SOLUCIONES SEGURAS
CYBERSECURITY
MAGAZINE

Edición No. 18

REVISTA REGIONAL DE CIBERSEGURIDAD

RANSOMWARE AS A SERVICE,
¿MODA O AMENAZA PERSISTENTE?

EN ESTA EDICIÓN:

GRANDES ATAQUES RANSOMWARE DEL 2022

CÓMO REDUCIR EL RIESGO DE SER VÍCTIMA DE RANSOMWARE

PROYECTO NO-MORE-RANSOM

Y MÁS...

2022
VOLUMEN 3

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

Hola a todos otra vez. Es un gusto para nosotros llegar a sus oficinas y hogares con esta edición de nuestro Cyber Security Magazine.

Hace ya muchos años, por el 2009 o quizás un poco antes, comenzaron las opciones de usar una nube computacional para ofrecer servicios que eran muy difíciles, costosos, o lentos de ofrecer con las estructuras en premisas existentes. Inicialmente se desplegaron Servidores Web en data center públicos, y después aparecieron algunas aplicaciones en la nube, como Salesforce o ServiceNow y otros CRMs que eran difíciles de instalar en premisas. Siguieron algunos servicios como GMail y Office365, donde se mueven los servidores de correo a la nube. Un tiempo después aparece la Infraestructura como Servicio y Plataforma como Servicio, principalmente ofertada por Microsoft Azure, Google AWS, entre otros.

De forma similar, los atacantes también vieron una oportunidad en migrar a nubes computacionales. Mercados negros en la Dark Web comenzaron a ofrecer servicios de Denegación de Servicio como una suscripción, y después el Ransomware como plataforma de ataque por servicio creció muchísimo. Hoy en día es fácil encontrar una plataforma que en cuestión de minutos les envíe a sus víctimas ataques de ransomware exitosos. Ya no es solamente a las grandes empresas, es a todo tipo y tamaño de organización que puede estar vulnerable a estos ataques.

¿Qué hacer? Los mismos consejos que hemos dado siguen siendo válidos: primero hay que concientizar a los usuarios, que son la primera línea de defensa. Después hay que tener buenas copias de respaldo para cualquier situación, y siempre hay que implementar herramientas que permitan prevenir los ataques y reaccionar proactivamente a ellos. Enfocarse en la detección no funciona: si detectaste el ataque es porque ya entró y comenzó a hacer daño. Hay que enfocarse en la prevención como el modelo de ciberseguridad que necesitan las empresas.

Gracias otra vez por compartir con nosotros esta revista, y esperamos mucho que sea de todo su agrado.

¡Suerte!

Eli Faskha
CEO

RAMSOMWARE AS A SERVICE
¿MODA O AMENAZA PERSISTENTE?

Como hemos visto en los últimos meses, los ataques de ransomware son cada vez más frecuentes, al punto donde casi no se escucha de otros tipos de ataques. ¿Qué está sucediendo? ¿Será Ransomware una moda pasajera o los atacantes han descubierto algo más? Primero, comencemos respondiendo la pregunta muy básica: ¿Qué es el Ransomware? Ransomware es un tipo de malware que cifra los archivos y carpetas de la víctima para luego cobrar un rescate a fin de liberar dichos archivos. Los últimos meses se ha visto un aumento masivo en los ataques de ransomware en todo el mundo y muchos de estos son impulsados por el aumento de una nueva modalidad tener acceso a estas herramientas, hablamos de Ransomware-as-a-Service (RaaS).

Ransomware as a Service

Los ataques exitosos de ransomware pueden generar enormes ganancias para los atacantes y usar RaaS puede ser económico y relativamente fácil. Si bien es fácil para un delincuente ejecutar ransomware, desarrollar el malware requiere conocimientos y habilidades técnicas. Ransomware-as-a-Service es la respuesta a este problema. Desarrolladores crean ransomware y lo venden para un uso generalizado.

Ransomware-As-A-Service es un modelo de negocio en el que los delincuentes desarrollan el malware para que lo usen los delincuentes. La gran diferencia es que, en este caso, el producto/servicio que se vende es una herramienta utilizada para actividades delictivas y para desencadenar ataques de ransomware.

¿Qué hace que RaaS sea tan peligroso?

Antes se requería de 3 cualidades para lanzar un ransomware (deseo, conocimiento y objetivo), y es que el más difícil de tener (conocimiento) ha sido facilitado por RaaS, por lo que hoy día prácticamente solo basta con tener el deseo y un objetivo, RaaS se encarga del resto.

Los delincuentes que buscan opciones de RaaS pueden obtener ofertas especiales y elegir entre diferentes modelos de suscripción, que es lo que hace que este servicio sea tan peligroso. Las ofertas de RaaS en la DarkWeb se parecen mucho a las ofertas de marketing tradicionales para servicios de software.

Entre algunos de las formas de adquirir el servicio de suscripciones RaaS se logran encontrar:

- Acceso ilimitado pagando una tarifa única.
- Suscripciones mensuales
- Participación de ganancias: el desarrollador obtiene una parte de cada ataque exitoso y rescate ganado.

Algunos modelos pueden incluir una combinación de tipos de pago, por ejemplo, la participación en las ganancias se puede combinar con una regalía o una tarifa mensual.

El ransomware es altamente personalizable, gracias a los avances tecnológicos, API y servicios Cloud; los compradores a menudo cuentan con interfaces elegantes donde pueden personalizar su malware. Muchos proveedores de RaaS permitirán que incluso un delincuente novato acceda a su conjunto de herramientas, mientras que muchos otros son muy selectivos con respecto a los afiliados con los que trabajan.

