Scareware está diseñado para imitar un problema informático, como un virus, y dirigir a las víctimas a un sitio para pagar para resolver el problema. Algunos solo usan ventanas emergentes en la pantalla para inundar la pantalla con alertas, mientras que otros bloquean el dispositivo para que el personal no pueda acceder a él.

4-Casilleros: los casilleros no cifran archivos individuales dentro de un sistema, sino que simplemente bloquean a los usuarios para que no puedan acceder a su infraestructura sin pagar para desbloquearla. Este ataque a menudo implica una pantalla simple que exige el rescate y puede incluir un temporizador para alentar una respuesta más

rápida de la organización.

5-Ransomware como servicio: RaaS se ha vuelto más popular en los últimos años y se refiere a actores de amenazas anónimos que actúan en nombre de otra parte para llevar a cabo un ataque. Desde infiltrarse en un sistema hasta cobrar el rescate, estos piratas informáticos anónimos reciben parte del pago a cambio de su ayuda.

Algunas de las debilidades clave que están bajo su control y que los actores de amenazas buscan para facilitar un ataque incluyen:

1-El uso de dispositivos o software desactualizados, que aumentan la probabilidad de que haya vulnerabilidades explotables en sus sistemas a las que los actores de amenazas pueden acceder a través de

2-Navegadores o sistemas operativos que no están parcheados

3-La falta de una copia de seguridad adecuada, lo que hace que el uso de malware para cifrar los archivos y datos de una organización sea más dañino y más fácil de aprovechar el pago de un rescate.
4- Concientización y capacitación en ciberseguridad que no se ha priorizado, lo que aumenta las posibilidades de que un ataque tenga éxito y la organización no tenga una respuesta de defensa coherente

Prevención ante el ransomware

Un sólido programa de capacitación en concientización ci-

bernética es una de las formas más impactantes en las que puede adelantarse a las amenazas potenciales. Las mejores prácticas incluyen:

1-No hacer clic en archivos adjuntos de correo electrónico sospechosos ni interactuar con enlaces que puedan contener malware

2-No compartir información personal que pueda ayudar a los atacantes a acceder a su sistema o dispositivo personal para infiltrarse en su organización

3-Mantener actualizados los sistemas operativos y las aplicaciones para aprovechar los últimos parches de seguridad que ayudan a proteger sus archivos y dispositivos

4-Evitar el uso de memorias USB desconocidas o fuentes de descarga no verificadas que podrían contener malware para infectar su dispositivo

5-Usar una VPN cuando se conecta a redes Wi-Fi públicas

6-Tener una copia de seguridad de datos sólida

7-Fortalecimiento de la autenticación de usuarios y otras políticas

8-Invertir en un programa anti-ransomware sólido

9-Implementación de ejercicios de simulación y capacitación específica sobre extorsión cibernética

10-Mantener un libro de jugadas de IR

Respuesta y recuperación

Entre los aspectos más importantes que debe incluir en su plan de respuesta se encuentran definiciones claras de roles y responsabilidades para los equipos e individuos involucrados, planes de continuidad comercial para minimizar el impacto de un ataque en sus clientes y usuarios, planes de comunicación y asociaciones con proveedores.

Los pasos básicos de una respuesta de ransomware generalmente se pueden dividir en las siguientes partes:

Evaluar y aislar

Después de validar que se está produciendo un ataque, es importante determinar su alcance: ¿cuán generalizado se ha vuelto? Comprender esto lo ayudará a detenerlo lo más rápido posible al sacar los dispositivos afectados de las redes de la organización a las que están conectados, evitando que el ransomware se propague a las unidades compartidas y otros dispositivos. También es una buena práctica desconectar sus copias de seguridad y otros sistemas para evitar que el ransomware también los infecte.

Analizar el daño

Una vez que haya protegido a su organización de daños mayores, sus equipos de respuesta pueden comenzar a investigar el alcance del ataque y determinar cuánto de su sistema se ha visto afectado. Determinar la variedad de ransomware que se usó, qué archivos y datos específicos se cifraron y si sus copias de seguridad son seguras y funcionan también son consideraciones que debe tomar al evaluar el incidente.

Ejecute su plan de respuesta

Una vez que tenga una visión clara de lo que se ha visto afectado, puede continuar con la recuperación de sus datos y encontrar una solución para restaurar el acceso al sistema a su personal.

De la A a la Z, el ransomware expuesto

Un informe realizado por la Dirección Nacional de Ciberseguridad explica en detalle todo lo que querés saber sobre el ransomware. Aquí el compartimos un resumen de tan interesante investigación.

Qué es el ransomware

El ransomware es un tipo de software utilizado generalmente por los cibercriminales para cifrar archivos o sistemas informáticos. El término incluye a todas las formas de código malicioso, como virus y gusanos informáticos. Su finalidad es "secuestrar información" y, de esta manera, impedir a una persona u organización el acceso a sus datos o dispositivos hasta que se haya pagado un dinero como rescate, que frecuentemente suele ser en criptomonedas para permitir al ciberdelincuente ocultar su rastro.

El ransomware se propaga, como otros tipos de malware, por múltiples vías. Algunas de ellas son a través de campañas de spam, vulnerabilidades o malas configuraciones de software, actualizaciones de software falsas, canales de descarga de software no confiables y herramientas de activación de programas no oficiales.

El ransomware es una de las amenazas más peligrosas para las organizaciones, pero la naturaleza y el alcance de sus ataques a menudo se malinterpretan, lo que lleva a precauciones inadecuadas, respuestas incorrectas y a ataques exitosos.

El ransomware es probablemente una de las amenazas cibernéticas más graves a las que se enfrentan personas usuarias y, sobre todo, organizaciones privadas y gubernamentales. ¿Por qué? Porque, en los últimos años, las bandas criminales -que crean este tipo de malware y lo ofrecen como servicio- han estado perfeccionando un enfoque diferente con objetivos más específicos, y las métricas de estos ataques son mucho más difíciles de obtener.

En los últimos años se ha visto una transición en los ataques de ransomware porque pasaron de ser ataques masivos (que apuntaban a un gran número de personas y solicitaban sumas modestas de rescates) a ser ataques dirigidos a sectores específicos, exigiendo montos mucho mayores a grupos de víctimas más pequeños. Estas víctimas elegidas tienen bolsillos más grandes y miembros que no pueden permitirse perder el acceso o el control de sus datos.

Cómo opera el ransomware

Una vez que el ciberdelincuente cifró los datos, es habitual que incluya un límite de tiempo para pagar, antes de que se produzca la destrucción total de los archivos secuestrados, su publicación o un incremento del valor del rescate, si no se paga a tiempo.

Las víctimas a menudo ven afectadas múltiples facetas de sus puntos de contacto digitales, desde ataques de denegación de servicios en sus sitios web hasta molestas demostraciones de la presencia de los cibercriminales en la red. Algunas de estas provocan una conmoción, como es el caso del print bombing, que consiste en utilizar las impresoras disponibles en la red de la víctima para imprimir el mensaje que exigen los ciberdelincuentes para el rescate. Esta situación impide que la gerencia pueda controlar la comunicación interna y externa sobre el incidente.

En resumen, el ransomware puede convertirse de un incidente de malware desafortunado en una guerra psicológica, cuyo objetivo es obligar a las víctimas a actuar contra su propia voluntad y sus intereses.

Los ataques pueden ser tan solo el resultado de malas prácticas de seguridad por parte de los empleados, una mala configuración del Protocolo de escritorio remoto (RDP) u otras herramientas de acceso remoto, o prácticas y procesos defectuosos, tanto dentro de su propia organización como de sus proveedores de servicios u otros eslabones de su cadena de suministro.

En qué consiste el cifrado de información

Cuando hablamos del cifrado criptográfico de información, nos referimos a una operación matemática que toma un dato y una clave, y modifica el dato en base a esta última. Para que el dato vuelva a su forma original, se debe aplicar una función de descifrado. En otras palabras, el cifrado consiste en ocultar la información con técnicas de codificación para evitar que los datos sean legibles por quien no tenga la clave de decodificación.

Existen dos esquemas de criptografía: Criptografía simétrica y Criptografía asimétrica.

En general, los ransomware aplican un esquema de criptografía simétrica sobre la información que afectan, generando claves de cifrado aleatorias. Estas claves se transmiten por Internet a los servidores de los atacantes, de modo que puedan ser enviadas a la víctima luego de pagado el rescate.

En algunos casos, también utilizan un esquema asimétrico para almacenar, junto con los archivos de la víctima, las claves utilizadas para cifrar la información. De esta forma, no necesitan contar con conexión a Internet al momento de cifrar los archivos. Simplemente cifran con la clave pública las claves de cifrado de los archivos y, al recibir el pago, enviarán un software de descifrado que conoce la clave privada necesaria para recuperar las claves.

