SOLUCIONES SEGURAS
CYBERSECURITY
MAGAZINE

Edición No. 15

REVISTA REGIONAL DE CIBERSEGURIDAD

DESARROLLANDO INMUNIDAD

ANTE LA CIBERPANDEMIA, EL GRAN RETO DEL 2022

EN ESTA EDICIÓN:

2021
VOLUMEN 4

SOLUCIONES SEGURAS
SOLUCIONES SEGURAS TRAINING CENTER
SOLUCIONES SEGURAS CYBERSECURITY REGIONAL TOUR
SOLUCIONES SEGURAS CYBERSECURITY MAGAZINE

SOLUCIONES SEGURAS CYBERSECURITY MAGAZINE

CONTENIDO

Randol Chen
Soluciones Seguras
Editor de la Revista SS CSM

SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

PALABRAS DE EDICIÓN

¡Ya pronto llega el nuevo año 2022!

El año 2021 no fue un año fácil, definitivamente. Después de la migración al teletrabajo apurado en el 2020, el regreso híbrido a la oficina trae a veces más preguntas que respuestas: cuando regresar, cómo regresar, qué balance es apropiado, y lo más importante, cómo tener la misma seguridad en premisas y afuera de las premisas.

Ya estamos viendo lo que es la nueva normalidad (perdón, última vez que uso el término): reuniones virtuales y presenciales, oficinas espaciadas, eventos con responsabilidad, y poder regresar a vernos en persona (aunque sea a los ojos). La pandemia todavía estará con nosotros, veremos las olas subir y bajar, pero aprendemos a vivir con ella. Lo que importa es como nos adaptamos y como seguimos adelante.

Perdón por ser egoísta, pero en lo personal mi highlight del año fue el evento que pudimos hacer con algunos de nuestros socios para celebrar los 20 años de Soluciones Seguras. No solamente por llegar a esa meta, sino por haber compartido unas horas muy amenas y alegres con personas que no habíamos visto en casi dos años. Habernos acompañado significó mucho para todos nosotros. Y a los que no pudimos ver en persona, estoy seguro que pronto podremos vernos ya sea en Panamá, Costa Rica, Guatemala o El Salvador.

Espero que todos estemos igual de ansiosos por comenzar el 2022. Todos en Soluciones Seguras les deseamos un año nuevo próspero, lleno de éxitos, felicidades, y por supuesto mucha salud.

¡Felicidades!

Gracias!
Eli Faskha
CEO

TENDENCIAS PARA EL 2022
QUE DEBE CONTEMPLAR EN SU ESTRATEGIA DE CIBERSEGURIDAD

Con el 2022 a la vuelta de la esquina y la reactivación económica que vemos globalmente luego de los progresos de la vacunación e inmunidad colectiva respecto al COVID-19, vemos también un aumento considerable en los ataques dirigidos a las empresas de todos los tamaños, por lo que desarrollar una inmunidad ante la ciberpandemia será el gran reto del 2022 para las organizaciones globalmente. Así como los atacantes cambian y perfeccionan sus armas constantemente, fabricantes líderes en ciberseguridad realizan nuevos desarrollos en ciberseguridad que pueden impactar positivamente la postura de seguridad de su negocio. Lamentablemente la implementación de estas soluciones no se realiza a la misma velocidad que se desarrollan, lo que les ha permitido a los atacantes estar un pie adelante para la mayoría de las organizaciones. Para apoyar la aceleración de estas implementaciones, algunos países tienen o han iniciado la implementación de regulaciones en torno a la ciberseguridad de datos.

REGULACIONES

En la medida que los gobiernos refuercen el control sobre la ciberseguridad a través de las regulaciones, las empresas tendrán que adaptarse para estar en cumplimiento. Algunos países de la región, como es el caso de Panamá, han empezado a establecer sus primeras normas y regulaciones entorno al manejo, control y seguridad de los datos confidenciales. Estas regulaciones son muy importantes, tomando como ejemplo que algunos países han iniciado las regulaciones de las criptomonedas, lo cual aumentará la visibilidad en las transacciones dificultándole a los malos actores la utilización de estas como medio de cobro en los ataques de extorción digital (Ransomware).

TENDENCIAS PARA EL 2022
QUE DEBE CONTEMPLAR EN SU ESTRATÉGIA DE CIBERSEGURIDAD

Para defenderse de estos ataques, y desarrollar Inmunidad ante la Ciberpandemia, debe mantenerse al tanto de las tendencias en ciberseguridad y aplicarlas a su negocio en la medida que le sea posible.

Estas son algunas de las tecnologías que serán las tendencias de ciberseguridad más importantes para el 2022:

- **Concientización del usuario**: es importante recordar que la seguridad es un asunto de todos, por lo que las herramientas que permitan automatizar el proceso de capacitación al personal respecto a las ciber amenazas será una tendencia en el 2022.

- **Inteligencia Artificial**: en la medida que los ataques se vuelven cada vez más complejos, las soluciones líderes del mercado en ciberseguridad irán incorporando cada vez más esta tecnología dentro de sus soluciones para hacerlas más eficientes, inteligentes y rápidas en la detección y mitigación de ciberataques.

- **Seguridad del trabajador remoto**: debido al aún vigente estado de pandemia, en muchos países aún será común el teletrabajo y con esto, estas personas se convierten en un blanco preferido por los cibercriminales. Asegurarlos seguirá siendo una prioridad para el 2022.

- **Seguridad IoT**: la tecnología no se detiene, ni siquiera con un estado de pandemia. Cada vez tenemos más dispositivos inteligentes conectados a la red, no solo en las organizaciones sino en los hogares, protegerse de amenazas dentro de estos dispositivos será una prioridad en el 2022.

- **Seguridad de Nube**: con la transformación digital acelerada que ha generado el COVID-19 muchas organizaciones están migrando a la nube, sino es que ya han migrado. Con esto, el núcleo empresarial está dejando de ser en las premisas y pasando a la nube, por lo que asegurar la nube nunca había sido tan importante.