Ejemplos de Ransomware-as-a-Service

Existen muchos tipos de RaaS en la DarkWeb. Los “operadores” están constantemente desarrollando software nuevo y mejor. Estos son algunos ejemplos de ransomware que se propaga a través del modelo RaaS:

Ryuk: Ryuk ransomware es una de las variantes de ransomware más prolíficas y costosas que existen. Las estimaciones dicen que Ryuk es responsable de aproximadamente un tercio de las infecciones de ransomware en el último año. El ransomware también es efectivo para convencer a los objetivos de que paguen sus demandas de rescate y ha hecho un estimado de $ 150 millones hasta la fecha.

Lockbit: Lockbit existe desde septiembre de 2019, pero solo recientemente ingresó al espacio RaaS. Se enfoca en cifrar rápidamente los sistemas de grandes organizaciones, minimizando la oportunidad detectar y eliminar el malware antes de que se produzca el daño.

REvil/Sodinokibi: REvil compite con Ryuk como la variante de ransomware más codiciosa. Este malware se propaga de varias maneras, y se sabe que los afiliados de REvil explotan Citrix y Pulse Secure VPN sin parches para infectar sistemas.

Egregor/Maze: La variante del ransomware Maze hizo historia como la primera en introducir la “doble extorsión”, que consiste en robar datos como parte de un ataque de ransomware y amenazar con publicar la información si no se paga un rescate adicional. Las variantes de ransomware, como Egregor, todavía están operativas y se ejecutan bajo el modelo de afiliado RaaS.

¿Pagar o no pagar?

Si el ataque de ransomware tiene éxito, la organización se enfrenta a la opción de pagar el rescate o no. De cualquier manera, las empresas deben volver al principio y averiguar por qué ocurrió el incidente. Ya sea que hayan fallado factores humanos o tecnología, vuelva a pasar por todos los procesos y reconsidere toda la estrategia para asegurarse de que nunca vuelva a ocurrir un incidente similar. Dar este paso es necesario independientemente de si una organización paga el rescate o no. Nunca se consuele con el hecho de que de alguna manera se ha recuperado los datos y considerar el incidente resuelto.

Entonces, ¿pagar o no pagar? La respuesta no es tan simple como parece a primera vista. Si bien las cantidades de rescate a veces son de cientos de miles o millones de dólares, las interrupciones de los sistemas críticos a menudo superan estas cantidades. Sin embargo, las empresas deben recordar que incluso si se paga el rescate, no significa que los datos, o incluso parte de ellos, se descifrarán. Incluso hay casos conocidos en los que los atacantes tienen errores en los códigos para que la organización no pueda recuperar los datos aún si quisiera.

No se apresure a tomar una decisión y considere todas sus opciones cuidadosamente. Apóyese de expertos en ciberseguridad primero. Pagar el rescate realmente debería ser el último recurso.

¿Moda o amenaza persistente?

Ransomware-as-a-Service definitivamente es una modalidad de ataque novedosa y extremadamente peligrosa de la cual debemos cuidarnos mucho. Podría decir que en este momento es un poco de ambos, es una moda de alta rentabilidad que lo convierte en una amenaza persistente que estaremos viendo por mucho tiempo todavía.

K-12 SCHOOLS IN THE CROSSHAIRS OF RANSOMWARE

Recurso: Cyberark Blog, Septiembre, 2022
https://www.cyberark.com/resources/blog/k-12-schools-in-the-crosshairs-of-ransomware

If staggering staffing shortages, razor-thin budgets, safety issues and politically driven controversies weren't enough to contend with, U.S. schools are facing another major crisis: skyrocketing ransomware attacks.

You've likely read news stories about educational institutions under attack in recent weeks. This timing is no coincidence: A new school year spells new opportunity for attackers. Just last week, the U.S. Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC) issued a joint cybersecurity advisory (CSA) warning that threat actors are "disproportionately targeting the education sector with ransomware attacks," especially kindergarten through twelfth grade (K-12) institutions.

These attacks have resulted in "restricted access to networks and data, delayed exams, canceled school days and unauthorized access to and theft of personal information regarding students and staff," CSA authors note.

Why K-12 schools? CyberArk's Matt Kenslea – whose years of public sector work give him insight into many of today's top education challenges – says it all comes back to opportunity. "Many attackers go after weakness and many of these schools are understaffed, underfunded and highly vulnerable. The attackers are many, their tools are varied and often-overworked staff can struggle to keep up."

"School districts, especially those in large, urban environments have to do so much: Feed students, bus students, teach students, provide individualized support for students – many of whom speak different languages – and keep students safe. With so many competing priorities, hiring and keeping specialized cybersecurity staff is a massive challenge," says Kenslea. "Many school districts don't – or can't – make investments in cybersecurity until after an attack."

According to the CSA, K-12 institutions are also attractive targets given "the amount of sensitive student data accessible through school systems or their managed service providers." Last year, an NBC News investigation found that ransomware groups had published sensitive personal data on American schoolchildren from more than 1,200 schools.

Frank W. Abagnale, a world-renowned identity fraud expert, has described why cyber criminals prefer to steal the identities of younger people in this way: "I'll take the student every time. Because a child has no credit, and the child is not likely to seek credit for many years. So I can steal the identity of a two-year-old, I can be that two-year-old for a long period of time before anyone ever finds out I've stolen that two-year-old's identity. That's why on the black market a two-year-old's identity sells for a lot more than a 14-year-old's, simply because you have a lot longer to sell it."

New-School Ransomware Attacks Target Faculty and Staff Endpoints as an Entry Point

With the benefit of ransomware-as-a-service platforms, it's easy for just about anyone with internet access to launch an attack on a school. In fact, 56% of K-12 schools worldwide report being hit by ransomware in the last year.

"By and large, ransomware attackers are getting in from local endpoints, such network-connected PCs, Macs and laptops used by staff and faculty members," Kenslea explains. Even if anti-virus is installed on the machine, attackers can often slip past it, since these tools rely primarily on known threats and behavior patterns and frequently miss targeted and novel threats (remember, ransomware is constantly changing).