Niveles de extorsión que utilizan los atacantes

Actualmente, existen diferentes niveles o marcos de extorsión:
Primera extorsión: consiste en el cifrado de la información, y la exigencia de un pago para recuperarla.

Doble extorsión: además del cifrado, se amenaza con filtrar públicamente la información secuestrada.

Triple extorsión: se añaden ataques de denegación de servicio, afectando aún más la disponibilidad de los servicios afectados por el cifrado de la información.

Cuádruple extorsión: los atacantes se comunican con clientes y proveedores de la víctima para exponer la situación y, eventualmente, filtrar información. En algunos casos, exigen el pago directamente a los proveedores y/ o clientes de la víctima.

Cada uno de estos niveles o marcos de extorsión contiene a los anteriores. Así, el último contiene a los tres anteriores, el tercero a los dos anteriores y el segundo al primero.

La seguridad de la información, la clave para prevenir el ransomware

Es necesario que se implementen procesos y políticas para garantizar la seguridad de las instalaciones y de los sistemas. Un escenario bastante común es que una organización sea atacada a través de un activo conectado a Internet, que el personal de seguridad de la organización no sabía que existía hasta después del ataque.

Sin embargo, por más que se

hayan implementado las políticas y protocolos de seguridad o se esté trabajando para implementarlos, las reglas por sí solas no garantizarán la seguridad total de los accesos.

Aún será necesario que la organización se asegure de que todo el personal cumpla con las instrucciones y que, al mismo tiempo, estén preparados para manejar un ataque, es decir, para saber qué hacer ante un incidente, cómo resolverlo y volver a estar operativos.

Asimismo, la organización deberá contar con políticas para abordar la seguridad del acceso remoto. Las recomendaciones se sustentan en diferentes estrategias y técnicas:

A. Documentar el problema: asegurarse de que todos los activos conectados a Internet de su organización sean conocidos por las personas a las que se les ha asignado la tarea de protegerlos. Disponer de un proceso para garantizar que se incluyan todos los dispositivos nuevos.

B. Limitar los activos expuestos: asegurarse de que ningún activo digital sea accesible de manera remota directamente desde Internet, a menos que haya sido aprobado para usarse de esa manera y esté configurado adecuadamente.

C. Proteger los activos expuestos: si definitivamente se debe usar el Protocolo de escritorio remoto (RDP) sin una red privada virtual (VPN), se deben tener en consideración las siguientes sugerencias:

a. Cambiar la contraseña de la cuenta de usuario a la que se está conectando en la máquina remota con regularidad. Asegurarse de cambiar la contraseña predeterminada que a veces se genera automáticamente para las instancias en la nube.

b. Hacer cumplir la complejidad de la contraseña. Es obligatorio que sea una frase de contraseña larga que contenga más de 15 caracteres, sin frases relacionadas con la organización, con los nombres de productos o con los usuarios.

c. Establecer un límite de bloqueo de cuenta para bloquear el acceso remoto después de cierta cantidad de intentos fallidos consecutivos de inicio de sesión. Al configurar la computadora para que bloquee una cuenta durante un período de tiempo tras una serie de conjeturas incorrectas, obstaculizará a los atacantes que utilizan herramientas automáticas de adivinación de contraseñas (ataque por fuerza bruta).

d. Probar e instalar los parches para todas las vulnerabilidades conocidas y asegurarse de que las más conocidas y obvias se encuentren entre los defectos corregidos. Si los parches no se pueden instalar en una computadora determinada, planificar su reemplazo oportuno.

e. Utilizar más de un factor de autenticación. Hay tres factores posibles: algo que uno sabe, como el nombre de usuario y la contraseña; algo que uno es, como la huella dactilar o de voz; y algo que uno tiene, como el teléfono, que puede recibir un código de acceso de un solo uso o ejecutar una aplicación de autenticación que generará el código cuando lo necesite. Sin embargo, si usa como segundo factor un código enviado a un teléfono, evitar los códigos por SMS, porque los delincuentes ya se las ingeniaron para interceptar este tipo de mensajes de autenticación.

f. Restringir los derechos de acceso al servidor para un grupo limitado de usuarios. Esto reduce la superficie de ataque de los servidores, ya que limita la can-

tidad de usuarios que pueden acceder a ellos.
g. Aislar las computadoras no seguras a las que se deba acceder desde Internet usando el Protocolo de acceso remoto (RDP).

Algunas modalidades de ataques de ransomware

El uso de software legítimo o "living off the land "

Algunos atacantes intentan introducir un fragmento de código malicioso lo más pequeño posible para minimizar la detección. A continuación, el malware emplea la estrategia conocida en inglés como "living off the land" (LotL), es decir, hace uso de software legítimo para extender su penetración en la red.

Uno de los ejemplos más arquetípicos, en donde los atacantes se aprovecharon de vulnerabilidades no corregidas en un software legítimo del sistema, fue el reconocido ransomware WannaCryptor, que se propagó usando indebidamente una vulnerabilidad de alta severidad.

Cómo evitar los ataques LotL

Será clave ejercer un acto de monitorización y seguimiento del sistema informático, atendiendo a todos los procesos que esté albergando para encontrar acciones sospechosas y accionar a tiempo.

Contar con una solución de ciberseguridad avanzada capaz de monitorizar todos los procesos del sistema en busca de comportamientos anómalos o posibles amenazas para acabar con ellas antes de que se manifiesten, entre otras.

Movimiento Lateral

El término movimiento lateral se utiliza para describir la estrategia de afianzarse en un sistema y utilizarlo para infectar otros dispositivos a los que se puede llegar desde allí. Por ejemplo, los atacantes pueden utilizar credenciales comprometidas para infectar un servidor que ni siquiera está presente en la organización objetivo, y luego usar su conexión a la infraestructura principal para entregar el ransomware.

Cómo prevenir los ataques de movimiento lateral en la red

Detectar en tiempo real y analizar las amenazas dentro de la red, captando el robo de credenciales, el esparcimiento lateral de programas maliciosos, ransomware y de ataques dirigidos dentro de redes de usuarios, centros de datos, nube, entornos IOT y SCADA.

Establecer alertas fundamentadas, evaluación de vulnerabilidades de las rutas de ataque, análisis detallado e informes y reproducción de ataques transcurridos en el tiempo para fortalecer las defensas generales.

Realizar pruebas de penetración puede ayudar a las organizaciones a cerrar las partes vulnerables de la red que podrían permitir un movimiento lateral.

La seguridad Zero Trust es una filosofía de seguridad de red que no confía por defecto en ningún usuario, dispositivo o conexión. Una red Zero Trust asume que todos los usuarios y dispositivos representan una amenaza y reautentíca continuamente tanto a los usuarios como a los dispositivos. Zero Trust también utiliza un enfoque de mínimos privilegios para el control de acceso y divide las redes en pequeños segmentos.

La seguridad en los puntos de conexión implica escanear con regularidad los dispositivos de los puntos de conexión (ordenadores de escritorio, portátiles, teléfonos inteligentes, etc.) con software antimalware, entre otras tecnologías de seguridad.

Gestión de acceso e identidad correcta (IAM) es un componente fundamental para evitar el movimiento lateral. Los privilegios de los usuarios se tienen que gestionar de forma estricta: si los usuarios tienen más privilegios de los que realmente necesitan, las consecuencias de una toma de posesión de la cuenta son todavía más graves.

Además, el uso de la autenticación en dos fases (2FA), que significa exigir a un usuario que demuestre su identidad de dos maneras diferentes antes de concederle acceso, lo cual puede ayudar a detener el movimiento lateral.

Amenazas dirigidas al Protocolo SMB

El protocolo Bloque de Mensajes del Servidor (SMB), que se utiliza sobre todo para compartir archivos e impresoras en redes corporativas, también se puede usar indebidamente como un servicio remoto para introducir el ransomware.

En el primer cuatrimestre de 2021, las tecnologías de una empresa privada bloquearon 335 millones de ataques por fuerza bruta a servicios SMB orientados al público. Aunque esa cifra representa una disminución del 50% en comparación con la de los últimos cuatro meses del 2020, los ataques a través de SMB siguen siendo una amenaza importante.

Recomendaciones para protegerse contra las amenazas dirigidas al protocolo SMB:

Deshabilitar SMBv1 y SMBv2. Tener en cuenta que se deberá gestionar cualquier dependencia existente en estas versiones obsoletas.

Actualizar a la última versión del protocolo SMB, que actualmente es SMBv3.