SOLUCIONES SEGURAS

CELEBRA 20 AÑOS DE EMPRESAS PROTEGIDAS Y TRANQUILAS

Soluciones Seguras, compañía líder en ciberseguridad en Centroamérica, ha celebrado sus 20 años de trayectoria en un cóctel que congregó a más de un centenar de invitados.

El evento, realizado en el marco de la celebración del Día Internacional de la Seguridad de la Información, contó con la participación de sus clientes, socios de negocios, aliados tecnológicos y colaboradores de la compañía.

En el encuentro, Eli Faskha CEO de Soluciones Seguras dio un repaso sobre la evolución de Soluciones Seguras desde su origen en Panamá hasta situarse como líder en ciberseguridad en la región, y cómo ha evolucionado la ciberseguridad a lo largo de estas dos décadas.

Hoy hemos logrado ser líderes en la industria porque comprendemos las necesidades de ciberseguridad de la región

BATIENDO RÉCORDS, AUMENTO DEL 178% EN EL NÚMERO DE SITIOS WEB MALICIOSOS DE COMPRAS ELECTRÓNICAS

Check Point SOFTWARE TECHNOLOGIES LTD.

Recurso: Check Point Blog, Noviembre, 2021
https://blog.checkpoint.com/2021/11/12/number-of-malicious-shopping-websites-jumps-178-ahead-of-november-e-shopping-holidays-breaking-records/

Destacados

- Check Point Research (CPR) detecta más de 5300 sitios web maliciosos diferentes por semana, marcando el más alto desde principios de 2021.
- Las cifras muestran un aumento del 178% en lo que va del 2021.
- 1 de cada 38 redes corporativas se ven afectadas en promedio por semana en noviembre. en comparación con 1 de cada 47 en octubre y 1 de cada 352 a principios de 2021

Background

La temporada navideña presenta un gran espectáculo de compras, especialmente para aquellos de nosotros que amamos las compras en línea. En Asia Pacífico, el Click Frenzy de Australia acaba de pasar el 9 de noviembre, el Día del Soltero de China acaba de pasar el 11 de noviembre y, finalmente, tenemos Black Friday y Cyber Monday en los Estados Unidos.

La pandemia ha provocado un cambio evidente en los hábitos y las compras no son diferentes, y la mayoría de las personas se han pasado a las compras en línea, lo que ha provocado un auge en el comercio minorista electrónico.

Los minoristas están encantados de aprovechar esta tendencia y la oportunidad que ofrecen los días especiales de compras. Sin embargo, en medio del rumor y la emoción, los actores de amenazas también aprovechan los eventos para sus propios propósitos maliciosos.

Fuerte aumento de nuevos sitios web maliciosos relacionados con compras

Desde principios de octubre de 2021, los investigadores de CPR presenciaron la mayor cantidad de sitios web maliciosos relacionados con ofertas de compra y venta. En promedio, se detectaron más de 5300 sitios web diferentes por semana, lo que representa un aumento del 178%, en comparación con el promedio en 2021, hasta el momento.

Cómo tener una experiencia de compra libre de amenazas

Aquí están nuestras recomendaciones y consejos para asegurar su experiencia de compra en línea este noviembre:

- Compre siempre de una fuente auténtica y confiable. No haga clic en los enlaces promocionales que reciba por correo electrónico o redes sociales.
- Esté atento a los dominios. Debe notar la precisión ortográfica en los correos electrónicos o sitios web, y tener en cuenta los remitentes de correo electrónico desconocidos.
- Demasiado buenas para ser ciertas, probablemente no lo son. Desafortunadamente, un iPad nuevo NO tendrá un descuento del 80% esta temporada.
- Busque siempre el candado. Realizar una transacción en línea desde un sitio web que no tiene el cifrado de capa de conexión segura (SSL) instalado es absolutamente NO-GO. Para saber si el sitio tiene SSL, busque la “S” en HTTPS, en lugar de HTTP. Aparecerá un icono de un candado cerrado, normalmente a la izquierda de la URL en la barra de direcciones o en la barra de estado de abajo. Ningún candado es una gran señal de alerta.
- Esté siempre atento a los correos electrónicos de restablecimiento de contraseña, especialmente cuando los volúmenes de tráfico en línea están en su punto máximo, Al enviar un correo electrónico de restablecimiento de contraseña falso que lo dirige a un sitio de phishing similar, pueden convencerlo de que ingrese las credenciales de su cuenta y se las envíe.

Las estadísticas y los datos utilizados en este informe presentan datos detectados por las tecnologías de prevención de amenazas de Check Point, almacenados y analizados en ThreatCloud. La inteligencia se enriquece con motores basados en inteligencia artificial y datos de investigación exclusivos de Check Point Research. Conozca más en www.checkpoint.com.

En 2021 la ciberdelincuencia ha pasado a convertirse en una preocupación principal en las empresas; ya que representa un alto costo asociado con la pérdida de información y la recuperación del curso del negocio.

Guatemala, 17 de septiembre de 2021.- Ángel Salazar, Gerente General de Soluciones Seguras Guatemala, participó este viernes en el Foro "Independientemente segurxs", organizado por el Instituto Nacional de Ciberseguridad INCIBE. En este impartió la charla "¿Cómo proteger a las empresas en épocas inciertas?".

Junto a otros expertos, se presentó una luz en la problemática relacionada al cibercrimen, cómo estar atentos y evitar riesgos tecnológicos, financieros, físicos o incluso de reputación de la empresa.

En la actualidad los ciberataques continúan en ascenso como una de las actividades más rentables; solo en Guatemala han aumentado con un promedio de 2,052 ataques por semana en los últimos seis meses. Los riesgos de malware son cada vez más especializado y contra un mayor número de víctimas, las cuales están desprotegidas. Estos incrementos son debido a que hay más usuarios que antes y con menos defensas.