Oftentimes, these endpoint devices have active accounts with local admin rights, which enable device users to perform tasks such as running system or software updates, controlling files and using hardware. The trouble is, those admin rights are exactly what many ransomware attackers need to move further into an environment, deploy malware, encrypt files and hold them for ransom. In almost every instance, attackers look for ways to penetrate, linger and lurk on a system, waiting for opportunities to move laterally and then escalate privileges by compromising accounts with local admin rights.

Even if they aren't meant to have local admin rights, users sometimes wind up with them anyway. "Scrambling to fill vacant positions, schools are issuing new staff members laptops and getting them into classrooms in a hurry. People make mistakes, especially when they're rushing," says Kenslea. Even when schools are on top of managing their Active Directory, they often overlook access control lists (ACL) and those legacy privileges can be exploited.

The obvious solution would be to just take local admin rights away, right? Not so fast, Kenslea warns. "Education is an open, collaborative environment, teachers share with students, parents and colleagues across the country and the world. Removing local admin rights on all endpoints will create friction and pushback – like when the superintendent can't even install a printer or read a textbook file. And as they say, 'You don't want that smoke.'"

"It can't be an all or nothing thing," he continues. "It's about finding a better balance between permission control and giving very overworked people the access they need to do their jobs."

"Hardening the endpoint – where ransomware attacks so often begin – is the best place to start," he continues. To do this, he urges schools to follow the CSA's guidance of immediately addressing known vulnerabilities, implementing multifactor authentication (MFA) for high-impact actions if it's not already enforced and getting serious about cybersecurity training to help faculty identify phishing and other credential theft attempts.

CIBERDELINCUENCIA ARMADA: LO QUE LAS ORGANIZACIONES PUEDEN APRENDER DEL CONFLICTO EN UCRANIA

Recurso: Check Point Blog, Septiembre, 2022
https://blog.checkpoint.com/2022/09/08/weaponized-cybercrime-what-organizations-can-learn-from-the-conflict-in-ukraine/

On February 24th, 2022, Russia launched a full-scale military invasion of Ukraine with attacks on land, sea, air. What has been less visible but nonetheless a critical element of the conflict is the battle being waged in cyberspace. Just like the military conflict with its wider consequences in terms of disruption to trade and the tragedy of the refugee crisis, the war in cyberspace has an impact beyond the borders of Ukraine and Russia. While no one can predict how long this war will last, we can say for certain that the cyber aspects of the conflict in Ukraine will continue to resonate long after the guns have been silenced, as highlighted in Check Point's Mid-Year Security Report 2022.

So, what does the conflict teach us about cyberwarfare and how can organizations prepare themselves for this new world order?

A new era of cyberwarfare

One thing we can take away from what's happening in Ukraine is that cyberwarfare has become an established component of global conflict both in the propaganda battle as well as in the actual conduct of military operations. From Distributed Denial of Service (DDoS) attacks and website defacements to destructive critical infrastructure attacks, activity on both sides has escalated dramatically since the initial invasion in February.

Just three days into the conflict in late February, Check Point Research (CPR) noted a 196% increase in cyberattacks on Ukraine's government and military sector. And these attacks have shown no signs of slowing down in the months since. New figures from CPR reports that between February and August of this year, cyberattacks on Ukraine's government and military sector more than doubled, increasing by a staggering 112%, while Russia's same sector decreased by 8%. While Russia has not completely disconnected from the internet as per previous reports, government and military networks and websites have implemented different measures to limit access to their resources from outside of Russia, which make the execution of some of the attacks more difficult. Indeed, Ukraine has been under constant attack – throughout the conflict, corporate networks have experienced over 1,500 cyberattacks a week on average. This is 25% higher than before the conflict, versus 1,434 weekly cyberattacks on Russia corporate networks.

CPR also reported that the most attacked industry during the conflict in Ukraine was the finance sector, with an average of 1,841 cyberattacks per organization every week, a decrease of 29% compared to the period before the conflict, followed by the government and military sector, with an average of 1,406 weekly attacks per organization, which also saw the highest increase in weekly cyberattacks with a 112% increase compared to before the conflict, which could be due to increased attacks inflicted on them by factions siding with Russia. Manufacturing was the third heavily attacked sector, with over 400 attacks per organization every week (64% decrease). Like Russia, the finance sector also saw major attacks, probably as an outcome of the various government and individual financial aid received, as well as cybercriminals who were looking to cash in on known donations being sent to Ukraine for the war and refugee efforts. It was not surprising to see the manufacturing sector also being heavily attacked as this is one of their key critical industries for any country to be sustained, with its global wheat exports contributing heavily to Ukraine's economy. Such disruptions would now not only impact inflows of funds into Ukraine, but negatively impact their exports.

But continued vigilance is just one of the factors at play here. The other notable impact has come from the army of volunteers who have flocked to support Ukraine, and whose involvement might change the face of cybersecurity as we know it.

Opening the floodgates for future cyberattacks

When the Russia-Ukraine war does come to an end, it is likely that the cybersecurity space will find itself in a far worse situation than it is today. Whether it's through the anonymous recruitment of Ukraine's IT army or the cybercriminals in Russia to whom this conflict has given an opportunity to hone their craft.

After the conflict, whatever the outcome, these APT groups, hacktivists and individuals are not just going to disappear. Instead, they will turn their newfound expertise and tooling toward fresh targets unleashing a tsunami of cyberattacks across the globe. We have already started to see early warning signs of this with attacks on NATO partners, as well as on those countries who have come to Ukraine's aid, increasing in both frequency and intensity.

This conflict has seen cyber activity change the face of warfare forever. But it has also had the 'collateral damage' effect of raising the threat level for cyber-attacks on government and commercial organizations globally. While we were already in an era of sophisticated fifth-generation cyberattacks, threat actors have raised their game during the war and we know that even more integrated and sophisticated cyberattacks are coming down the line.

Organizations need to ready themselves now. Mitigating attacks won't be enough, companies must adopt a prevent-first cybersecurity strategy.