Utilizar la configuración de la directiva de grupo para asegurar que se requiera la firma de SMB entre los hosts y los controladores de dominio para evitar ataques de reproducción en su red, entre otras.

Ataques de ransomware por correo electrónico

Algunos atacantes todavía siguen usando archivos adjuntos en correos electrónicos para instalar malware como etapa inicial de una infección que termina con ransomware. Los ciberdelincuentes pueden usar este vector para instalar malware en la máquina del destinatario del correo electrónico o para lograr afianzarse en una máquina que está dentro de la red de una organización. Esta presencia les sirve de base para luego intentar robar los datos valiosos y cifrar los archivos de toda la organización, para más tarde hacer un pedido de rescate.

Recomendaciones para proteger a la organización contra ataques de ransomware provenientes del correo electrónico:

La primera línea de defensa es filtrar todo el correo entrante en busca de spam y mensajes de phishing.

Es posible ir un paso más lejos mediante la implementación del bloqueo de todos los tipos de archivos adjuntos que la organización normalmente no espera recibir por correo electrónico. Sin embargo, esta estrategia sólo será adecuada para ciertos tipos de sectores y probablemente requerirá cambiar algunos hábitos de trabajo.

Verificar que todos los endpoints (dispositivos informáticos remotos que se comunican a una red a la que están conectados, como por ejemplo ordenadores de escritorio o portátiles, tablets, servidores y estaciones de trabajo) estén ejecutando un software de protección de alta calidad. De esa manera, se espera evitar que los empleados accedan a páginas web, donde se sabe que se alojan malware. También se puede utilizar el filtrado de contenido web como capa adicional de protección.

Además de bloquear sitios web maliciosos, un filtro de contenido web puede impedir que los em-

pleados visiten sitios web que se consideran inapropiados en el ámbito laboral.

Asimismo, será necesario verificar que todos los dispositivos estén ejecutando la última versión del producto de seguridad y que estén recibiendo correctamente las actualizaciones.

Otra medida, será mantener actualizada la capacitación en ciberseguridad de los empleados para que refleje las últimas tendencias en el panorama de amenazas.

Ataques de ransomware por cadena de suministro

Un vector de ataque de ransomware que merece especial atención en la actualidad es la cadena de suministro de software. Así como el ransomware se remonta al siglo pasado, los riesgos en la cadena de suministro de software también. Cuando el vector de ataque principal para los virus informáticos eran los discos de computadora, y estos eran la forma principal en que las personas adquirían software, el malware a veces terminaba en discos de producción o en los discos de software de prueba que solían distribuirse con revistas de informática.

La primera línea de defensa contra este tipo de ataques es tener un buen producto de protección para endpoints que incluya herramientas de EDR.

Ataques por vulnerabilidades

Si bien los ciberdelincuentes pueden beneficiarse tanto de las vulnerabilidades conocidas como de las desconocidas, el uso de vulnerabilidades 0-day por lo general pertenece al mundo de los grupos de Amenaza Persistente Avanzada (APT)-un conjunto de amenazas sofisticadas que evaden las herramientas de seguridad tradicionales- y los actores maliciosos patrocinados por Estados.

Antes de avanzar, cabe aclarar que un exploit es un ataque que aprovecha las vulnerabilidades de las aplicaciones, las redes, los sistemas operativos y/o el hardware. Generalmente, toman la forma de un programa de software o de una secuencia de código previsto para tomar el control de los ordenadores o robar datos de la red.

El uso de las redes privadas virtuales (VPN) en grandes instituciones y empresas, si bien es altamente efectivo, añade una responsabilidad adicional con respecto a la actualización del producto cuando sea necesario.

Otras medidas preventivas

Segmentación de la red

Existen varios enfoques para implementar una estrategia de seguridad y el más importante es la segmentación de la red, que consiste en una técnica de seguridad que divide una red en distintas subredes más pequeñas, que permiten a los equipos de red compartimentar las subredes y otorgar controles y servicios de seguridad únicos a cada subred.

Seguridad en la nube

El bajo costo y la relativa facilidad con la que se pueden aprovisionar nuevos servidores en la nube y conectarlos al resto de la infraestructura digital de la organización han convertido a ésta en un terreno de caza fértil para los delincuentes. Sin duda, cualquier uso de la nube por cualquier parte de la organización debe estar debidamente autorizado y configurado de manera segura. Además, como todos los otros sistemas, los que están en la nube deben tener programado un régimen apropiado de creación de backups y recuperación.

Algunos de los sistemas de tu organización pueden depender de software que deja de funcionar cuando actualiza a la última versión de una aplicación o sistema operativo. Sin embargo, el elevado costo de un ataque de ransomware dentro de su red justifica el esfuerzo de abordar esos desafíos y mantener un régimen de instalación de parches rápido y completo para que el ransomware se quede afuera.

Creación de backups

Se suele decir que si el ransomware ingresa a la organización, un programa de backup y recuperación completa, adecuadamente administrado, es un mecanismo de defensa vital y constituye un elemento crucial para la recuperación posterior. Hay mucha verdad en esta afirmación y son varias las buenas razones para tener un programa de este tipo, pero hay que recordar que algunos ataques de ransomware se ejecutan en un período de tiempo prolongado, durante el que también puede haber hecho un backup del ransomware, comprometiendo así la posibilidad de lograr una restauración sin problemas.

Un backup completo incluye los datos y el estado del sistema en todas los endpoints, servidores, buzones de correo, unidades de red, dispositivos móviles y máquinas virtuales. El análisis detallado de la estrategia de backup y recuperación para grandes corporaciones está fuera del alcance del presente white paper, pero debe quedar claro que contar con una estrategia de este tipo es más crítico que nunca.

Almacenamiento externo

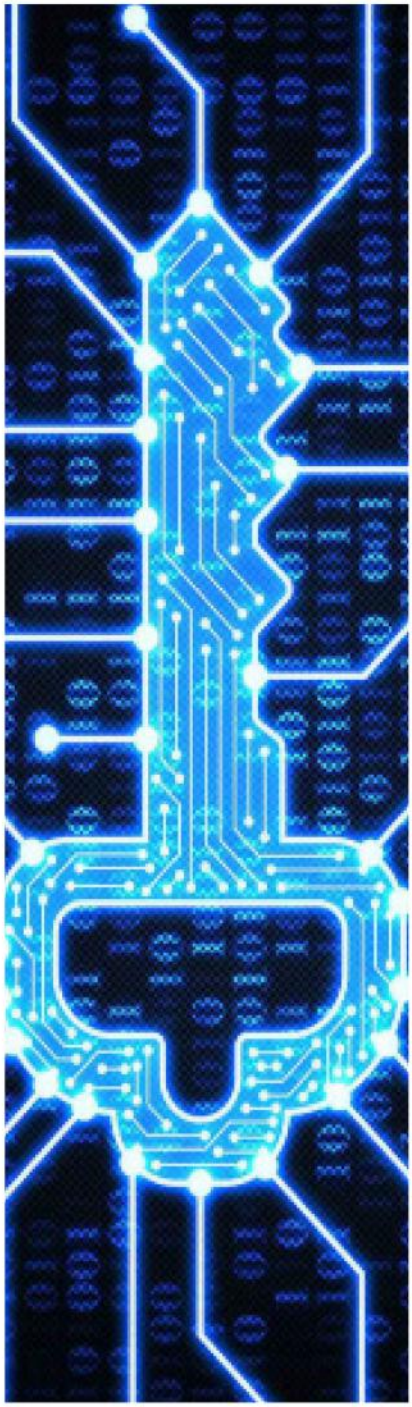
No esté online en forma rutinaria y permanente;

Proteja los datos respaldados de modificaciones o sobreescrituras automáticas y silenciosas por malware cuando la instalación remota esté online;

Proteja las generaciones anteriores de datos respaldados contra las infecciones, de modo que incluso si ocurre un desastre en los últimos backups, al menos se puedan recuperar algunos datos, incluyendo las versiones anteriores de los datos actuales;

Proteja al cliente detallando las responsabilidades legales o contractuales del proveedor, por ejemplo, que indique qué sucede si el proveedor cierra, etc.

El informe completo puede verse en está página



Ransomware: panorama de ataques y tendencias

El Índice de Inteligencia de Amenazas de IBM Security X-Force mapea nuevas tendencias y ataques patrones extraídos de miles de millones de puntos de datos que van desde dispositivos de detección de redes y terminales, respuesta a incidentes (IR) y más.

En esta nota nos enfocaremos sobre lo que el Índice de Inteligencia de Amenazas de IBM Security X-Force dice sobre el ransomware.