"Los ataques han crecido exponencialmente. Podemos comparar a Guatemala con el resto del mundo en una situación muy similar a la del Covid-19, en donde tenemos el ingreso de nuevas variantes pero bajo porcentaje de personas vacunadas. Eso mismo sucede en el ambiente digital, las mismas amenazas que en primer mundo, pero las empresas guatemaltecas cuentan con menos infraestructura, leyes y educación digital." asegura Ángel Salazar, gerente general de Soluciones Seguras Guatemala.

El impacto en una pequeña empresa puede ser fatal, cerca de un 60% que sufre un ataque corre riesgo de cerrar definitivamente. En otra posición, algunas empresas más robustas tienen una inversión considerable en ciberseguridad permitiéndole hacer frente a ataques más eficientemente.

Es vital que las empresas validen el estado de sus sistemas, cuente con estrategias que puedan actualizarse con eficiencia para no quedar obsoletas ante la rapidez con que mutan los ataques de los cibercriminales. "La clave es que las organizaciones mantengan un monitoreo de los componentes de ciberseguridad y estar alerta para dar respuesta ante cualquier posible evento, a esto le llamamos Ciber Resilicencia." , explicó Salazar.

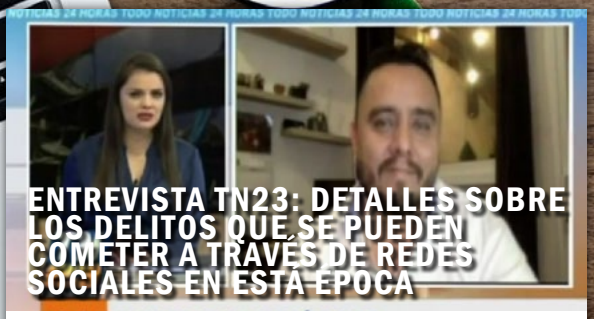
Para construir un sistema de respuesta rápida y de protección, las empresas pueden tomar varias acciones que les permita responder de una manera efectiva:

- Identifique y ubique los activos, información sensible o sistemas más importantes; mantenga siempre un backup de los sistemas e información.
- Proteja sus activos; asegure e implemente soluciones de seguridad, de defensa automatizada. Entre estas acciones se pueden utilizar contraseñas robustas y de doble factor de autenticación, cifrar la información sensible de cliente o data de negocio, crear políticas de ciber-seguridad e implementar softwares de protección.
- Detecte situaciones extrañas. Siempre de la mano de la protección preventiva, se debe tener un factor de monitoreo o vigilancia. Acompañando esto utilice software original, lo que permitirá identificar con mayor facilidad posibles fallos o deficiencias.
- Responda ante posibles amenazas. Prepárese y documente las acciones a tomar en una posible falla de seguridad y que le permita restaurar los sistemas críticos lo más rápido posible.

SOLUCIONES SEGURAS EN LAS NOTICIAS

DÍA INTERNACIONAL DE LA SEGURIDAD INFORMÁTICA

tvn Noticias



ENTREVISTA TN23: DETALLES SOBRE LOS DELITOS QUE SE PUEDEN COMETER A TRAVÉS DE REDES SOCIALES EN ESTA ÉPOCA

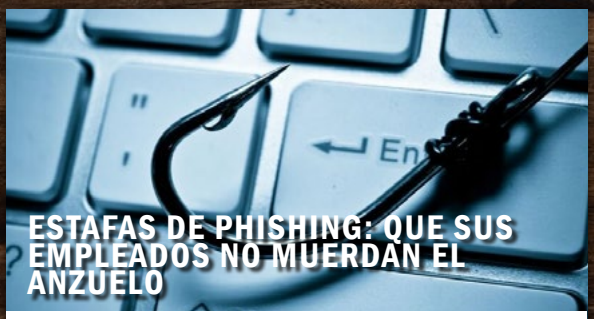
TN23

¿SABES QUÉ HACER SI SUFRES UN ATAQUE DE RANSOMWARE?

Forbes CENTROAMÉRICA

NUEVE TENDENCIAS Y RETOS DE LA CIBERSEGURIDAD QUE MARCARÁN 2022

MARTES FINANCIERO
LA REVISTA FINANCIERA DE PANAMÁ



ESTAFAS DE PHISHING: QUE SUS EMPLEADOS NO MUERDAN EL ANZUELO

TyN MAGAZINE

EL PHISHING, UN VECTOR DE ATAQUE POPULAR PARA LOS CIBERDELINCUENTES

Entre COMILLAS MAGAZINE

SOLUCIONES SEGURAS

Empresas Protegidas, Empresas Tranquilas

DESARROLLAR INMUNIDAD ANTE LA CIBER PANDEMIA SERÁ EL GRAN RETO DEL 2022

MERCADOS & TENDENCIAS

EN GUATEMALA EN PROMEDIO SE COMETEN CADA SEMANA 2,219 ATAQUES CIBERNÉTICOS

CON CRITERIO

MÓVILES Y CIBERATAQUES

METRO LIBRE
LA VERDAD DE LA NOTICIA

¿CÓMO FUNCIONAN LAS ESTAFAS DE PHISHING?

E&N

POR CORREO ELECTRÓNICO SE DAN LOS PRINCIPALES ATAQUES CIBERNÉTICOS EN ÉPOCA DE PANDEMIA

El Observador

NEXPANAMA: ENTREVISTA DE CIBERSEGURIDAD

Nex

PHISHING & RANSOMWARE, LAS AMENAZAS MÁS LATENTES DEL CIBERCRIMEN

El Phishing y el Ransomware son dos de las amenazas más comunes dirigidas a las organizaciones todos los días y pueden generar desafíos importantes.

Según una encuesta realizada en una investigación patrocinada por Trend Micro, ambos son una de las principales preocupaciones de los encuestados.