GRANDES ATAQUES RANSOMWARE DEL 2022

Los ataques de ransomware continúan en aumento mes a mes, año a año, y 2022 no ha sido la excepción. Ya habíamos mencionado en ediciones anteriores la existencia de la Ciberpandemia, el constante incremento de incidencias ransomware son prueba de ello. Les mostraremos a continuación 5 casos particulares de ataques de ransomware, sin ningún orden o filtro en particular. Estos ejemplos que traemos buscan evidenciar que los ataques pueden sucederle a cualquiera, y crear diversos tipos de afectaciones a nivel de la organización, gobierno o sociedad.
Analizar estos ejemplos nos ayudará a observar más de cerca las estrategias e intenciones, lo que nos llevará a ser más conscientes del fenómeno de los ataques de ransomware y con suerte estar mejor preparados ante una incidencia:

1. NVIDIA

La compañía de chips de semiconductores líder a nivel mundial se vio comprometida por un ataque de ransomware en febrero de 2022. La compañía confirmó que el actor de amenazas había comenzado a filtrar las credenciales de los empleados e información de propiedad en línea.

El grupo de ransomware, Lapsus$, asumió la responsabilidad del ataque y afirmó que tenían acceso a 1 TB de datos de la empresa exfiltrados que filtrarían en línea. También exigió $ 1 millón y un porcentaje de una tarifa no especificada de Nvidia.

Nvidia respondió rápidamente al ataque de ransomware fortaleciendo su seguridad e involucrando a expertos en respuesta a incidentes cibernéticos de inmediato para contener la situación.

2. Gobierno de Costa Rica

Este ha sido probablemente el ataque del que más se ha hablado en 2022, ya que es la primera vez que un país declara una emergencia nacional en respuesta a un ataque cibernético. El primer ataque de ransomware en la nación comenzó a principios de abril, lo que afectó no solo a los servicios gubernamentales, sino también al sector privado dedicado a la importación/exportación.

El grupo de ransomware Conti asumió la responsabilidad del primer ataque, le pidió al gobierno que pagara el rescate de $10 millones y luego lo aumentó a $20 millones.

El 31 de mayo, otro ataque sumió en el caos al sistema de salud del país. Este ataque, vinculado a HIVE, afectó a la caja costarricense del seguro social. Este ataque afectó directamente al pueblo costarricense, ya que desconectó los sistemas de salud del país.
Si bien los trasfondos políticos y las implicaciones de este ataque son muchos y la cronología de la forma en que se desarrolló el ataque puede llenar páginas, la idea de presentar este ataque en esta lista es mostrar los resultados profundos y dañinos que un ataque de ransomware puede tener en las organizaciones gubernamentales.

Naciones enteras pueden quedar paralizadas si no se han invertido los recursos adecuados en la preparación para ataques de ransomware, soluciones de protección y capacitación en seguridad cibernética para empleados, miembros del personal, etc. para responder a tales ataques.

GRANDES ATAQUES RANSOMWARE DEL 2022

CONTINUACIÓN

3. Condado de Bernalillo, Nuevo México

Este fue uno de los primeros grandes ataques en 2022. El 5 de enero, el condado más grande de Nuevo México descubrió que se había convertido en víctima de un ataque de ransomware paralizante, que desconectó varios departamentos del condado y oficinas gubernamentales. Los funcionarios del condado, sin embargo, dijeron que no pagaron rescate a los piratas informáticos.

Además de la grave angustia de los ciudadanos que acompaña a cualquier departamento gubernamental que se desconecte, este ataque de ransomware atrajo la atención particular del condado, ya que desconectó una cárcel de la red.

Cuando el ataque de ransomware derribó las cámaras de seguridad y las puertas automáticas del Centro de Detención Metropolitano, los reclusos tuvieron que ser confinados en sus celdas. Los sistemas de bloqueo electrónico de las puertas de las celdas fallaron, lo que obligó al Centro a restringir severamente el movimiento de los reclusos, una posible violación de un acuerdo de conciliación de 25 años sobre las condiciones de confinamiento de los reclusos.

La razón por la que mencionamos esto aquí es para demostrar la variedad de formas en que los ataques de ransomware pueden afectar el bienestar de los ciudadanos, las operaciones organizacionales y la salud general de las empresas o los departamentos gubernamentales.

4. Toyota

Entre febrero y marzo de 2022, tres proveedores de Toyota fueron pirateados, lo que nos muestra que un actor malicioso determinado puede y encontrará alguna brecha sin cubrir.

Cuando el proveedor de Toyota, Kojima Industries, sufrió un ataque cibernético (no necesariamente un ataque de ransomware), el gigante tuvo que detener las operaciones en 14 de sus plantas japonesas. Se dice que esto causó una enorme caída del 5% en la capacidad de producción mensual de la empresa.
Lo peor es que otros dos proveedores de Toyota, Denso y Bridgestone, fueron víctimas de ataques de ransomware en un lapso de 11 días. La subsidiaria de Bridgestone experimentó un ataque de ransomware que provocó el cierre de las redes informáticas y las instalaciones de producción en América Central y del Norte. Lockbit asumió la responsabilidad de este ataque.

En el caso de Denso, una empresa del grupo en Alemania supuestamente se vio comprometida por el grupo de ransomware Pandora. La lección aquí es simple pero aterradora: incluso las empresas con los recursos de Toyota están siendo víctimas de estos ciberataques masivos. ¿Qué significa esto para las empresas más pequeñas con presupuestos más ajustados y menos experiencia?

5. SpiceJet

La aerolínea india SpiceJet enfrentó un intento de ataque de ransomware a principios de este año, lo que dejó a cientos de pasajeros varados en varios lugares del país.

Si bien la aerolínea subrayó el hecho de que solo fue un “intento” de ataque de ransomware y que su equipo de TI logró contener la situación, el incidente expuso serias brechas de seguridad cibernética en uno de los mercados de aviación más grandes del mundo.