Durante más de tres años, el ransomware ha sido el principal tipo de ataque observado por X-Force, y 2021 no fue una excepción. Veintiún por ciento de los ataques remediados por la respuesta a incidentes de X-Force en 2021 fueron ataques de ransomware. Esto es ligeramente inferior al año anterior, cuando el 23 % de los ataques que remedió X-Force fueron ataques de ransomware; sin embargo, el volumen de ataques de ransomware se ha mantenido constante año tras año.

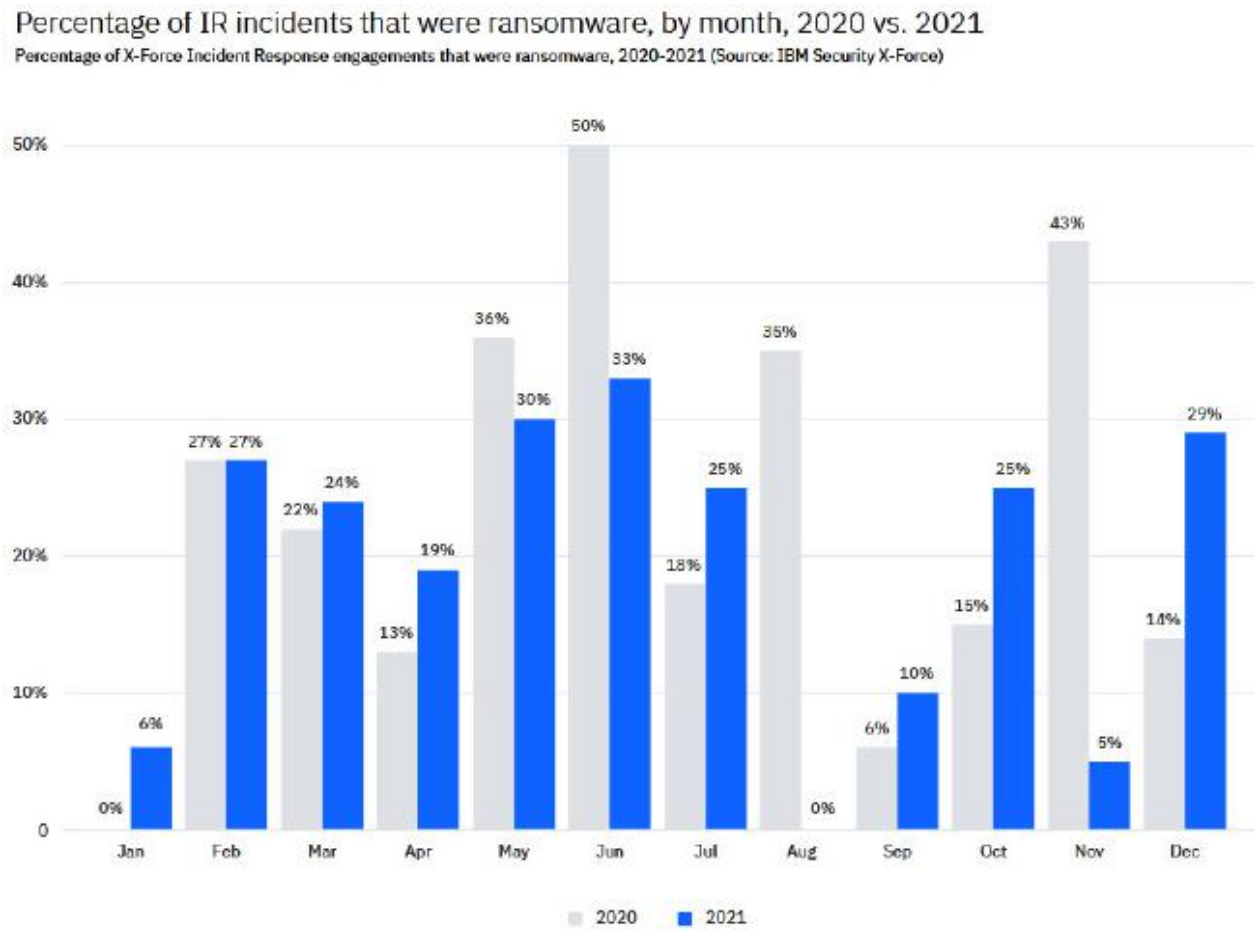
La frecuencia de los ataques de ransomware que observa X-Force tiende a cambiar a lo largo del año, con mayo y junio tendiendo a ver mayores frecuencias de ataques, mientras que enero tiende a ver más abajo. Además, los ataques de ransomware parecen disminuir a fines del verano o principios de otoño. En 2021, esa caída se produjo en gran medida en agosto y nuevamente en noviembre, probablemente impulsado por el cierre permanente o temporal de varios grupos en los meses anteriores: DarkSide y Babuk en mayo, Avaddon en junio y REvil en octubre.

Según la investigación de X-Force, 17 meses es el promedio tiempo antes de que un grupo de ransomware cambie de marca o cierre hacia abajo, con una mediana de 18 meses. Grupos de ransomware a menudo surgen y cambian de marca una vez que hay una amenaza de arresto o acción por parte de la policía. En algunos casos, la ley la acción de cumplimiento obliga a los grupos de ransomware a cerrar abajo por completo. A pesar de este ambiente dinámico, o tal vez por eso, muchos actores de ransomware permanecen en general, y X-Force evalúa que el ransomware criminal la actividad continuará en el futuro previsible, con base de los altos beneficios que genera esta actividad y de la actual limitación en la aplicación de la ley para el cierre generalizado reducir la actividad del ransomware

De las cepas de ransomware observadas por X-Force en 2021, REvil representó el 37%, más de un tercio: de todos los incidentes de ransomware que nuestro equipo remedió. Un fuerte segundo fue Ryuk, representando el 13% de los ataques observados el año pasado. Actores de REvil a mediados de octubre de 2021 parecen haber cerrado permanentemente las operaciones, probablemente debido a la aplicación de la ley actividad. Tanto Ryuk como REvil constituyen algunos de los ransomware de más larga duración, habiendo surgido en abril de 2019 y agosto de 2018, respectivamente.

Cómo ocurren los ataques de ransomware

Desde el X-Force Incident Response han desarrollado un sistema de cinco etapas modelo que define el patrón común observado en la mayoría de los incidentes de ransomware.



Etapa 1: Acceso inicial

Los vectores de acceso más comunes para Los ataques de ransomware siguen siendo phishing, explotación de vulnerabilidades, y servicios remotos como control remoto Protocolo de escritorio.

Etapa 2: Post explotación

Dependiendo del vector de acceso inicial, la segunda etapa puede implicar una herramienta intermedia de acceso remoto (RAT) o malware antes de establecer interactivo acceder con una herramienta de seguridad ofensiva como como Cobalt Strike o Metasploit.

Etapa 3: Comprender y ampliar

Durante la tercera etapa del ataque, los atacantes se han centrado sistemáticamente en la comprensión del sistema local y dominio al que actualmente tienen acceso y adquirir credenciales adicionales para permitir el movimiento lateral.

Etapa 4: Recopilación y exfiltración de datos

Casi todos los incidentes de ransomware X-Force IR ha respondido desde 2019 ha implicó la táctica de la “doble extorsión” de robo de datos y ransomware.

Durante la etapa 4 del ataque, el foco del ransomware los operadores cambiaron principalmente a identificar datos valiosos y exfiltrarlos.

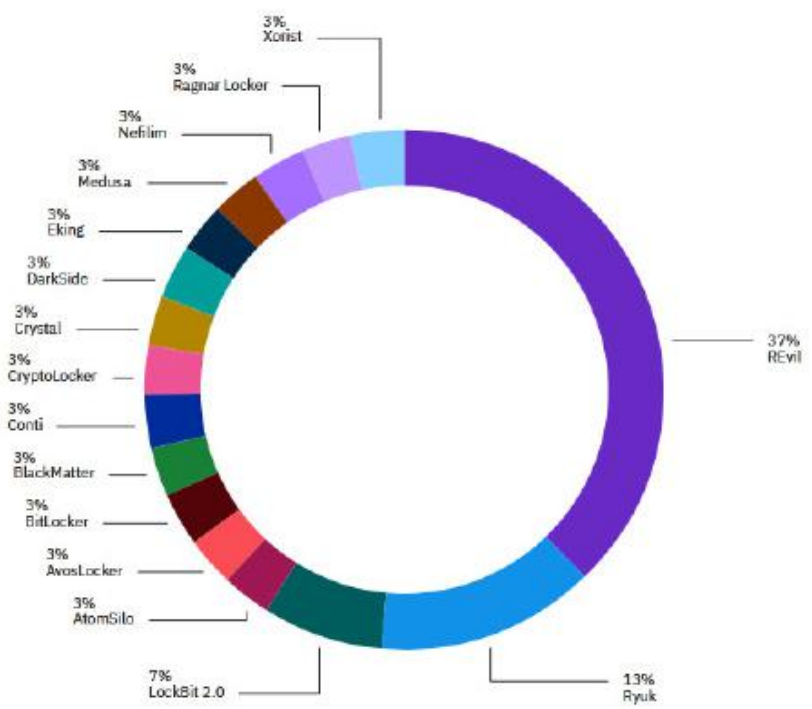
Etapa 5: implementación de ransomware

En casi todos los incidentes de ransomware al que ha respondido X-Force IR, los operadores de ransomware apuntaron a un dominio controlador como el punto de distribución para la carga útil del malware.