Issues of High Concern to Security Teams
Percentage Responding "Concerned" or "Extremely Concerned"

Security Issue	%
Phishing attempts making their way to end users	65%
Employees failing to spot phishing and social engineering attacks before clicking on a link or attachment	64%
Breaching of corporate data by a ransomware attack	61%
Ransomware attacks successfully infecting endpoints	59%

Veamos primero de qué se trata el Phishing y Ransomware y por qué son las amenazas más comunes utilizadas en ataques cibernéticos.

Para realizar un ataque de forma satisfactoria necesito suplantar una identidad de una empresa, para ello debo robar primero la identidad y luego con este acceso plantar el ataque. De hecho, una descripción de Wikipedia sobre Suplantación de Identidad describe ambos muy bien: "El phishing es un tipo de ingeniería social en el que un atacante envía un mensaje fraudulento (p. Ej., Falsificado, falso o engañoso) diseñado para engañar a una víctima humana para que revele información confidencial al atacante o para implementar software malicioso en la infraestructura de la víctima, como ransomware."

En la primera etapa se debe engañar al usuario, generalmente con ingeniería social, para ganar la identidad o el acceso, esto se conoce como Phishing. El phishing puede llegar de muchas formas, hoy día la más común es por correo electrónico, pero puede darse también por mensajes SMS, Whatsapp o similares, o inclusive llamadas telefónicas. Una vez la víctima cae, se puede tener control de alguna de sus identidades, estas pueden ser cuentas de banco, accesos a empresas, entre otros.

A nivel organizacional, los ataques de ransomware modernos ahora siguen un modelo en el que el atacante se infiltra en la red de la víctima utilizando un método como el phishing, luego los actores se trasladarán lateralmente a sus sistemas comerciales críticos para implementar el Ransomware. De hecho, el Ransomware suele ser el último ataque a la red, ya que es muy visible. Antes de ejecutar el Ransomware, es posible que hayan exfiltrado datos en un esfuerzo de doble extorsión. Entonces, en muchos casos, estas dos amenazas son parte de una sola campaña contra una organización y deben verse como tales.

Algo preocupante en los resultados de la encuesta fue que el 37% de las organizaciones creían que eran altamente efectivas para contrarrestar 11 o más de las amenazas de phishing y Ransomware. Esto significa que casi dos tercios de estas organizaciones sintieron que no eran muy efectivas para contrarrestar estas dos amenazas. Parte del desafío es qué tan bien se educa a los empleados sobre estas amenazas. Según la encuesta, menos de la mitad (45%) estaban bastante o completamente seguros de que todos los empleados podían reconocer una amenaza de phishing basada en correo electrónico. Esto fue aún peor para reconocer intentos de malware o ransomware (39%).

Para protegerse contra ataques de phishing:

- Habilite la autenticación multifactor en todas las cuentas que le sea posible.
- Habilite Inteligencia Artificial / Machine Learning dentro de sus soluciones de seguridad de correo electrónico, especialmente si está utilizando Office365
- Eduque a sus empleados sobre el phishing y ayúdelos a reconocer correos electrónicos sospechosos.

Para prevenir ataques de ransomware:

- Habilite la autenticación de múltiples factores para sus cuentas administrativas
- Parche sus aplicaciones y sistemas operativos, y utilice parches virtuales para ayudar
- Utilice soluciones EDR / XDR que pueden ayudar a identificar las actividades de alerta temprana que conducen a un ataque de ransomware
- Implementar una estrategia de respaldo
- Desarrollar y ejecutar un programa de formación de conciencia de seguridad en toda la empresa

ATAQUES DDOS DIRIGIDOS A SERVICIOS DE PAGO DE INSTITUCIONES FINANCIERAS GLOBALES

radware Recurso: Radware Blog, Diciembre 4, 2021
https://blog.radware.com/security/alert/2021/12/ddos-attacks-targeting-payment-services-of-global-financial-institutions/

Un actor o grupo de amenazas está apuntando activamente a los servicios en línea de las sucursales de instituciones financieras globales. Los servicios de protección contra DDoS de Radware Cloud impidieron que múltiples ataques interrumpieran la banca web en línea, los servicios de validación de pagos y los servicios de acceso remoto de sucursales de instituciones financieras en varios países de todo el mundo. Durante dos semanas, Radware observó una mayor sofisticación y mejoras para evadir la detección y mitigación a medida que avanzaban los ataques. Si bien las instituciones financieras objetivo tienen su sede en Europa, Radware fue testigo de ataques a sucursales en otros continentes.

De noviembre a enero es la temporada de compras mundial. No es raro ver un aumento en la actividad de los ataques dirigidos al comercio electrónico, los sistemas financieros y de pago, un período en el que la interrupción de los servicios de pago o de los servicios de banca móvil y web no pasará desapercibida.

Los piratas informáticos expertos que demuestran sus capacidades para la venta generalmente se anuncian en foros de piratería y, por lo que pudimos verificar, los ataques no han sido denunciados. Dicho esto, los ataques no tuvieron éxito en lo que respecta a nuestros clientes, por lo que no hay mucho que reclamar a menos que hayan tenido éxito con otras víctimas de las que aún no tenemos conocimiento.

No es la técnica, más bien considere el objetivo

Cuando los ataques de nivel récord aparecen en los titulares, la gente tiende a perder de vista el objetivo y simplemente considera la táctica. Los ataques DDoS volumétricos que superan los 2Tbps reciben mucha atención, pero estos ataques se mitigaron con éxito y la defensa contra ellos depende principalmente de la capacidad de uno para consumir grandes cantidades de tráfico. Ninguno de los que informaron sobre ataques masivos interrumpieron los servicios o causaron agravios prolongados a sus víctimas.