Destacó cómo las aerolíneas de todo el mundo deben evaluar su preparación para el ransomware y ampliar su preparación para responder a tales ataques de manera rápida y efectiva.

El hecho de que los pasajeros de SpiceJet estuvieran, aparentemente, esperando información sobre la salida de sus vuelos durante más de 6 horas afectó la reputación de la marca de la aerolínea según los informes de noticias. También destacó cuán crítica es la respuesta de emergencia y la comunicación oportuna en industrias como la aviación, un espacio donde una buena planificación de respuesta a incidentes puede desempeñar un papel muy importante.

Conclusión

Nadie está a salvo. El próximo correo electrónico de phishing podría parecer auténtico para un empleado de su organización y eso puede ser el comienzo del caos definitivo: comprometer datos confidenciales, archivos cifrados, sistemas fuera de línea y más.

Toda organización debe invertir en preparación y mitigación de ransomware si quiere protegerse de los altos costos que conlleva un ataque de ransomware, tanto monetarios como de reputación.

Estos 5 ataques de ransomware de 2022 han resaltado la importancia de que las empresas de todas las escalas y tamaños inviertan en revitalizar su infraestructura de ciberseguridad y piensen seriamente en su preparación y capacidades de respuesta de ransomware. Brindar a los equipos internos acceso a capacitación en ciberseguridad de alta calidad también se ha vuelto vital para la salud de cualquier organización.
Tener un plan de respuesta a incidentes de ransomware adecuado es esencial hoy en día y ensayar este plan con la ayuda de expertos es aún más importante.

SOLUCIONES SEGURAS EN LAS NOTICIAS

TELETICA: DÍA MUNDIAL DE LAS REDES SOCIALES: ¿CÓMO PROTEGERSE DE LOS RIESGOS CIBERNÉTICOS?

TELETICA.com

TVN NOTICIAS: PIDEN HACER USO RESPONSABLE DE LAS REDES SOCIALES

tvn Noticias

PRENSA LIBRE: LA ERA DIGITAL Y LA AMENAZA DE ATAQUES CIBERNÉTICOS

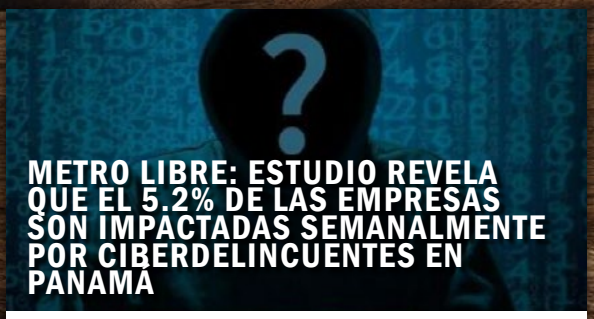
PRENSA LIBRE
Periódico líder de Guatemala

LA REPÚBLICA: "REDES SOCIALES SON UN CANAL PREDILECTO POR LOS HACKERS PARA REALIZAR FECHORÍAS": JOEY MILGRAM, SOLUCIONES SEGURAS COSTA RICA

SOLUCIONES PARA PROFESIONALES
LA REPÚBLICA.net

TYN MAGAZINE: ¿CUÁNTO LE CUESTA A LAS EMPRESAS SER VÍCTIMA DEL RANSOMWARE?

TyN MAGAZINE



METRO LIBRE: ESTUDIO REVELA QUE EL 5.2% DE LAS EMPRESAS SON IMPACTADAS SEMANALMENTE POR CIBERDELINCUENTES EN PANAMÁ

METRO LIBRE
LA VERDAD DE LA NOTICIA

SOLUCIONES SEGURAS

Empresas Protegidas, Empresas Tranquilas

TELEMETRO: TECH DAY 2022 ANALIZÓ TEMA DE CIBERSEGURIDAD PARA ENFRENTAR ATAQUES

telemetro.com

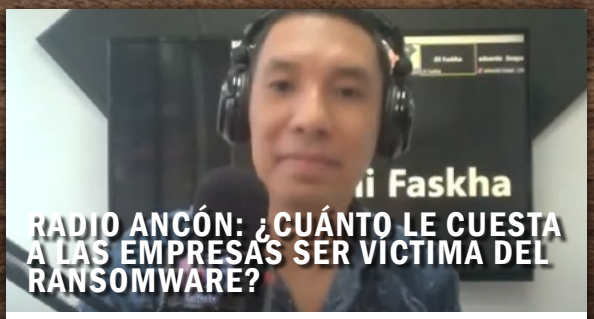
PRENSA LIBRE: LAS PEQUEÑAS Y MEDIANAS EMPRESAS TAMBIEN ADOPTAN LA TECNOLOGÍA Y LO HACEN DE VARIAS MANERAS

PRENSA LIBRE

Periódico líder de Guatemala

ESTRATEGIA & NEGOCIOS: ELI FASKHA, EL CEO DIGITAL DEBE CREAR UNA CULTURA SEGURA

E&N



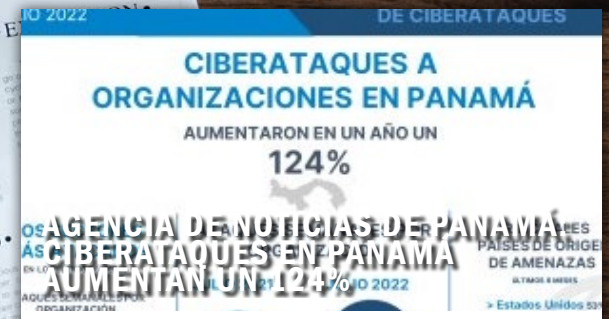
RADIO ANCÓN: ¿CUÁNTO LE CUESTA A LAS EMPRESAS SER VÍCTIMA DEL RANSOMWARE?

