Una visión a la ciberseguridad del futuro

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Una visión a la ciberseguridad del futuro

Check Point Software Technologies organizó el pasado mes de junio una nueva edición de su cita anual, CyberDay 2017, un evento dirigido a profesionales de TI y de ciberseguridad con el objetivo de mostrarles cuál es la situación real del malware y el mundo de la prevención y la ciberseguridad. El ransomware, la ciberseguridad de la nube, los móviles, IoT y las infraestructuras de riesgo, han sido los grandes protagonistas de la reunión.

INFINITY, LA ARQUITECTURA DE CIBERSEGURIDAD DEL FUTURO

CLICAR PARA VER EL VÍDEO

Los departamentos de TI deben balancear, en una mano, los deseos de los usuarios y los departamentos de negocio en cuanto a acceso a información, libertad de movimiento, velocidad de adaptación, y un largo etcétera de peticiones; en la otra, las necesidades de la empresa de mantener su información, dispositivos y usuarios dentro de un entorno seguro que garantice, por una parte, la supervivencia de la compañía, y, por otra, las adecuadas condiciones para que el negocio pueda desarrollarse sin sobresaltos ni cortes.

A este difícil equilibrio tenemos que añadirle , por una parte, un incremento de las amenazas -no solo en vectores conocidos- sino también en nuevos vectores de ataque (movilidad, IoT…) con nuevas formas evolucionadas que buscan puertas ocultas para entrar en nuestra red (ransomware) y otras amenazas desconoci-

SOBREVIVIR A LA PLAGA DE RANSOMWARE

CLICAR PARA VER EL VÍDEO

das que van surgiendo y para las que la seguridad tradicional no da respuesta. Por otro lado, tenemos los presupuestos que manejan los departamentos de TI que no crecen a la velocidad necesaria para estar siempre a la última en todo momento. Es decir, que los departamentos de TI se hallan en medio de lo que podríamos denominar una tormenta perfecta y son una embarcación que, si han hecho bien su trabajo, podría permitirles seguir navegando, pero que, si no, ya porque tenga grietas o ya porque el diseño sea demasiado anticuado para responder a las exigencias actuales, empezará a hacer aguas y podría llevar a la empresa a acabar hundida en el fondo del mar.

Pero dejemos las metáforas marineras y hablemos de tecnología, y de cómo las nuevas tendencias en la ciberseguridad buscan más la prevención como forma de atajar cualquier posible ataque antes de que se produzca. Porque no podemos olvidar que el departamento de TI debe atender demandas de usuarios y negocio que parecen no tener límites, y esto convive con la a explosión de nuevas tecnologías que prometen simplificación, eficiencias incalculables y ahorro de costes, pero mientras, crean incertidumbre, complejidad y riesgo. Es necesario que haya una estrategia global que asuma el compromiso de permitir aprovechar la promesa de estas nuevas tecnologías para el beneficio de las operaciones comerciales y los clientes, sin que esto suponga un problema para la ciberseguridad de la empresa, los datos y el propio negocio.

En el caso de Check Point Software Technologies hablamos de Check Point Infinity, una arquitectura de ciberseguridad consolidada en redes, nube y móviles que apuesta por la prevención de amenazas.

Un cambio de estrategia en la ciberseguridad

La tradicional concepción de la ciberseguridad como una muralla alrededor de un castillo (el centro de datos) ha saltado por los aires porque, para empezar, los límites que marcaban la red hace unos años ahora han desaparecido. La proliferación de dispositivos móviles inteligentes, instancias virtuales, nube pública, nube privada, todo como servicio (EaaS), Internet de las cosas (IoT)… han hecho que los límites de la red sean difusos, los puntos de acceso se hayan multiplicado, y

El ransomware, la ciberseguridad de la nube, los móviles, IoT y las infraestructuras de riesgo, han sido los grandes protagonistas de CyberDay 2017

el reto de los responsables de la ciberseguridad se hayan incrementado exponencialmente. Para adecuarse a esta realidad, las empresas deben transformarse digitalmente. La transformación digital consiste en cambiar la forma en que el negocio opera, y esto, necesariamente, también afecta a la ciberseguridad de TI. Se trata de aprovechar la interconexión y satisfacer el flujo y el reflujo natural de los negocios con una infraestructura elástica que entrega automáticamente todos los servicios de la manera más eficiente y rentable. Se trata de una completa transformación a un nuevo paradigma mediante el aprovechamiento de las redes virtuales, móviles, cloud, EaaS y más para ofrecer operaciones de negocios rápidas y confiables de una manera más conectada, dinámica, eficiente y rentable.