Una nueva tendencia preocupante en ransomware ha sido la expansión de la táctica de "triple extorsión". En este tipo de ataque, los actores de amenazas encriptan y roban datos y también amenazan participar en un ataque de denegación de servicio distribuido (DDoS) contra los afectados. Este tipo de ataque es particularmente problemático para las organizaciones porque las víctimas tienen sus redes rehenes con dos tipos de ataques maliciosos, a menudo simultáneamente, y luego son víctimas aún más por el robo (y a menudo) fugas de datos.

Types of ransomware observed in 2021

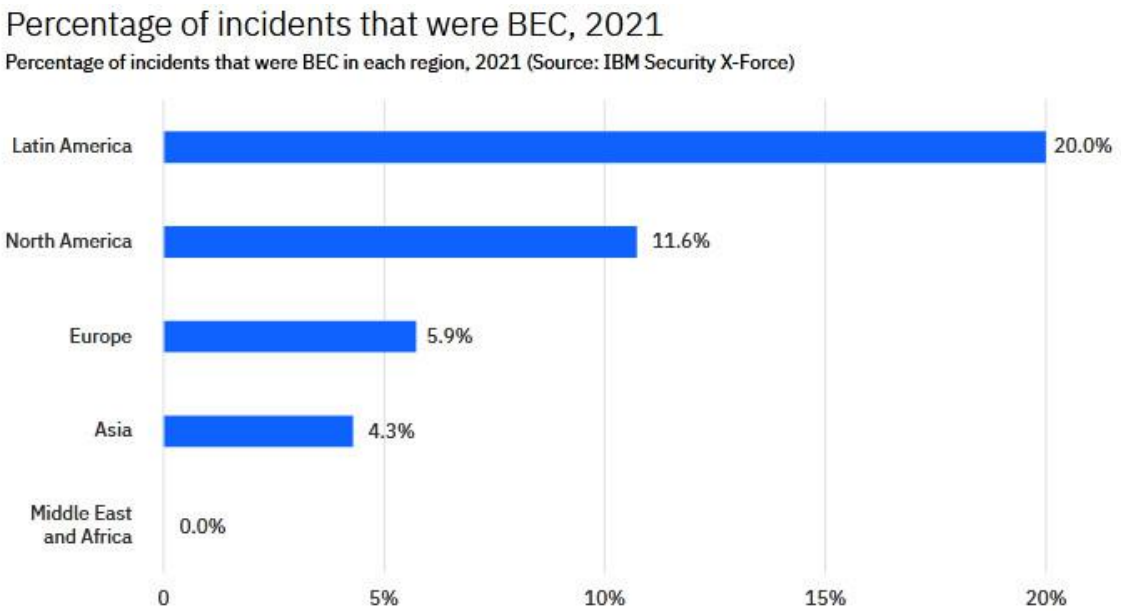
Ransomware types observed by X-Force Incident Response in 2021
(Source: IBM Security X-Force)



La industria manufacturera la más atacada de las OT por ransomware

En términos de industrias con redes OT, X-Force observó que la fabricación fue la más atacada en 2021 por un margen significativo, víctima del 61 % de los incidentes que X-Force ayudó a remediar. Los actores de ransomware en particular consideran que la fabricación es un objetivo atractivo, probablemente debido a la baja tolerancia de estas organizaciones al tiempo de inactividad.

Para todas las industrias con redes OT en las que X-Force observó ataques en 2021 (ingeniería, minería, servicios públicos, petróleo y gas, transporte y fabricación), el ransomware volvió a liderar los tipos de ataque, representando el 36 % de todos los ataques y haciéndose eco del ataque general, tendencia en todas las industrias. Mientras las redes de TI estaban comprometidas en la gran mayoría de estos ataques, el impacto se trasladó a la tecnología opera-



tiva de las víctimas en muchos de estos casos.
Otros tipos principales de ataques incluyeron acceso al servidor, DDoS, RAT, información privilegiada y operaciones de recolección de credenciales.

Enfoque de ransomware en ESXi

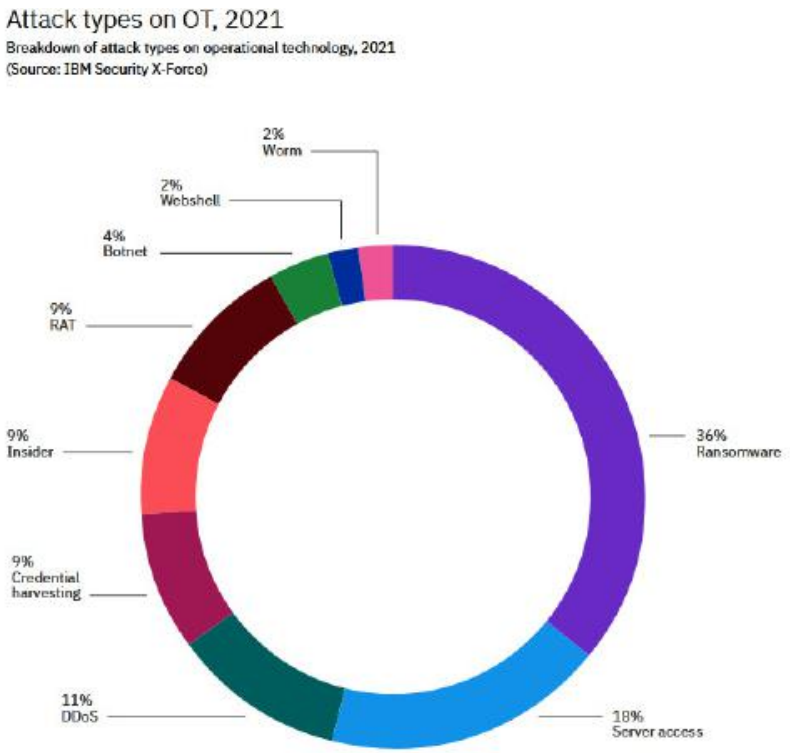
Al analizar las tendencias de malware que afectan los entornos de Linux, X-Force observó que varias familias de ransomware cambiaron sus miras para apuntar a los servidores VMWare ESXi basados en Linux.

A medida que más organizaciones confían cada vez más en la virtualización, los autores de ransomware descubren que puede ser más efectivo cifrar los archivos de la máquina virtual (VM) en lugar de infectar los sistemas operativos que se ejecutan dentro de ellos.

En 2020, X-Force IR observó una variante de Linux del ransomware SFile implementada contra un servidor ESXi, y en 2021 varias otras familias de ransomware parecieron seguir su ejemplo, incluidas REvil, HelloKitty, Babuk y BlackMatter. Estas variantes a menudo harán uso de la propia herramienta de administración de línea de comandos de ESXi, esxcli, para enumerar y apagar las máquinas virtuales en ejecución antes de cifrarlas.

América Latina

El principal tipo de ataque para América Latina en 2021 fue ransomware, conformando el 29% de los ataques, seguido por BEC (21%) y credenciales cosecha (21%), empatando en el segundo lugar. REvil fue lo más cepa de ransomware común observada en América Latina, que constituye 50% de los ataques de ran-



somware X-Force remediados, con Ryuk y AtomSilo también se está observando apuntando a organizaciones en la región.

Recomendaciones de mitigación de riesgos

Zero Trust ayuda a disminuir el riesgo de ataques principales

La confianza cero es un cambio de paradigma, una nueva forma de abordar los problemas de seguridad, que asume que ya ha ocurrido una violación y tiene como objetivo aumentar la dificultad para que un atacante se mueva a través de una red. En esencia, es comprender dónde residen los datos críticos y quién tiene acceso a estos datos, y crear medidas de verificación sólidas en toda una red para garantizar que sólo las personas adecuadas accedan a esos datos de la manera correcta.