RADIO ANCÓN

LA PRENSA MARTES FINANCIERO: CÓMO LAS MIPYMES PUEDEN BLINDARSE ANTE LOS CIBERATAQUES

MARTES FINANCIERO

LA REVISTA FINANCIERA DE PANAMÁ



AGENCIA DE NOTICIAS DE PANAMÁ: CIBERATAQUES EN PANAMÁ AUMENTAN UN 124%

ANPanamá Agencia de Noticias

CÓMO REDUCIR EL RIESGO DE SER VÍCTIMA DE RANSOMWARE

Un ataque de ransomware exitoso puede ser devastador para una empresa. Las organizaciones sorprendidas sin preparación podrían tener que elegir entre pagar una demanda de rescate o cancelar por completo los datos robados.

Sin embargo, hay varias acciones que una empresa puede tomar para minimizar su exposición y los posibles impactos de un ataque de ransomware:

#1 Copia de Seguridad

El objetivo del ransomware es obligar a la víctima a pagar un rescate para recuperar el acceso a sus datos cifrados. Sin embargo, esto solo es efectivo si el objetivo realmente pierde el acceso a sus datos o no tiene forma de restaurarlos. Una solución sólida y segura de respaldo de datos es una forma efectiva de mitigar el impacto de un ataque de ransomware. Si se realizan copias de seguridad de los sistemas con regularidad, la pérdida de datos por un ataque de ransomware debería ser mínima o inexistente.

#2 Entrenamientos de Concienciación en Ciberseguridad

El phishing es una de las formas más populares de propagar malware. Al engañar a un usuario para que haga clic en un enlace o abra un archivo adjunto malicioso, los ciberdelincuentes pueden obtener acceso a la computadora del empleado y comenzar el proceso de instalación y ejecución del programa ransomware en ella. Una capacitación frecuente sobre seguridad cibernética es crucial para proteger a la organización contra el ransomware. Esta capacitación debe instruir a los empleados a:

- No hacer clic en enlaces maliciosos.
- Nunca abrir archivos adjuntos inesperados o que no sean de confianza.
- Evitar compartir/revelar datos personales o confidenciales a través de medios no verificados.
- Verificar la legitimidad del software antes de descargarlo.
- Nunca conectar un USB desconocido a su computadora.
- Usar una VPN cuando se conecte a través de Wi-Fi público o no confiable.

#3. Autenticación de usuario sólida y segura

Los ciberdelincuentes suelen utilizar el Protocolo de escritorio remoto (RDP) y herramientas similares para obtener acceso remoto a los sistemas de una organización utilizando credenciales de inicio de sesión adivinadas o robadas. Una vez dentro, el atacante puede colocar ransomware en la máquina y ejecutarlo, encriptando los archivos almacenados allí. Este potencial vector de ataque se puede cerrar mediante el uso de una fuerte autenticación de usuario. Establezca políticas de contraseña segura, que además requiera el uso de autenticación de múltiples factores son componentes críticos de la estrategia de seguridad cibernética de una organización.

#4. Sistemas Parchados y Actualizados

WannaCry, una de las variantes de ransomware más famosas que existen, es un ejemplo de gusano ransomware. En lugar de depender de correos electrónicos de phishing o RDP para obtener acceso a los sistemas de destino, WannaCry se propagó explotando una vulnerabilidad en el protocolo de bloque de mensajes del servidor (SMB) de Windows.

En el momento del famoso ataque de WannaCry en mayo de 2017, existía un parche para la vulnerabilidad EternalBlue utilizada por WannaCry. Este parche estaba disponible un mes antes del ataque y etiquetado como “crítico” debido a su alto potencial de explotación. Sin embargo, muchas organizaciones e individuos no aplicaron el parche a tiempo, lo que resultó en un brote de ransomware que infectó miles de computadoras en un par de días. Mantener las computadoras actualizadas y aplicar parches de seguridad, especialmente aquellos etiquetados como críticos, puede ayudar a limitar la vulnerabilidad de una organización a los ataques de ransomware.

#5. Soluciones Anti-Ransomware

Si bien los pasos anteriores de prevención de ransomware pueden ayudar a mitigar la exposición de una organización a las

amenazas de ransomware, no brindan una protección perfecta. Algunos operadores de ransomware utilizan correos electrónicos de phishing selectivo bien investigados y altamente dirigidos como su vector de ataque. Estos correos electrónicos pueden engañar incluso al empleado más diligente, lo que da como resultado que el ransomware obtenga acceso a los sistemas internos de una organización.
La protección contra estos tipos de ransomware avanzados requiere una solución de seguridad especializada. Para lograr su objetivo, el ransomware debe realizar ciertas acciones anómalas, como abrir y cifrar una gran cantidad de archivos. Las soluciones anti-ransomware monitorean los programas que se ejecutan en una computadora en busca de comportamientos sospechosos comúnmente exhibidos por ransomware, y si se detectan estos comportamientos, el programa puede tomar medidas para detener el cifrado antes de que se produzcan más daños.

Les compartimos un listado resumido y un poco más amplio de las formas más importantes y fundamentales de ayudar a su organización a protegerse de los ataques de ransomware:

- Copia de seguridad de sus datos.
- Mantenga su software actualizado.
- Utilice una solución especializada para detección de amenazas.
- Adopte la autenticación multifactor.
- Principio de privilegios mínimos.
- Analice sus correos electrónicos.
- Mejore la concientización de los colaboradores.
- Si es objeto de un ataque, no pague el rescate, consulte a expertos inmediatamente.

PROYECTO NO-MORE-RANSOM

Empresas encargadas de hacer cumplir la ley y de seguridad informática se han unido para interrumpir los negocios de los ciberdelincuentes con conexiones de ransomware.

El sitio web "No More Ransom" es una iniciativa de la Unidad Nacional de Delitos de Alta Tecnología de la policía de los Países Bajos, el Centro Europeo de Delitos Cibernéticos de Europol, Kaspersky y McAfee lanzada en julio de 2016 con el objetivo de ayudar a las víctimas del ransomware a recuperar sus datos cifrados sin tener que pagar a los delincuentes.