Desafortunadamente, con demasiada frecuencia, las estrategias y diseños de ciberseguridad para estos nuevos entornos se remontan a los primeros años del 2000, donde se desplegó un sinfín de productos no integrados y dispares. Así que, en lugar de una arquitectura de ciberseguridad unificada, las empresas están de nuevo atascadas con las ineficiencias de la gestión de múltiples

WANNACRY 3.0, PRÓXIMAMENTE EN SUS PANTALLAS... DEL MÓVIL

CLICAR PARA VER EL VÍDEO

2016 fue un año de récord para el ransomware y 2017 será peor todavía, según Check Point Software

Aprovechando la celebración del CyberDay 2017, Check Point Software Technologies ha hecho un repaso de la actualidad en el mundo de la ciberseguridad, una actualidad marcada por la notoriedad del ransomware, que en 2016 vivió un año de récord en volumen de malware, en número de afectados, en innovación y en beneficios. Pero lo más preocupante es que desde la firma esperan que en 2017 vamos a ver cómo se incrementan estos datos.

Y es que en este 2016 se ha producido un cambio de estrategia de los ciberdelincuentes. Hasta la fecha, trataban de conseguir información personal de los usuarios y las empresas para venderla y convertirla en dinero. Sin embargo, ahora buscan vender sus datos al propio usuario, una práctica menos arriesgada y más beneficiosa, sobre todo por la anonimidad y la imposibilidad de rastrear el pago en Bitcoins. Con todo, los datos del ransomware se resumen afirmando que el 40% de la base atacada es infectada, y, de ellos, el 70% acaba pagando, lo que, solo en Estados Unidos, según datos del FBI, ha reportado más de mil millones de dólares. Y es que en este año se ha mejorado el mecanismo de entrega del malware, se atacan datos importantes para el usuario, y, somo hemos comentado, se ha mejorado el sistema de pagos.

De cara a 2017, se espera la expansión del ransomware as a service, los programas de filiación y nuevos modelos de pago, además de mejorar el malware, con capacidades para encriptar los backups, por ejemplo, y el despliegue por nuevos dispositivos, principalmente el smartphone, pero también todos los conectados a IoT.

productos de ciberseguridad separados que, al final, no protegen eficazmente la nueva operación de TI o el negocio.

En resumen, ¿qué necesita una empresa? Necesita una plataforma unificada de ciberseguridad que le permita gestionar entornos móviles, de nube y de red; que se adelante a los problemas con la prevención integrada de amenazas; con una política de ciberseguridad que integra las necesidades de la empresa; y que puede adaptarse al ritmo que necesite adaptarse el negocio.

Check Point Infinity

El pasado mes de abril, Check Point Software Technologies presentó Check Point Infinity, una arquitectura de ciberseguridad diseñada para satisfacer las necesidades de ciberseguridad de las empresas. Check Point Infinity incorpora protección consolidada a través de las redes, la nube y los dispositivos móviles, y proporciona prevención de amenazas para mantener a los clientes a salvo frente al creciente número de ciberataques.

Tal y como señaló en su presentación Gabi Reish, vicepresidente de gestión de productos de Check Point, "Check Point Infinity es la culminación de nuestra visión global de construir una arquitectura de ciberseguridad que unifique la mejor protección, la mejor inteligencia y la mejor gestión que podemos ofrecer a través de las redes, la nube y los dispositivos móviles".

Asimismo, este responsable añadía que Check Point Infinity "está diseñada para asegurar que las organizaciones estén preparadas para manejar la dinámica tan cambiante de la TI del futuro. El principio es muy simple: una arquitectura de ciberseguridad unificada mantendrá a las empresas a salvo en todos los entornos, con operaciones de TI más eficientes y efectivas".

Check Point Infinity se apoya en tres elementos clave:

- Una única plataforma de ciberseguridad: aprovecha las plataformas comunes, la inteligencia

UN VIAJE SEGURO A LA NUBE

CLICAR PARA VER EL VÍDEO

El 20% de operadores de infraestructuras críticas no han hecho ninguna evaluación de riesgo

Durante la celebración del CyberDay 2017, Check Point Software Technologies ha presentado en informe Estado de la Ciberseguridad en los operadores de infraestructuras críticas en España.