La automatización de la seguridad mejora la respuesta a incidentes

El equipo de respuesta a incidentes de X-Force aborda cientos de incidentes cada año, en una variedad de geografías, asiste a los analistas de respuesta a incidentes internos y aborda una variedad de tipos de ataques. La velocidad es esencial, ya sea que eso signifique identificar y erradicar a los actores de amenazas antes de que puedan implementar ransomware en una red, o resolver problemas de manera rápida y eficiente para crear ancho de banda para el próximo incidente. En este entorno acelerado, la automatización de la seguridad es clave: externalización de tareas mecánicas que pueden requerir horas de un analista humano o de un equipo, e identificación de mecanismos para mejorar los flujos de trabajo.

La detección y la respuesta extendidas brindan una ventaja significativa sobre los atacantes

Las tecnologías de detección y respuesta, en particular cuando se combinan varias soluciones diferentes en una solución extendida de detección y respuesta (XDR), brindan a las organizaciones una ventaja significativa para identificar y erradicar a los atacantes de una red antes de que puedan llegar a la etapa final de su ataque. como la implementación de ransomware o el robo de datos.

El ABC del SOC: funcionalidades, tipos, y retos de los profesionales

Un centro de operaciones de seguridad (SOC) es una instalación centralizada para un equipo de especialistas en seguridad de la información y profesionales de TI que analizan, monitorean y protegen una organización contra ataques cibernéticos.

Los equipos de SOC monitorean continuamente las redes, el tráfico de Internet, los servidores, los escritorios, las bases de datos, los dispositivos de punto final, las aplicaciones y otros activos de TI en busca de indicaciones de un evento de seguridad y manejan la respuesta a incidentes.

El personal del SOC suele tener todas las habilidades que necesita para identificar y responder a los incidentes de ciberseguridad. Sin embargo, también cooperan con otros departamentos o equipos para compartir información sobre incidentes con las partes interesadas relevantes. La mayoría de los SOC funcionan las 24 horas del día, los 7 días de la semana, con empleados que trabajan por turnos para mitigar las amenazas y administrar la actividad de registro. Algunas organizaciones externalizan su SOC a proveedores externos.

Los SOC son una estrategia clave para minimizar los costos de las filtraciones de datos. Ayudan a las organizaciones a responder rápidamente a las intrusiones y mejoran constantemente los métodos de prevención y detección de amenazas.

Beneficios de un SOC

La principal ventaja de tener un centro de operaciones de seguridad es mejorar la detección de incidentes de seguridad a través del análisis continuo y el monitoreo continuo de la actividad. Al estudiar esta actividad en los terminales, servidores, redes y bases de datos de una organización las 24 horas del día, los 7 días de la semana, los equipos de SOC garantizan una identificación y una respuesta oportunas a los incidentes de seguridad. Las organizaciones confían en el SOC para protegerse contra incidentes de seguridad e intrusiones, independientemente de la hora del día, la fuente o el tipo de ataque.

Muchos estudios han demostrado que el tiempo promedio para detectar y responder a una infracción es de más de 100 días. Establecer un SOC ayuda a las organizaciones a mejorar su capacidad para detectar y reaccionar ante amenazas de manera oportuna para eliminar o reducir el impacto catastrófico de los ataques cibernéticos.

10 funciones de seguridad del SOC

1. Mantenimiento de inventario de recursos disponibles

El SOC supervisa dos tipos de activos: procesos, dispositivos y aplicaciones que requieren protección y herramientas defensivas que pueden ayudar a lograr esta protección.

Qué protege el SOC: los equipos del SOC no pueden proteger datos y dispositivos que no pueden ver. Sin control y visibilidad desde el dispositivo hasta la nube, habrá áreas que se pasan por alto en la postura de seguridad de la red que los atacantes pue-

channeltalks

Actualiza tu modelo de negocios

Un evento presencial enfocado en la actualización del modelo de negocios para el canal IT junto a las principales marcas y mayoristas locales.


NEUQUÉN
12MAY


TUCUMÁN
9JUN


SANTA FE
7JUL


SANTA CRUZ
14JUL


RESISTENCIA
4AGO


ASUNCIÓN
18AGO


SANTIAGO
8SEPT


MONTEVIDEO
6OCT


GUAYAQUIL
12OCT


CÓRDOBA
20OCT


LA PAZ
27OCT


LIMA
10NOV


MENDOZA
17NOV

¡Agendá el lineup del Channel!

den identificar y explotar. El SOC tiene como objetivo lograr una visión integral del panorama de amenazas de la organización, incluidas las redes, los puntos finales, las aplicaciones y los servidores. Esta vista también debe incluir el tráfico que fluye entre estos activos y los servicios de terceros.

Cómo protege el SOC: los equipos del SOC también deben tener las habilidades para usar todas las herramientas de ciberseguridad disponibles y deben ejercer correctamente todos los flujos de trabajo de seguridad y las mejores prácticas para maximizar la agilidad y la eficiencia de los procesos del SOC.

2. Preparación y Mantenimiento Preventivo

Incluso la metodología de respuesta mejor equipada y más ágil no es tan buena como para evitar que ocurran problemas en primer lugar. Para detener los ciberataques antes de que sucedan, el SOC utiliza dos tipos de medidas preventivas:

Preparación: los miembros del equipo deben mantenerse actualizados sobre las últimas innovaciones de seguridad, las últimas tendencias en ciberdelincuencia y el desarrollo de amenazas innovadoras. Esta investigación puede ofrecer orientación para las iniciativas de seguridad cibernética en el futuro y ayudar a crear planes de recuperación ante desastres para guiar a la organización en una emergencia .

Mantenimiento preventivo: implica todas las acciones que pueden dificultar el éxito de los ataques cibernéticos, incluida la actualización y el mantenimiento de los sistemas existentes con regularidad, la reparación de vulnerabilidades, la actualización de las políticas de firewall, las listas blancas, las listas negras y el fortalecimiento de los sistemas de TI.

3. Monitoreo Continuo

El SOC utiliza herramientas para escanear la red continuamente y marcar cualquier actividad sospechosa o anomalía. El monitoreo de la red 24/7 proporciona al SOC notificaciones de amenazas emergentes, lo que permite mitigarlas o prevenir ataques en sus primeras etapas.

Las herramientas de monitoreo pueden incluir detección y respuesta de punto final (EDR) e información de seguridad y gestión de eventos (SIEM). Las herramientas avanzadas emplean análisis de comportamiento para aprender la distinción entre las operaciones cotidianas normales y el comportamiento de amenaza real, lo que limita el grado de clasificación y análisis que deben realizar los humanos.

4. Priorización y gestión de alertas

Cuando las herramientas de monitoreo brindan alertas, el SOC debe examinar cada una de ellas detenidamente, eliminar los falsos positivos y decidir qué tan serias son las amenazas reales y a qué podrían estar dirigidas. El SOC es responsable de priorizar las alertas, identificar cuáles pueden ser incidentes de seguridad reales e investigarlos para permitir una respuesta rápida.

5. Respuesta a amenazas

Tan pronto como el equipo SOC identifica un incidente, actúa como el primer respondedor y lleva a cabo acciones como aislar o cerrar puntos finales infectados, detener procesos dañinos, eliminar malware y más. El objetivo es mitigar la amenaza con una interrupción mínima de la continuidad de la organización.

6. Recuperación y remediación

Un SOC supervisa los pasos que se toman después de un ataque, lo que garantiza que la organización mitigue la amenaza de manera efectiva y se comunique con las partes afectadas. No es suficiente que los equipos SOC

emitan alertas y vean registros. Un componente central de la respuesta a incidentes es ayudar a las organizaciones para que puedan recuperarse de manera efectiva de un incidente.

Por ejemplo, la recuperación puede implicar la limpieza de ransomware o malware de los sistemas afectados, el restablecimiento de contraseñas para cuentas comprometidas, la limpieza y la creación de nuevas imágenes de puntos finales infectados.

7. Gestión de registros

El SOC debe recopilar, mantener y revisar periódicamente los registros de todas las comunicaciones y actividades de la red en toda la organización. Esta información ayuda a establecer una línea de base para la actividad regular de la red, puede exponer amenazas y puede ser utilizada por especialistas en seguridad y TI para análisis forense y remediación después de un incidente.

Muchos SOC utilizan un SIEM para correlacionar y agregar las fuentes de datos de los firewalls, los sistemas operativos, los puntos finales y las aplicaciones, creando un depósito central de datos de seguridad.

