La Seguridad es Infinity

Check Point
SOFTWARE TECHNOLOGIES LTD.

Noviembre 2018

La Seguridad es Infinity

Coincidiendo con el 25 aniversario de la compañía, Check Point Software Tehcnologies celebró los días 17 y 18 de octubre en El Escorial una nueva edición de CPX España, en el que participaron más de 400 profesionales del sector de la seguridad informática. Los expertos más destacados de la compañía explicaron cuál es el panorama de la ciberseguridad en España, así como los principales desafíos y amenazas actuales como los ataques a móviles e infraestructuras cloud y las herramientas de las cuales se dispone para enfrentarse a estas amenazas, como la aplicación de la Inteligencia Artificial de forma práctica.

Check Point cumple 25 años en el mercado. 25 años de evolución de la seguridad, de pasar de una generación a otra, de la primera a la quinta, que es en la que estamos. Una sucesión de ataques y contra-ataques, de la llegada de los antivirus para hacer frente a los virus que sólo afectaban a los ordenadores; de la de los firewalls para hacer frente a las amenazas que llegaban a través de Internet; de los sistemas de prevención de intrusiones para intentar controlar la seguridad de las aplicaciones; de las tecnologías de sandboxing y antibots para hacer frente a las cargas útiles y los ataques polimórficos… hasta llegar a la actual, a la quinta, en la que los ataques son a gran escala, multiverctoriales y utilizan tecnologías patrocinadas por estados, técnicas en las que el nivel de sofisticación es realmente avanzado.

Hablaba sobre ello Mario García, director general de Check Point para España y Portugal durante el CPX España 2018, un evento celebrado los días 17 y 18 de octubre en El Escorial, coincidiendo con el 25º aniversario de la empresa; un evento que incluyó ponencias, formaciones, laboratorios y sesiones prácticas y que estuvo patrocinado por Aruba, BackBox, Arrow, Tufin, V-Valley y Westcon, y al que acudieron 400 profesionales del sector de la seguridad informática.

La Seguridad es Infinity

CPX ESPAÑA 2018

CLICAR PARA VER EL VÍDEO

Con el apoyo de la arquitectura Infinity, Check Point CloudGuard SaaS proporciona protección contra amenazas de quinta generación para aplicaciones SaaS

Decía Mario García que hay que ser consciente de que hay que proteger la empresa y el entorno y que “tenemos una importante tarea que realizar para hacer frente al futuro de la seguridad”, un futuro marcado por la prevención, que es “la mejor forma de combatir el malware para que no entre”.

Considera Mario García que WannaCry fue una llamada de atención y que estamos llegando a un momento de inflexión, a esa quinta generación de amenazas, de ataques, que llegan por todos lados y están esponsorizados por los estados. ¿Cómo podemos protegernos de ellas? “Con las mejores tecnologías de seguridad, con tecnologías de prevención de amenazas en tiempo real”, decía el directivo. La protección llega a través de Check Point Infinity, una arquitectura de ciberseguridad consolidada en redes, nube y móviles que apuesta por la prevención de amenazas, “una consola centralizada que te avisa si está pasando algo”.

Check Point Infinity busca dar solución a la pérdida del perímetro, esa muralla que rodeaba a la empresas y que ha ido desapareciendo con la llegada de los dispositivos móviles, de las instancias virtuales, de la nube, del IoT… Estos avancen han difuminado ese perímetro, han multiplicado el número de endpoints que hay que proteger, y ha incrementado y potenciado los retos de los responsables de seguridad de las empresas.

Todo el mundo tiene cosas en el cloud, recordaba Mario García durante su ponencia. “No van a dejar de existir las tiendas físicas, ni las infraestructuras físicas, pero el cloud tampoco”, aseguraba el directivo, añadiendo que el cloud va a pasar y está pasando, “y si no tenéis una estrategia de seguridad

Infinity Total Protection, la seguridad a tu alcance por un coste fijo

Para poder sacar partido a la protección Infinity de Check Point, la compañía ha desarrollado Infinity Total Protection, una propuesta que permite a los clientes poder consumir y acceder a todas sus soluciones de seguridad por un coste fijo por usuario y mes.