De los datos del informe se desprende que el 20 por ciento de los operadores de infraestructuras críticas no han realizado ninguna evaluación de riesgo, dato que se duplica cuando hablamos de los sectores de agua y transporte.

Otro de los datos que llaman la atención es que el 22% de las empresas encuestadas no tienen proceso de gestión de incidentes o solo funcionan de forma reactiva. Además, solo el 27 por ciento de ellos mantienen sus redes industriales separadas del resto con múltiples niveles de segmentación.

En cuanto a los responsables de negocio, el 40% dice tener una sensibilidad alta, si bien en el 25% es escasa o nula (un 67% en el sector del agua). De ahí que solo el 35% de los encuestados planifican acciones de ciberseguridad en el tiempo. Es más, solo el 12% dice mejorar por exigencias provenientes de la dirección.

La nota positiva llega de la mano de la previsión de presupuestos para el año próximo, dado que tres de cada cuatro esperan incrementar esta partida. Eso sí, no es igual en todos los sectores, dado que, si bien es el 100% en el sector eléctrico, nuclear, agua y financiero, apenas alcanza el 37% en el sector del transporte.

Por último, cabe destacar que, pese a la pérdida de predominio en otros segmentos por el desarrollo y la expansión de la Transformación Digital, esta preocupación y contratación de proyectos de ciberseguridad sigue en manos del área de TI.

La tradicional concepción de la ciberseguridad como una muralla alrededor de un castillo (el centro de datos) ha saltado por los aires porque, para empezar, los límites que marcaban la red hace unos años ahora han desaparecido

de amenazas y la infraestructura abierta. Ofrece protección sin precedentes en todas las plataformas, independientemente de la red o del tamaño.

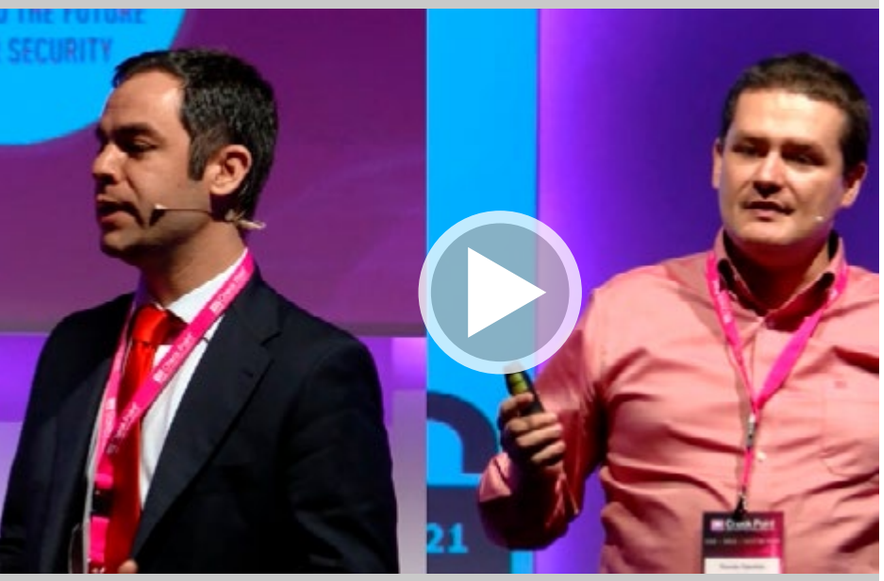
- Prevención de amenazas anticipada: se centra en la prevención para bloquear los más sofisticados ataques conocidos y desconocidos antes de que sucedan.
- Sistema consolidado: una gestión única, gestión de políticas modular y visibilidad integrada de las amenazas para centralizar eficientemente la ciberseguridad a través de un cuadro de mando único

Check Point Infinity permite a las empresas tomar el control de su ciberseguridad y proteger y administrar toda su operación de TI como una arquitectura única cohesiva para el beneficio de sus operaciones comerciales y sus clientes.