Recientemente, varias campañas de ataques fueron noticia debido a que afectaron los servicios durante períodos más prolongados, y sus víctimas creyeron que los ataques disminuyeron solo para tomarlos desprevenidos un par de horas / días después. Estos ataques impactantes no se acercaron a los niveles de terabit por segundo y no requirieron millones de solicitudes por segundo para degradar o interrumpir los servicios de sus víctimas.

Golpeando donde duele

Cuando ocurren interrupciones o un servicio sufre un ataque prolongado, los clientes están (o al menos deberían estar) informados y, a medida que se resuelve el problema, la gente recupera la confianza en el servicio. Si las fallas ocurren al azar, las interrupciones temporales se siguen repitiendo; los clientes comenzarán a desconfiar y cuestionar el servicio.

La pandemia hizo que la sociedad fuera más consciente de la higiene y parece haber afectado las preferencias de las personas por el pago con tarjeta. El volumen de efectivo utilizado en el Reino Unido se redujo hasta en un 60% en 2020. En los EE. UU., El 28% de las personas dejaron de usar efectivo por completo. Las compras en línea representaron el 28% de las ventas en el Reino Unido en 2020. La banca móvil, los pagos en línea y los servicios de validación de tarjetas de crédito o débito se han convertido en una mercancía. Los consumidores están adaptando los pagos digitales a tasas récord, sin darse cuenta de la compleja infraestructura detrás de esos pagos de rutina. Hasta que un pago falla porque un servicio está fuera de línea. Empezamos a sudar frío los próximos pagos, esperando que el servicio esté disponible esta vez. De noviembre a enero son posiblemente los meses que más dependen del desempeño de los servicios de pago en línea.

Al comparar las técnicas aprovechadas en las últimas dos semanas durante múltiples ataques que creemos que están relacionados con los mismos actores o grupos de amenazas, observamos un aumento gradual en la sofisticación y el refinamiento a medida que avanzaban las campañas y los ataques se mitigaban con éxito. Los ataques se distribuyeron aleatoriamente entre países, ramas y organizaciones, pero las técnicas parecieron transformarse en sintonía.

Su estrategia de defensa debe enfocarse en los activos y servicios expuestos

La protección de una red contra los ataques DDoS volumétricos de nivel de saturación requiere soluciones de protección en la nube que tengan la capacidad suficiente para consumir incluso los ataques más grandes conocidos y limpiar el tráfico antes de que vuelva a enrutarse a la red protegida. Las soluciones de protección de capa de red sin estado son adecuadas para proteger los dispositivos de red y los servidores contra ataques de escasez de recursos en las instalaciones.

Al exponer aplicaciones en línea con las que interactúan los usuarios, tanto la red como la capa de aplicación deben protegerse. Tal solución debería poder hacer la distinción entre humanos y máquinas (bots) y entre bots buenos y malos. La protección de las API en línea o las aplicaciones móviles de una sola página es diferente de la protección de las aplicaciones web. Los consumidores de API son en su mayoría dispositivos o máquinas, por lo que distinguir entre humanos y máquinas no es relevante y se requerirán mecanismos de detección más avanzados.

Cada semana, más de 1200 organizaciones en todo el mundo son víctimas de un ataque de Ransomware o «secuestro de datos» y todas las empresas, sin excepciones están en riesgo. Según Cybersecurity Ventures, el daño causado por el Ransomware alcanzará aproximadamente US$20 mil millones este año.

En 2021 los ataques de Ransomware se han convertido en la principal amenaza y cuestan millones de dólares al año a las empresas reponerse de estos ataques.

Por su parte, Check Point, partner de Soluciones Seguras, reveló recientemente que los ciberataques a empresas crecieron un 29% en todo el mundo, destacando un dramático aumento global del 93% en el número de ataques de ransomware en los últimos 6 meses, impulsados por la técnica de ataque Triple Extorsión.

"Este es el tipo de ataque que es más fácil de detectar, porque las empresas reciben un mensaje solicitando un pago para volver a tener acceso a la información personal o de la empresa. Hemos visto casos en los que, a pesar de realizar el pago, la información sigue circulando, por lo que el impacto del mismo es mucho más sensible", dice Ángel Salazar, gerente general de Soluciones Seguras Guatemala.

El Ransomware empieza con tácticas sencillas, la más común es un ataque de phishing en donde envían un correo electrónico a los usuarios de la empresa para hacer clic en el mismo. Con esta acción se le entrega acceso a los cibercriminales a los archivos y sistemas de la empresa. Una vez dentro de los sistemas, el criminal puede moverse y colocar un "secuestro" de datos y a menudo amenazando con la destrucción permanente de datos a menos que se pague un rescate.

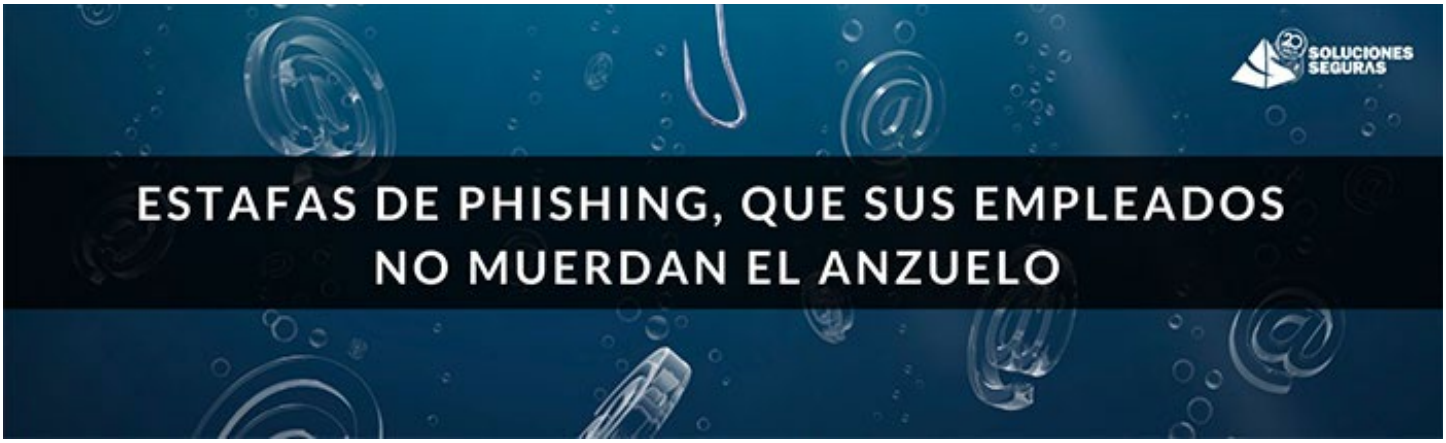
Más allá de simplemente pagar el rescate, las empresas pueden tomar varias acciones que les permita responder de una manera efectiva:

- Desconectar los sistemas infectados del resto de la red para evitar daños mayores. De manera simultánea se puede identificar la fuente de la infección. Dado que los piratas informáticos pueden haber estado en el sistema durante mucho tiempo, encontrar la fuente puede requerir de asesoría externa por parte de expertos.

- Una de las fases del ataque suele ser un intento de localizar y cifrar o eliminar copias de seguridad, por lo tanto es recomendable realizar copias de seguridad con datos cifrados.

- No realizar actualizaciones o mantenimiento de los sistemas si está siendo atacado. Eliminar archivos temporales o realizar otros cambios podría complicar las investigaciones y la solución.

- Una vez que descubra que ha sido infectado, es importante determinar en qué falló el proceso, ya sea un error humano o tecnológico. Esto impedirá que un suceso de este tipo se vuelva a repetir.



En el contexto de la crisis sanitaria los dispositivos móviles cambiaron las reglas de juego para muchas organizaciones, y los cibercriminales son absolutamente conscientes que el uso de los mismos en un entorno de trabajo híbrido son el punto débil de las empresas y uno de los blancos perfectos para introducirse a una red corporativa.

De acuerdo a los investigadores de Check Point, partner de Soluciones Seguras en su Informe de Seguridad Móvil 2021, al menos el 40% de los dispositivos móviles a nivel mundial son inherentemente vulnerables a los ciberataques.

El phishing o la suplantación de identidad es un vector de ataque popular para los ciberdelincuentes porque son simples y efectivos, ya que es la forma más sencilla de atacar a un usuario en internet. En el entorno empresarial, un clic falso de un empleado podría derribar la red y sistemas de toda la empresa.

La motivación del atacante "phisher" es puramente financiera. Sus "anzuelos" utilizados son: el correo electrónico, los mensajes de texto también conocido como smishing, las llamadas telefónicas o mensajes de voz (vishing) y las aplicaciones móviles.

Los atacantes envían por correo electrónico con sentido de urgencia incitando al usuario a "morder el anzuelo", haciendo clic en un enlace a un sitio web fraudulento para instalar software malicioso (malware) en el dispositivo o robar información, o abrir un archivo para instalarle en el mismo un código malicioso. También emplean las llamadas telefónicas o mensajes de voz o texto falsos de fuentes falsas con el objetivo de robar información confidencial de la compañía.

A través de la gran cantidad de aplicaciones instaladas en los dispositivos móviles, los ciberdelincuentes también utilizan las redes sociales y aplicaciones falsas para engañar a sus víctimas.

Educando a los usuarios

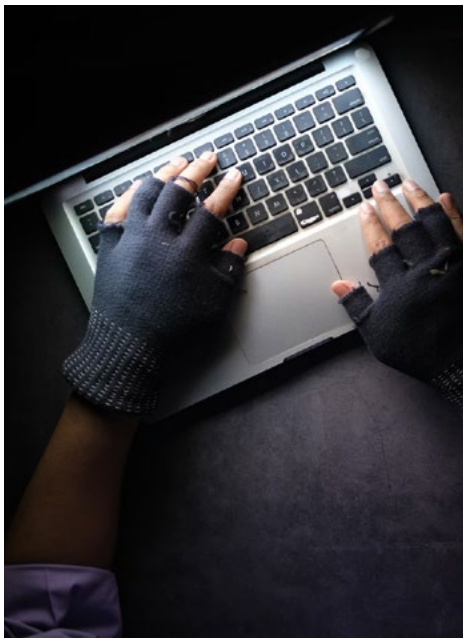
La capacitación para la concientización de los empleados de las organizaciones es fundamental para que estos comprendan los riesgos, identifiquen señales de suplantación de identidad y reportar episodios sospechosos a las áreas de tecnología de su empresa.

A continuación, los expertos de Soluciones Seguras brindan una serie de recomendaciones para reducir el riesgo de ataques de phishing:

- Prestar especial atención a los correos electrónicos de restablecimiento de contraseña no solicitados. Si recibe uno de estos, visite siempre el sitio web directamente sin hacer clic en los enlaces adjuntos.