Los equipos SOC producen análisis basados en datos. Este análisis ayuda a una organización a afinar las herramientas de monitoreo y alerta de seguridad y atender las vulnerabilidades. Por ejemplo, basándose en la información recopilada de los archivos de registro y de diferentes fuentes, un equipo de SOC pue-

de presentar una estrategia de segmentación de red mejorada o un régimen de aplicación de parches. Mejorar la ciberseguridad existente es una responsabilidad central de un SOC.

8. Investigación de la causa raíz
Después de un incidente, el SOC debe determinar con precisión qué sucedió, por qué, cómo y cuándo. A lo largo de esta investigación, los equipos de SOC se basan en los datos de registro y otros detalles para descubrir el origen del problema, lo que les ayudará a evitar que surjan problemas similares en el futuro.

9. Mejora del proceso de seguridad
Los ciberdelincuentes refinan constantemente sus tácticas y herramientas para estar un paso por delante de las defensas, el SOC debe realizar mejoras de forma continua. Una forma de mejorar el proceso de seguridad es realizar investigaciones post-mortem de los incidentes e identificar cómo podría haberlo hecho mejor el equipo SOC. Otra forma es realizar sesiones de práctica realistas como juegos de guerra con equipos azules y equipos rojos.

10. Gestión de Cumplimiento
Las organizaciones se protegen a sí mismas mediante estándares de seguridad externos y el cumplimiento de una política de seguridad. Los estándares externos incluyen ISO 27001x, el Reglamento general de protección de datos (GDPR) y el Marco de ciberseguridad (CSF) del NIST. Las organizaciones necesitan un SOC para ayudar a asegurarse de que cumplen con los requisitos de las mejores prácticas clave y los estándares de seguridad.

¿Cuáles son los roles de equipo del SOC?

El SOC está formado por ingenieros expertos, analistas de seguridad y supervisores que se aseguran de que todo funcione sin problemas. Son especialistas capacitados específicamente para administrar y monitorear amenazas de seguridad. Los equipos de SOC dominan muchas herramientas de seguridad y deben tener experiencia práctica en clasificación de incidentes, investigación forense y respuesta a incidentes de seguridad reales. Muchos SOC utilizan un enfoque jerárquico para tratar los problemas de seguridad: los ingenieros y analistas se asignan a un nivel jerárquico según su experiencia y habilidades. Una estructura de equipo clásica es la siguiente:

Nivel 1: Analista de Seguridad
Los analistas de seguridad son generalmente las primeras personas en responder a un incidente. Son los combatientes de primera línea que protegen contra los ataques cibernéticos e investigan las amenazas. Su función es identificar amenazas, analizarlas y responder rápidamente. Además, es posible que los analistas deban implementar medidas de seguridad según lo especificado por la gerencia. También podrían contribuir a los planes de recuperación ante desastres de la organización. En muchos SOC, los analistas de seguridad deben responder a los incidentes que ocurren fuera del horario comercial.

Nivel 2: Analista de seguridad sénior
Los analistas sénior se activan cuando los analistas de nivel 1 descubren amenazas graves o incidentes de seguridad a gran escala. Los analistas senior investigan los sistemas afectados, revisan los informes de inteligencia e identifican el tipo de ataque. Crean planes para reparar los activos dañados, proteger otros activos y trabajar para erradicar la amenaza.

Nivel 3: Gerente de Seguridad
Los administradores de seguridad son analistas de seguridad expertos de alto nivel que buscan

activamente vulnerabilidades dentro de la red de la organización. Utilizan herramientas avanzadas de detección de amenazas para encontrar y evaluar debilidades y desarrollar recomendaciones para mejorar la postura general de seguridad. Este grupo incluye especialistas como auditores de cumplimiento e investigadores forenses.

Nivel 4: Director de seguridad de la información (CISO)

Los CISO definen y supervisan las operaciones de seguridad de la organización. Son la autoridad en políticas, procedimientos y estrategias en todas las áreas de las operaciones de seguridad cibernética de la organización. En algunas organizaciones también gestionan el cumplimiento, pero en otras hay equipos independientes centrados en esta tarea.

Generalmente, un CISO se comunica directamente con el CEO y tiene una línea directa de contacto con la alta dirección. Los puestos de CISO requieren más que habilidades técnicas o de seguridad: la comunicación es una parte clave del rol, porque los CISO deben comunicar problemas complejos a la alta dirección y a las partes interesadas, que pueden no estar versados en asuntos técnicos.

Ingenieros de seguridad

Los ingenieros de seguridad son responsables de construir los sistemas y la arquitectura de seguridad: mantienen las herramientas de seguridad y recomiendan el uso de nuevas herramientas. Por lo general, tienen un conocimiento profundo de las plataformas SIEM. También documentan procedimientos, requisitos y protocolos para garantizar que otros usuarios tengan los recursos necesarios.

Gerente de Respuesta a Incidentes

En una organización grande, el SOC podría emplear un Director de Respuesta a Incidentes dedicado. Este rol es responsable de comunicar el impacto de incidentes graves a toda la organización, coordinando y priorizando acciones durante la identificación, análisis y contención de un evento.

6 desafíos clave del SOC y cómo superarlos

Brecha de talento

Desafío: hay una gran escasez de profesionales de ciberseguridad y, por lo tanto, muchas vacantes de trabajo en ciberseguridad. En todo el mundo, hay millones de puestos de seguridad cibernética que no se pueden cubrir debido a la falta de talento. Dada esta escasez, a la gerencia del SOC le resulta difícil contratar personal y enfrenta el riesgo de agotamiento y desgaste de los miembros existentes del equipo.

Solución: un SOC debe buscar talento desde adentro y considerar capacitar a los empleados para llenar los vacíos dentro del equipo SOC. Además, cada rol crítico de SOC debe tener un respaldo: una persona que tenga las habilidades necesarias para mantener las cosas en funcionamiento si el puesto queda vacante inesperadamente.

Atacantes sofisticados

Desafío: la defensa de la red es un elemento central de la estrategia de ciberseguridad de una organización. Requiere atención, ya que los ciberdelincuentes sofisticados tienen el conjunto de habilidades y las herramientas para eludir las defensas convencionales, incluida la seguridad de punto final y los firewalls.

Solución: implemente herramientas con capacidades de aprendizaje automático o detección de anomalías, que pueden descubrir amenazas sofisticadas, lo que reduce la necesidad de investigación humana

.

Grandes datos

Desafío: el volumen de datos y tráfico de red con el que trata

una organización típica es tremendo. Con un crecimiento tan enorme en los datos de registro, surge un desafío cada vez mayor para analizar todos estos datos en tiempo real.

Solución: los SOC utilizan herramientas automatizadas para analizar, filtrar, correlacionar y agregar información para permitir un análisis conveniente y centralizado.

Alerta de fatiga

Desafío: en muchos sistemas de seguridad, hay muchas anomalías y una gran cantidad de alertas de seguridad. Si el SOC se basa en alertas sin filtrar, estas alertas pueden volverse abrumadoras rápidamente. Muchas alertas son falsos positivos o no contienen suficiente contexto para investigar el incidente. Estos tipos de alertas de baja calidad desvían a los equipos de incidentes de seguridad reales.

Solución: un SOC debe tener una estrategia sólida para la priorización de alertas. Es fundamental mejorar la calidad de las alertas y diferenciar entre alertas de baja y alta importancia. Utilice herramientas de análisis de comportamiento para garantizar que los equipos de SOC atiendan primero los problemas más graves.

Amenazas desconocidas

Desafío: la detección tradicional basada en firmas, los firewalls y la detección de puntos finales no pueden descubrir una amenaza desconocida. A los SOC les resulta difícil detectar y defenderse de las amenazas de día cero.

Solución: los equipos de SOC pueden mejorar sus reglas, firmas y soluciones de detección de amenazas basadas en umbrales mediante el uso de análisis de comportamiento para descubrir comportamientos inusuales.

Sobrecarga de la herramienta de seguridad

Desafío: muchas organizaciones adquieren varias herramientas de seguridad para identificar todas las posibles amenazas. Estas herramientas tienden a estar desconectadas entre sí, tienen un alcance restringido y no pueden identificar amenazas sofisticadas que atraviesan los silos de seguridad.

Solución: implemente tecnología como Detección y respuesta extendidas (XDR), que combina datos de todas las capas del entorno de TI para identificar amenazas sofisticadas o evasivas.

Los cinco tipos de modelos de centros de operaciones de seguridad (SOC)

Aquí te explicamos la diferencia entre estos modelos. Sopesamos los modelos en términos de costo, sus ventajas y desventajas, brindamos pautas que lo ayudarán a tomar la mejor decisión y sugerimos alternativas para las organizaciones que necesitan opciones más asequibles.

SOC virtuales

¿Qué es un SOC Virtual?