Innovación en ciberseguridad

Los avances en tecnología han impulsado innumerables mejoras en la forma de trabajar de las empresas, pero también han alterado la forma en que deben abordar la ciberseguridad. Check Point Infinity responde a esta necesidad e introduce nuevas capacidades:

CYBERTALKS: MAPFRE Y FERROVIAL



CLICAR PARA VER EL VÍDEO

- Gestión de la ciberseguridad: El lanzamiento de la versión R80.10 de Security Management cuenta con docenas de nuevas mejoras, incluidas capas de políticas, múltiples zonas de ciberseguridad y rendimiento potenciado para mantener a las organizaciones a salvo de cualquier amenaza, en cualquier momento y en cualquier lugar.
- Cloud: La cartera integral actualizada de vSEC Cloud Security de Check Point se integra con las plataformas de nube privadas y públicas, lo que garantiza la ciberseguridad de los entornos cloud.
- Móvil: El nuevo SandBlast Mobile es la única solución unificada y multiplataforma del sector, que protege a las empresas de las brechas móviles. SandBlast Mobile detecta y bloquea malware conocido y desconocido, protección contra redes Wi-Fi envenenadas y ataques man-in-the-middle, así como esquemas de phishing SMS.
- Prevención de amenazas: La nueva tecnología Check-Point Anti-Ransomware permite a las empresas mantenerse protegidas contra la ciberextorsión e incluso los programas de ransomware más sofisticados.

Gestión de ciberseguridad

Las redes crecientes, las tecnologías disruptivas y la proliferación de dispositivos interconectados exigen un nuevo enfoque para gestionar la ciberseguridad. La arquitectura de Check Point Infinity consolida la gestión de múltiples capas de ciberseguridad, proporcionando una eficacia superior y permitiendo gestionar la ciberseguridad a través de un único panel.

Con R80.10 una única plataforma gestiona toda la infraestructura de TI, desde el centro de datos hasta las implementaciones de nube privadas / públicas, para garantizar la eficacia y la coherencia de la ciberseguridad. La gestión de políticas está unificada para que pueda crearse y supervisarse de forma única. Una sola política gestiona sus usuarios, dispositivos, aplicaciones, datos y redes. Con esta política unificada, también obtiene un control granular más amplio.

Las empresas necesitan una plataforma unificada de ciberseguridad que le permita gestionar entornos móviles, de nube y de red y que se adelante a los problemas con la prevención integrada de amenazas

ESTADO DE LA CIBERSEGURIDAD EN OPERADORES DE INFRAESTRUCTURAS CRÍTICAS ESPAÑOLAS

CLICAR PARA VER EL VÍDEO

La API R80.10 facilita la integración segura con sistemas de orquestación, gestión de cambios y ticketing. Con la capacidad de controlar exactamente lo que la integración puede y no puede hacer, las organizaciones tienen la confianza necesaria para integrar la ciberseguridad en su ecosistema de TI. Las tareas rutinarias pueden ser automatizadas y delegadas, liberando equipos de ciberseguridad de tareas repetitivas para centrarse en tareas estratégicas de ciberseguridad como la respuesta a las incidencias.

ENTREVISTA CON GABI REISH, VP MUNDIAL DE MARKETING Y GESTIÓN DE PRODUCTO EN CHECK POINT

CLICAR PARA VER EL VÍDEO

Las organizaciones necesitan una ventana de control única para el análisis de eventos, el monitoreo de amenazas y la mitigación para asegurar una visibilidad completa de las amenazas a través de la red. Los datos deben ser recolectados de todas las pasarelas desplegadas y pasados por fuentes externas de inteligencia de amenazas para proporcionar información contextual.

VSEC para la ciberseguridad de la nube pública y privada

La eficiencia de los procesos y la mayor agilidad de la red están impulsando la adopción de la tecnología IaaS y SDN a un ritmo rápido. Pero esta nueva infraestructura también está presentando a las empresas un conjunto único de desafíos de ciberseguridad. Check Point

Check Point Infinity es una arquitectura de ciberseguridad consolidada en redes, nube y móviles que apuesta por la prevención de amenazas

vSEC protege los activos en la nube de las amenazas más sofisticadas con escalabilidad dinámica, provisión inteligente y control constante a través de redes físicas y virtuales.

La virtualización de la red ha creado un cambio en el comportamiento del tráfico. Ahora, más y más tráfico se mueve en el centro de datos creando nuevos desafíos de ciberseguridad. Con pocos controles para asegurar este tráfico, las amenazas pueden viajar sin obstáculos una vez dentro del centro de datos. Check Point vSEC ofrece protección avanzada contra amenazas para evitar su propagación lateral dentro de los centros de datos definidos por software, así como la visibilidad y el control para gestionar eficazmente la ciberseguridad tanto en entornos físicos como virtuales, desde una única solución de gestión unificada.