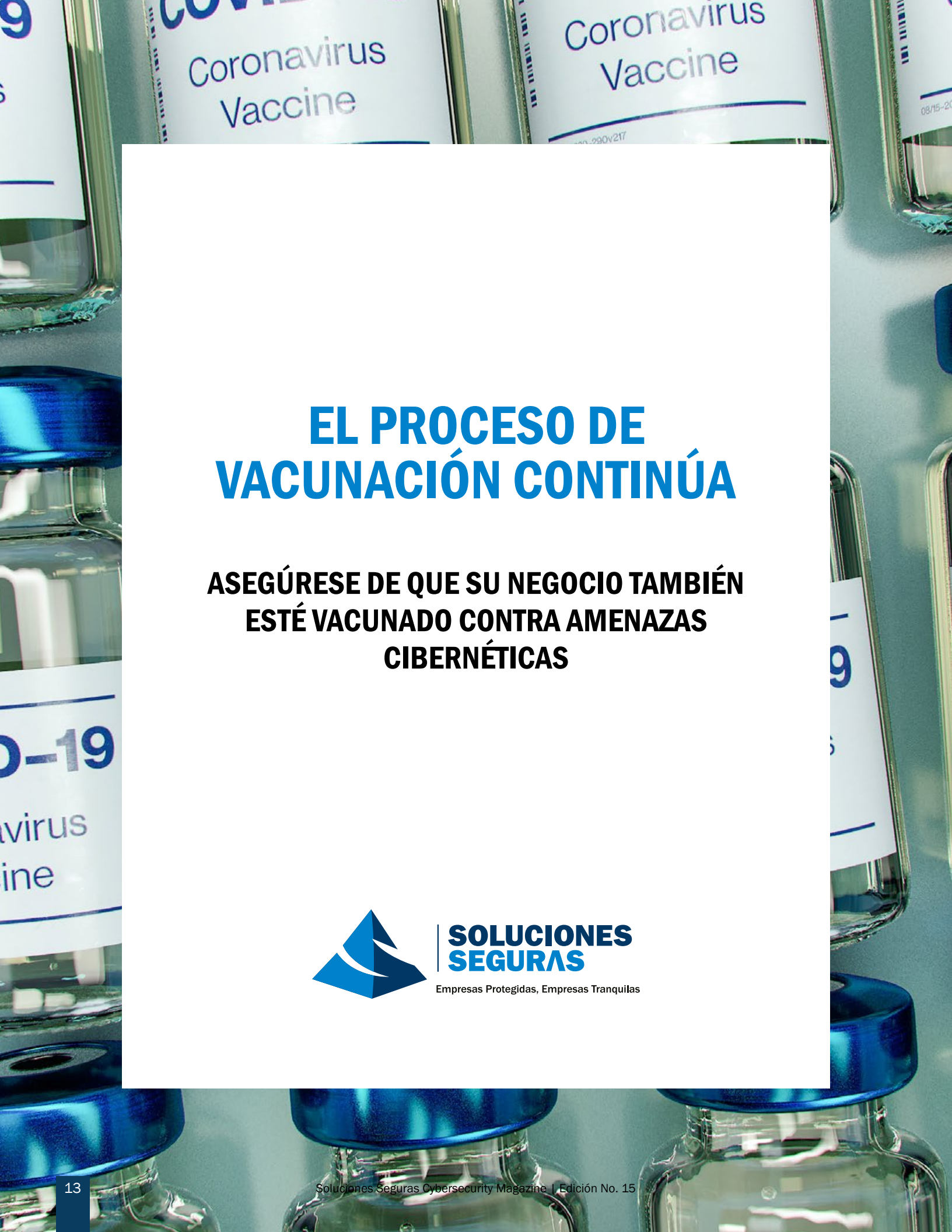
- Nunca comparta sus credenciales. Los ciberdelincuentes utilizan diferentes estafas para intentar robar las contraseñas de sus cuentas tanto personales como empresariales.

- Sitios web falsos: Analizar en detalle los sitios donde ingresan. Al navegar por sitios que requieren de la utilización de credenciales, validar siempre que se encuentre en el sitio con certificado digital seguro y confiable indicado con un candado al lado de la URL y que la misma comience con https (certificado de seguridad) y no http.



- No proporcionar información personal como datos bancarios, tarjetas de crédito, contraseñas u otra información confidencial. Las empresas serias nunca solicitan este tipo de información a través de correos o mensajes de voz y texto.

- No abrir o descargar archivos adjuntos que provengan de usuarios que no conoce o usuarios no solicitados.



EL PROCESO DE VACUNACIÓN CONTINÚA

ASEGÚRESE DE QUE SU NEGOCIO TAMBIÉN ESTÉ VACUNADO CONTRA AMENAZAS CIBERNÉTICAS

SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

CURSOS VIRTUALES 2022

CCSA

Check Point SOFTWARE TECHNOLOGIES LTD.

Check Point Certified

SECURITY ADMINISTRATOR

Conceptos y habilidades necesarias para gestionar las operaciones diarias de ciberseguridad utilizando la tecnología de Check Point

CCSE

Check Point SOFTWARE TECHNOLOGIES LTD.

Check Point Certified

SECURITY EXPERT

Habilidades avanzadas para proteger y mantener eficazmente la seguridad de las redes de su empresa

> **CURSOS VIRTUALES DISPONIBLES**
> **Contáctenos para obtener más información**

CCVS

Check Point SOFTWARE TECHNOLOGIES LTD.

Check Point Certified

VSX SPECIALIST

Habilidades importantes para implementar seguridad de red virtual

CCCS

Check Point SOFTWARE TECHNOLOGIES LTD.

Check Point Certified

CLOUD SPECIALIST

Gestione las soluciones de Check Point CloudGuard IaaS dentro de su entorno de seguridad en la nube

CCES

Check Point SOFTWARE TECHNOLOGIES LTD.

Check Point Certified

ENDPOINT SPECIALIST

Implemente y administre la tecnología de seguridad de Endpoint dentro de su entorno de red

> **CURSOS VIRTUALES DISPONIBLES**
> **Contáctenos para obtener más información**

Consúltenos para obtener más información:

entrenamiento@solucionesseguras.com

www.solucionesseguras.com

SOLUCIONES SEGURAS TRAINING CENTER

Check Point PARTNER ELITE

Check Point
SOFTWARE TECHNOLOGIES LTD.

PROTECCIÓN DE REDES, ENDPOINTS Y MOVILES

Check Point ofrece la más reciente protección de seguridad de redes en una plataforma integrada. Con protección para su centro de datos, empresa, móviles, estaciones de trabajo y oficina en el hogar, Check Point tiene una solución para usted.