El portal y servicio web es hospedado gracias a Amazon AWS y Barracuda Networks. Y desde el lanzamiento del sitio web, el proyecto ha dado la bienvenida a grandes socios que han contribuido al desarrollo de nuevas herramientas de descifrado y claves de descifrado únicas, entre ellos líderes en ciberseguridad como Check Point y TrendMicro.

Dado que es mucho más fácil evitar la amenaza que luchar contra ella una vez que el sistema se ve afectado, el proyecto también tiene como objetivo educar a los usuarios sobre cómo funciona el ransomware y qué contramedidas se pueden tomar para prevenir la infección de manera efectiva. Cuantas más partes apoyen este proyecto, mejores serán los resultados. Esta iniciativa está abierta a otras partes públicas y privadas.

El consejo general que da el proyecto es no pagar el rescate. Al enviar su dinero a los ciberdelincuentes, solo confirmará que el ransomware funciona y no hay garantía de que obtenga a cambio la clave de descifrado que necesita.

BUENAS NOTICIAS

La prevención es posible. Seguir unos sencillos consejos de ciberseguridad puede ayudarle a evitar ser víctima de un ransomware.

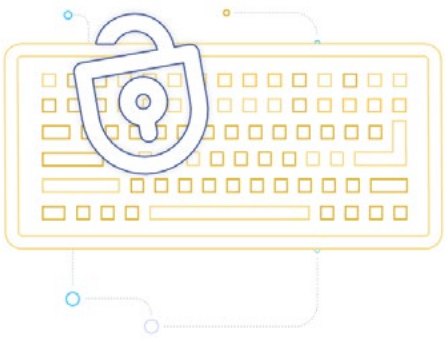
MALAS NOTICIAS

Desafortunadamente, en muchos casos, una vez que el ransomware se ha liberado en su dispositivo, es poco lo que puede hacer a menos que tenga un software de respaldo o seguridad.

BUENAS NOTICIAS

Sin embargo, a veces es posible ayudar a los usuarios infectados a recuperar el acceso a sus archivos cifrados o sistemas bloqueados, sin tener que pagar. El Proyecto No-More-Ransom ha creado un repositorio de claves y aplicaciones que pueden descifrar datos bloqueados por diferentes tipos de ransomware.

El proyecto ha puesto fin a amenazas como Loocipher, Astralocker, Atomsilo, Babuk, Prometheus, entre otros. En el sitio del proyecto puede explorar el listado completo de las amenazas y pulsando sobre el nombre del tipo de ransomware puede acceder a una herramienta de decifrado.



Le invitamos a visitar el proyecto en su sitio web oficial:

nomoreransom.org

¿CUÁNTO LE CUESTA A LAS EMPRESAS SER VÍCTIMA DEL RANSOMWARE?

El costo real para una empresa que sufre un ataque de ransomware o secuestro de datos, es 7 veces más alto que el monto de rescate pagado.

La acelerada transformación digital de las organizaciones abrió un sin fin de oportunidades para los ciberdelincuentes, quienes han perfeccionado sus técnicas para desplegar ataques de ransonware o secuestro de datos con mayor precisión. Es tanta la evolución de estos ataques que, en los primeros cuatro meses del año, se registraron ataques a 1 de cada 60 organizaciones en todo el mundo cada semana.

"El ransomware es un ataque que encripta la información y roba datos, por los cuales piden un rescate. Generalmente, la información es liberada hasta que se pague la suma de dinero solicitada por los delincuentes cibernéticos. Este malware ha tenido un crecimiento muy rápido, y es utilizado tanto en ataques a usuarios domésticos como grandes empresas o gobiernos", explica Eli Faskha, CEO de Soluciones Seguras.

De acuerdo a los investigadores de Check Point, partner de Soluciones Seguras, se ha detectado un aumento del 24 % en los ataques de ransomware año tras año a organizaciones de todo el mundo. Particularmente en Panamá, el 5.2% de las organizaciones son impactadas semanalmente por ataques de ransomware en los últimos 6 meses.

Hace pocos meses el grupo Conti lanzó ataques masivos de ransomware a instituciones públicas a dos naciones de América latina, Perú y Costa Rica, en este último caso, el Gobierno llegó a declarar estado de emergencia nacional y más tarde, que el país está en guerra cibernética.

"En Panamá se debe poner especial atención a este tipo de amenazas después de los efectos que tuvo el ataque al gobierno de Costa Rica; pues los cibercriminales observaron que son capaces de amenazar la estabilidad de un país centroamericano y presionar para que los gobiernos se presten a negociar", indica Faskha.

Entre los tipos de ransomware más sofisticados actualmente utilizados está la llamada "doble extorsión", en la que los ciberdelincuentes amenazan con publicar datos privados además de encriptarlos. También se puede encontrar la táctica de "triple extorsión", con la cual no solo envían un pedido de pago de rescate a la organización vulnerada, sino a sus clientes, usuarios o terceros.

¿Cuál es el verdadero costo de no prevenir un ataque de ransomware?

Hay que tener en cuenta que el costo de la extorsión es mínimo en comparación con otras pérdidas sufridas por la víctima.

No importa el tamaño o sector, cualquier organización puede ser vulnerable. Sin embargo, el costo total de un ataque de ransomware se puede dividir en dos áreas principales sin importar el tipo de organización: el costo de recuperación y, segundo, el costo de inactividad.

"En la mayoría de las empresas de la región, un ataque exitoso resulta, como mínimo, en el cierre completo de operaciones por tres días. Además, la perdida de datos financieros son difíciles o muy costosos de recuperar, y existe un costo por el daño a la imagen de la compañía. Esto es porque también están en riesgo los datos confidenciales de clientes, proveedores y demás personas o empresas ligadas", añade el experto.