Mover recursos y datos de computación a nubes públicas significa que las responsabilidades de ciberseguridad se comparten entre la empresa y su proveedor de la nube. Mientras que la protección de la infraestructura es trabajo del proveedor, las empresas quieren la capacidad de controlar sus propios datos y mantenerlos en privado, así como proteger los activos de la nube,

todo mientras cumple los mandamientos regulatorios. Check Point vSEC permite una conectividad confiable a los activos de la nube pública mientras protege las aplicaciones y los datos con la prevención avanzada de amenazas en entornos de nube públicos e híbridos.

Check Point vSEC ofrece también ciberseguridad avanzada de múltiples capas para entornos virtuales de centro de datos y virtualización de la función de red (NFV) y está diseñado para equipar a los proveedores de servicios con ciberseguridad integral contra amenazas, protección de día cero, entrega ágil, administración y automatización a través de la red básica.

SandBlast Móvil

El uso de teléfonos inteligentes y tabletas para acceder a información crítica en cualquier momento tiene muchos beneficios, pero puede exponer sus datos confidenciales a riesgos. SandBlast Mobile de Check Point protege sus dispositivos de amenazas móviles avanzadas, asegurando que puede desplegar y defender dispositivos con confianza.

ENTREVISTA CON MARIO GARCÍA, DIRECTOR GENERAL DE CHECK POINT PARA ESPAÑA Y PORTUGAL

CLICAR PARA VER EL VÍDEO

Los principales beneficios de esta solución son la posibilidad de detectar, evaluar y mitigar amenazas avanzadas de ciberseguridad para móviles; proteger los datos empresariales confidenciales en reposo, en uso y en tránsito en dispositivos móviles iOS y Android de ataques cibernéticos; mejorar la visibilidad y la protección mediante la integración con los sistemas existentes de movilidad y ciberseguridad (MDM, MAM, NAC, SIEM...); habilitar la respuesta rápida a ataques de amenazas persistentes avanzadas (APT) entre plataformas; preservar la experiencia del usuario y la privacidad, a la vez que añade la protección requerida por los mandatos organizacionales o regulatorios.

SandBlast Mobile es una solución de ciberseguridad móvil completa que protege los dispositivos de las amenazas en el dispositivo, en las aplicaciones y en la red y ofrece la mayor tasa de captura de amenazas de la industria para iOS y Android. SandBlast Mobile utiliza la detección de aplicaciones malintencionadas para detectar amenazas conocidas y desconocidas aplicando emulación de amenazas, análisis de código estático avanzado, reputación de aplicaciones y aprendizaje automático.

SandBlast Mobile está diseñado para ayudar a proteger los dispositivos móviles de forma rápida y segura a través de la integración con todas las soluciones EMM. Esto ayuda a que la solución sea altamente escalable y ofrece eficiencias operativas sólidas para administrar la ciberseguridad móvil dentro de una infraestructura de ciberseguridad más amplia.

Prevención de amenazas

El Ransomware se ha convertido en una gran amenaza para las empresas y los individuos de todo el mundo. La incapacidad de hacer frente eficazmente a los ataques de ransomware puede causar pérdidas significativas y grandes interrupciones a las organizaciones. La implementación de mejores prácticas convencionales y protecciones anti-malware puede defenderse contra algunas variantes conocidas y antiguas de ransomware, pero dada la sofisticación y la evolución continua de los ransomware modernos, no son suficientes por sí solos para identificar y bloquear nuevos ataques de día cero.

La tecnología Anti-Ransomware de Check Point utiliza un motor de propósito específico que se defiende contra las variantes de día cero más sofisticadas y evasivas de ransomware y recupera con ciberseguridad los datos cifrados, garantizando la continuidad del negocio y la productividad.

¿Te ha gustado este reportaje?
Compártelo en tus redes sociales
Twitter Facebook LinkdeIn beBee

SandBlast Agent incluye la tecnología Anti-Ransomware y proporciona protección a los navegadores web y puntos finales, aprovechando las protecciones Check Point. SandBlast Agent ofrece una prevención completa de amenazas y remediación en tiempo real a través de todos los vectores de amenazas de malware, permitiendo a los empleados trabajar con ciberseguridad sin importar dónde se encuentren y sin comprometer la productividad.

Enlaces relacionados

- El futuro de la ciberseguridad
- Sobrevivir a la plaga de ransomware
- WannaCry 3.0... en sus móviles
- Check Point Mobile Threat Penvention
- SandBlast
- vSec
- Security CheckUP