Un SOC virtual (VSOC) no reside en una instalación dedicada ni tiene una infraestructura dedicada. Es un portal basado en la web creado con tecnologías de seguridad descentralizadas, que permite a los equipos fuera del sitio monitorear eventos y responder a las amenazas.
¿Cuáles son los beneficios de un SOC virtual?
Le ahorra los costos significativos de hardware en las instalaciones y otra infraestructura, y puede confiar en que los equipos virtuales se activen cuando haya un incidente.

Desventajas de un SOC virtual

Un VSOC es principalmente un enfoque reactivo. Es mucho más probable que las tecnologías y los procesos descentralizados dejen brechas de seguridad, lo que hace que la detección y la respuesta ante amenazas sean menos eficientes. Y debido a que el VSOC generalmente opera con personal a tiempo parcial distribuido geográficamente, no podrá contar con un equipo dedicado a la seguridad las 24 horas del día, los 7 días de la semana.

Aproximaciones alternativas

El VSOC se puede mejorar a través de la automatización, la tecnología SIEM y el análisis. Algunas organizaciones también optan por subcontratar su VSOC. Si bien esto aumenta las capacidades de seguridad y el acceso a recursos expertos, también disminuye la visibilidad interna en todo el entorno y puede generar tiempos de respuesta más prolongados cuando un evento se intensifica.

SOC/NOC multifunción

¿Qué es un SOC/NOC multifunción?

Una combinación de un SOC con un centro de operaciones de red (NOC), este modelo tiene un equipo, una instalación y una infraestructura dedicados. Un SOC/NOC multifunción va más allá de las funciones de seguridad para incluir operaciones de TI, cumplimiento y gestión de riesgos.

¿Cuáles son los beneficios de un SOC/NOC?

La principal ventaja de este modelo es la reducción de costos, ya que consolida el personal y minimiza el desembolso de capital. Es más adecuado para organizaciones más pequeñas con exposiciones de bajo riesgo y aquellas que ya tienen responsabilidades de seguridad superpuestas en diferentes equipos.

Desventajas de un SOC/NOC

El SOC/NOC multifunción incluye menos énfasis en la seguridad. Si bien el equipo multifuncional realiza tareas de seguridad centrales, dividir la atención entre diferentes necesidades de TI, redes y seguridad inevitablemente da como resultado defensas de seguridad más débiles.

Además, un equipo multifuncional debe tener conjuntos de habilidades más amplios para abordar una amplia variedad de problemas. Esto significa que no es probable que tengan una gran experiencia en seguridad. Esa es una gran desventaja, porque la defensa contra las amenazas sofisticadas y en evolución de la actualidad requiere un conocimiento avanzado y actualizado de las mejores prácticas de seguridad.

SOC cogestionado

¿Qué es un SOC cogestionado? En un SOC cogestionado, las soluciones de monitoreo en el sitio aumentan, mientras que algunas responsabilidades pueden transferirse al personal externo.

Las razones clave para elegir este modelo son las limitaciones de recursos y los límites presupuestarios. Las ventajas y desventajas son la pérdida de control y la falta de personalización de servicios y responsabilidades. Debe encontrar el equilibrio adecuado entre el control que mantiene internamente y el que subcontrata al proveedor, ya que la eficacia de este modelo depende de esas dos opciones.

¿Cuáles son los beneficios de un SOC coadministrado?

Un SOC coadministrado ofrece más flexibilidad porque puede implementar alguna tecnología, como herramientas de administración de eventos e información de seguridad (SIEM) en las instalaciones o en la nube. También puede decidir qué tamaño de equipo interno se adapta mejor a sus necesidades. Cuando se maneja bien, este modelo ofrece grandes beneficios y puede dar buenos resultados.

Desventajas de un SOC cogestionado

Un SOC coadministrado típico es entregado por proveedores de servicios de seguridad administrados (MSSP) cuya experiencia principal no es TI ni operaciones de seguridad. Este modelo suele

ser más caro porque es posible que tenga que invertir en hardware adicional y también tiene mayores gastos generales.

SOC dedicado

¿Qué es un SOC dedicado?

Un SOC dedicado es un SOC centralizado con una infraestructura, un equipo y procesos dedicados centrados completamente en la seguridad. El tamaño de un SOC dedicado varía según el tamaño, los riesgos y las necesidades de seguridad de la organización.

Por lo general, un SOC dedicado tiene al menos de cinco a ocho expertos en seguridad internos en varios niveles para el monitoreo y las operaciones las 24 horas del día, los 7 días de la semana. Un SOC dedicado es esencial para las empresas globales que tienen datos privados en varios lugares y deben cumplir con las regulaciones y políticas de seguridad.

¿Cuáles son los beneficios de un SOC dedicado?

Un SOC dedicado proporciona propiedad total sobre la tecnología y los procesos. El equipo interno también tiene la mejor capacidad para monitorear su entorno y tendrá la mejor visibilidad para obtener una imagen completa de su panorama de amenazas y seguridad.

Desventajas de un SOC dedicado

Este modelo requiere una gran inversión inicial, lo que significa que no se ajusta al presupuesto de muchas organizaciones. Es más adecuado para grandes empresas y agencias gubernamentales con una amplia infraestructura de TI que está constantemente bajo ataque, ya que estas organizaciones suelen tener los recursos para construirla y mantenerla.

Comando SOC

¿Qué es un SOC de comando?

Un SOC de comando tiene varios SOC distribuidos en varias ubicaciones, a menudo a nivel mundial. Las organizaciones que utilizan este modelo incluyen empresas Global 2000, grandes proveedores de telecomunicaciones y agencias de defensa. El comando SOC generalmente controla otros SOC y también realiza análisis forense y otros procesos de recuperación.

¿Cuáles son los beneficios de un Command SOC?

El comando SOC está gestionado por un gran equipo de expertos en seguridad y un equipo de investigación de seguridad con capacidades de búsqueda de amenazas.

¿Cuáles son las desventajas?

Este modelo se centra más en la gestión de la inteligencia de amenazas y el conocimiento de la situación que en las operaciones de seguridad del día a día.

¿Cuál es el mejor SOC para su organización?

Un SOC se puede implementar como parte de una estrategia integral para proteger a las organizaciones grandes y pequeñas contra amenazas avanzadas. Pero no existe una solución única que brinde el equilibrio perfecto entre costo y efectividad.

Para algunas empresas, los presupuestos de seguridad limitados y la falta de experiencia interna crean barreras para implementar un programa que sea efectivo y brinde suficiente protección. Para resolver este problema, las organizaciones deben considerar seleccionar el SOC de un proveedor de operaciones de seguridad administrada.

La seguridad administrada es un

modelo subcontratado que amplía las capacidades de su equipo de seguridad o TI interno. Incluye una solución de detección y respuesta administrada (MDR), que elimina la carga de determinar la mejor metodología o tecnología para la detección y respuesta de amenazas.

Un modelo de operaciones de seguridad administradas aumenta las herramientas de seguridad de red actuales con monitoreo, detección y respuesta continuos a las amenazas. También puede incluir otras soluciones de operaciones de seguridad que ayuden a evaluar y eliminar vulnerabilidades y reducir el riesgo cibernético

.

¿Qué desafíos enfrentan los centros de operaciones de seguridad en la actualidad?

Los SOC tienen muchas responsabilidades, y el equipo de SOC puede verse abrumado fácilmente si estos problemas no se gestionan adecuadamente. Algunos de los desafíos que enfrentan los SOC en la actualidad incluyen:
Gestión de grandes datos. Los SOC tienen la tarea de recopilar y manejar una gran cantidad de datos (Kelley, 2022). Estos datos masivos pueden ser un desafío para los equipos de SOC, a quienes les puede resultar abrumador monitorear y analizar.

Seguir el ritmo de las nuevas tecnologías. La ciberseguridad está en constante evolución y parte de la responsabilidad de un SOC es mantenerse al día con los últimos cambios en tecnologías y técnicas de ataque para mantenerse a la vanguardia.

Encontrar personal calificado. Los SOC requieren un equipo de analistas capacitados que puedan identificar y mitigar las amenazas de seguridad. Dada la escasez de talento en ciberseguridad, esto puede ser difícil de encontrar en el mercado actual (Li, 2021).
La creciente complejidad de los entornos de datos. La cantidad de dispositivos que una organización tiene en su red aumenta la complejidad del entorno. A medida que una organización escala, se vuelve más desafiante para los analistas de SOC rastrear y responder a las amenazas de seguridad.

El creciente número de ciberataques. La frecuencia de los ciberataques aumenta día a día, lo que dificulta que los SOC se mantengan al día.

Con información de Cynet, EC-Council, y Artic Wolf

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


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