Por ende, se estima que el costo total de un ataque de ransomware es 7 veces más que la cantidad que se paga por un rescate. Tomando en cuenta los costos de respuesta, restauración, honorarios legales, la supervisión, el costo por inactividad o pérdidas de productividad, entre otros montos adicionales.

¿Cómo protegerse del ransomware?

La inteligencia de amenazas y las capacidades de respuesta rápida son vitales, por ello, Faskha recomienda que las organizaciones, independientemente de su tamaño, efectúen hábitos de higiene cibernética y mejores prácticas. Por ejemplo, realizar periódicamente copias de seguridad de datos críticos, contar con base de datos y servidores en ubicaciones no conectadas a la red.

También es fundamental habilitar doble factor de autenticación y políticas de contraseñas seguras; la implementación de herramientas de detección de amenazas comprobadas y efectivas; conservar el software actualizado; y la capacitación de los colaboradores sobre seguridad informática, indicó el experto.

La llegada e implementación del 5G, la quinta generación de redes móviles, tiene el potencial de hacer que Panamá esté mucho más conectado; con velocidades más altas, menor latencia (el tiempo de respuesta de la web) y un mayor número de dispositivos IoT (Internet de las cosas) conectados. Sin embargo, con este crecimiento, también surgen implicaciones de ciberseguridad.

Tomando en cuenta que la expectativa es que surjan nuevas formas de trabajo y modelos de negocio, las empresas que implementen dispositivos inteligentes conectados a la red 5G necesitarán soluciones de seguridad capaces de monitorear y protegerse contra nuevas o mayores amenazas cibernéticas.

"La entrada del 5G permitirá que más dispositivos estén constantemente conectados a Internet y con un mejor rendimiento. Sin embargo, este aumento de dispositivos traerá nuevas vulnerabilidades y ampliará la superficie de ataques, lo que proporciona más puntos de entrada para que los cibercriminales amenacen las redes, la nube y aplicaciones, con el objetivo de secuestrar o robar información de las organizaciones", explica Eli Faskha, CEO de Soluciones Seguras.

Además, con la entrada del 5G aumenta la complejidad para mantener la privacidad de los datos; por lo que es aún más importante contar con soluciones de ciberseguridad y análisis para prevenir ataques tanto a nivel de red como a nivel de dispositivo. Según investigaciones se estima que una gran cantidad de los dispositivos inteligentes conectados a Internet (IoT) no cuentan con ningún tipo de herramientas de protección instaladas. Los panameños todavía no están acostumbrados a utilizar soluciones para proteger las conexiones móviles.

En este contexto, Soluciones Seguras recomienda que las empresas implementen soluciones de protección; que estén actualizadas con tecnología capaz de comprender y supervisar una enorme complejidad de relaciones y estructuras, a menudo vinculadas entre sí.

"Vemos el aumento exponencial de los ataques en el país, por lo que en Soluciones Seguras instamos a las empresas a iniciar una transformación hacia una cultura de seguridad entre los empleados para que puedan apoyar en el trabajo de protección. Además, crear políticas de seguridad de la identidad, políticas de conexiones remotas y, aún más importante, buscar soluciones avanzadas que permitan agilidad y seguridad a los sistemas de la empresa", explica Faskha.

Joey Milgram, uno de los directivos de Soluciones Seguras, asistió al CYBERARK IMPACT 2022, conferencia global sobre ciberseguridad organizada por su partner CyberArk, líder mundial en seguridad de identidad.

Impact es uno de los eventos más interesantes y valiosos sobre la gestión de acceso privilegiado (PAM) y la seguridad de la identidad, que reúne a profesionales de seguridad para conéctese, aprender, colaborar y discutir la importancia crítica de las estrategias basadas en Seguridad de Identidad, y ayudar a proteger los negocios digitales de la próxima generación de atacantes.

En el encuentro de tres dias, que tuvo lugar en el Hynes Convention Center en Boston del 12 al 14 de julio, se realizaron conferencias magistrales, capacitaciones y seminarios dirigidos por expertos clave en el ámbito de la seguridad, para dar a las organizaciones la confianza que necesitan para acelerar la transformación empresarial con menos riesgo.

Los oradores principales del CyberArk Impact 22022 incluyeron al fundador, presidente y CEO de CyberArk, Udi Mokady, Clarence Hinton, Director de Estrategia y Director de Desarrollo Corporativo de CyberArk, Chen Bitan, Gerente General Israel, Director de Producto de la compañía, Merritt Baer, Director, Oficina del CISO, AWS, y Robert

Herjavec CEO, Cyderes, Shark on ABC's Shark Tank, and Bestselling Author, entre otros.

El informe de seguridad de mitad de año 2022 de Check Point Software revela un aumento global del 42% en los ataques cibernéticos con el ransomware como la amenaza número uno.

Acceda de forma gratuita para experimentar el informe interactivo en línea, donde podrá obtener información detallada sobre:

1. Aumento global de los ataques cibernéticos.
2. Ataques cibernéticos consolidados como un arma a nivel estatal
3. El ransomware es la amenaza número uno
4. Perspectiva de respuesta a incidentes (IR)
5. Ataques a la cadena de suministro en la nube
6. Interrupción importante de la vida cotidiana

DESCARGAR EL INFORME

CURSOS VIRTUALES 2022

CCSA

CHECK POINT

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

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

Check Point Certified
VSX SPECIALIST

Habilidades importantes para implementar seguridad de red virtual

CCCS

CHECK POINT

Check Point Certified
CLOUD SPECIALIST

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

CCTA

CHECK POINT

Check Point Certified
TROUBLESHOOTING ADMINISTRATOR

Conceptos y habilidades necesarias para solucionar problemas

> **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

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.

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.

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.

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.

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.

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.

IPS Y PROTECCION 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.

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.

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.

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.

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.

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

SÍGUENOS EN NUESTRAS REDES SOCIALES

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 CYBERSECURITY MAGAZINE