Infoblox
CONTROL YOUR NETWORK

SEGURIDAD Y SERVICIOS DNS, DHCP & IPAM

Consolide los servicios DNS, DHCP & IPAM en una sola plataforma, administrada centralmente. Para DNS externos elimine la interrupción del servicio DNS mediante una defensa automatizada contra ataques volumétricos basados en DNS y exploits.

imperva

PROTECCIÓN DE BASE DE DATOS Y APLICACIONES WEB

Soluciones de auditoría y protección a datos críticos mediante protección de Bases de Datos, además de protección para aplicativos web (WAF). Brindando una protección completa lo más cerca de la fuente de información.

radware

MITIGACIÓN DE ATAQUES | ENTREGA DE APLICACIONES

Soluciones para seguridad, disponibilidad, balanceo y rendimiento de infraestructura y aplicaciones web. Sistema Mitigador de Ataques para protección perimetral y alta disponibilidad en sus aplicaciones web manteniéndolas seguras y optimizadas.

CYBERARK

SEGURIDAD DE CUENTAS PRIVILEGIADAS

CyberArk es líder y experto en seguridad de cuentas privilegiadas. Gestión de privilegios, análisis de amenazas privilegiadas y registro de sesiones. Las contraseñas privilegiadas se mantienen en una bóveda segura.

ForeScout
Access ability.

VISIBILIDAD Y CONTROL DE ACCESO A LA RED

Solución de seguridad heterogénea que puede ver dispositivos, controlarlos y organizar respuestas de amenazas en instalaciones cableadas e inalámbricas, centros de datos, campus, nube y tecnología operativa sin agentes.

TREND MICRO

IPS Y PROTECCIÓN AVANZADA PARA REDES Y SERVIDORES

Soluciones que frecen alta tecnología en prevención de intrusiones para proteger contra toda la gama de amenazas en cualquier lugar de su red y servidores en ambientes físicos, virtuales y en la nube.

Barracuda

FILTRADO DE CONTENIDO Y ARCHIVADO DE DATOS

Barracuda le birnda una única fuente para proteger todos sus vectores de amenazas, incluidos el correo electrónico, sitios web, aplicaciones web, y el rendimiento de la red, ya sea en el sitio o en la nube.

Progress

MONITOREO DE RENDIMIENTO DE REDES Y SERVIDORES

El monitoreo de su infraestructura completa desde una solución centralizada todo-en-uno. Es de rápida implementación brindando alertas proactivas y vistas instantáneas, permitiendo resolver incidencias de red lo más rápido posible.

indeni

ANÁLISIS DE EVENTOS DE DISPOSITIVOS DE SEGURIDAD

Plataforma con integración profunda a dispositivos críticos, con automatización pre-cargada e instrucciones de remediación fácil de leer que proveen herramientas valiosas al equipo.

DARKTRACE

SISTEMA INMUNE DE LAS EMPRESAS

Detección de amenazas en tiempo real, visualización de la red y capacidades avanzadas de investigación en un solo sistema unificado.

RAPID7

SIEM BASADO EN LA NUBE | ANÁLISIS DE VULNERABILIDADES

Solución SIEM basado en la nube con User Behavior Analytics y Deception Technology (HOneypot). Además de solución para análisis de vulnerabilidades.

LA ATENCIÓN QUE USTED NECESITA

El Soporte de Soluciones Seguras con Atención de Emergencias 24x7 le da protección completa y el servicio que usted espera de un líder en ciberseguridad de redes.

RECONOCIDOS POR LA INDUSTRIA

Hemos recibido múltiples reconocimientos por los fabricantes y mayoristas líderes que representa.

EMPRESAS PROTEGIDAS, EMPRESAS TRANQUILAS

20 AÑOS SOLUCIONES SEGURAS

Empresas Protegidas, Empresas Tranquilas

Check Point PARTNER ELITE

ACERCA DE SOLUCIONES SEGURAS

Con 20 años de experiencia en la gestión de seguridad de redes, aplicaciones y telecomunicaciones, Soluciones Seguras es la compañía líder en ciberseguridad en Centroamérica. Nuestra reputación se ha creado en base al excelente servicio que ofrecemos, el total conocimiento de las líneas que manejamos, y los productos líderes que representamos.

PERSONAL EXPERTO Y CERTIFICADO

Somos un equipo de profesionales del más alto nivel, certificados por los fabricantes más reconocidos de la industria de seguridad.

CENTRO REGIONAL DE ENTRENAMIENTO AUTORIZADO

Centro Regional de Entrenamiento Autorizado Check Point número uno en la región, con profesionales expertos que forman parte del equipo de desarrollo del contenido de los entrenamientos.

SOLUCIONES SEGURAS TRAINING CENTER

LÍDER EN CIBERSEGURIDAD EN CENTROAMÉRICA

PRESENCIA REGIONAL

SOLUCIONES SEGURAS EN PANAMÁ

Edificio 237, 2do piso
Ciudad del Saber, Panamá
Tel: +507 317-1312
Fax: +507 317-1320
info@sseguras.com

SOLUCIONES SEGURAS EN COSTA RICA

Edificio Atrium piso 3.
Escazú, San José, Costa Rica
Tel: +506-4000 0885
Fax: +506-4001 5822
infocr@sseguras.com

SOLUCIONES SEGURAS EN GUATEMALA

Edificio Zona Pradera
Torre IV, Nivel 6, Oficina 608
Boulevard Los Próceres 24-69.
Tel: +502 2261-7101
infogt@sseguras.com

SOLUCIONES SEGURAS EN EL SALVADOR

Edificio Vittoria, 5to Nivel,
Calle El Mirador 4814
San Salvador, El Salvador
Tel: +503 2206-6929
infosv@sseguras.com

Alianzas

SOLUCIONES SEGURAS

Empresas Protegidas, Empresas Tranquilas

Panamá | Costa Rica | Guatemala | El Salvador

www.solucionesseguras.com

Soluciones Seguras

SOLUCIONES SEGURAS
CYBERSECURITY
MAGAZINE