Infinity Total Protection es la única solución de suscripción disponible actualmente que incluye hardware y software de seguridad de red, con protección integrada para endpoints, nubes y dispositivos móviles, y prevención de amenazas de día cero, junto con una administración unificada y soporte premium 24×7.

Este modelo utiliza componentes de la arquitectura Infinity de Check Point, que proporciona elevados niveles de seguridad y, al mismo tiempo, reduce los costes al consolidar los componentes de seguridad.

Todos los sectores empresariales están experimentando ciberataques Gen V, que se caracterizan por ser a gran escala y de rápido movimiento en múltiples industrias. Estos sofisticados ataques dirigidos a dispositivos móviles, la nube y redes empresariales, evitan fácilmente las defensas convencionales y estáticas basadas en la detección que utilizan la mayoría de las organizaciones en la actualidad. Para proteger las redes y los datos contra estos ataques, las organizaciones deben optar por Check Point Infinity, que combina prevención de amenazas en tiempo real, inteligencia compartida y seguridad avanzada en redes, nubes y dispositivos móviles.

cloud debéis planteárosla". Los datos están ahí, la seguridad está creciendo y si en entornos móviles ha crecido un 300%, en entornos cloud el incremento es del 350%.

Check Point Infinity unifica la mejor protección, la mejor inteligencia y la mejor gestión a través de las redes, la nube y los dispositivos móviles, y está diseñada para asegurar que las organizaciones estén preparadas para manejar la dinámica tan cambiante de la TI del futuro. Y es que con Infinity, con la arquitectura de seguridad de la compañía, no sólo se hace frente a las actuales amenazas de seguridad, de la Gen I a la Gen V, sino a las que vengan.

"Los ataques de quinta generación se acaban y llega la VI de la mano del IoT", decía Mario García al tiempo que aclaraba que la estrategia de defensa en IoT y en cloud no es la misma que la del datacenter; "nacen y mueren más rápido, y la seguridad tiene que cambiar de la misma manera. La Gen VI es la generación de la nano seguridad".

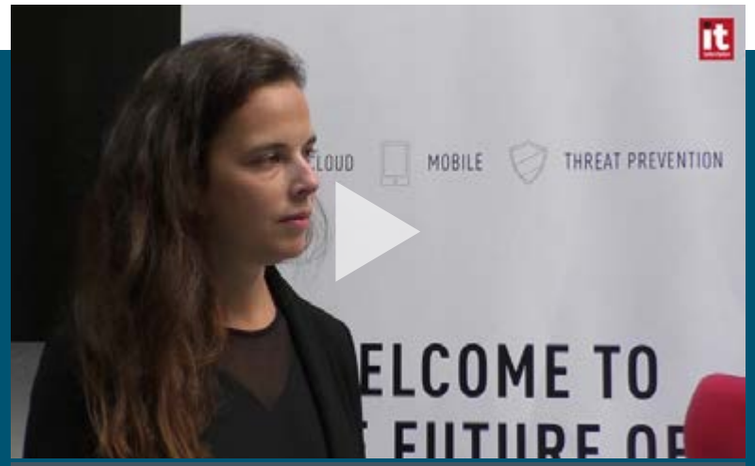
Queda mucho trabajo por hacer para que las empresas estén al día en seguridad, y Check Point propone más Infinity para hacer frente al reto. En este caso se trata de Infinity Total Protection y es "un plan de cómo trabajar con vosotros", un acuerdo que permite a las empresas tener acceso a todas las herramientas de seguridad por un coste fijo por usuario, un acuerdo "tan largo, o tan corto como queráis", que ofrece a los clientes la flexibilidad que necesitan.

Y concluía Mario García su ponencia asegurando: "En Check Point tenemos gente con talento, gente realmente buena. Bienvenidos al futuro de la seguridad".

IA aplicada a la seguridad

Tal Eisner, Product Marketing Manager, participaba en el evento explicando la importancia de la Inteligencia Artificial y su prometedor futuro en la industria de la ciberseguridad.

La Seguridad es Infinity



ENTREVISTA CON MAYA HOROWITZ, THREAT INTELLIGENCE GROUP MANAGER DE CHECK POINT

CLICAR PARA VER EL VÍDEO

ENTREVISTA CON ALBERTO MAESTRE, SOLUTION ARCHITECT DE TUFIN

CLICAR PARA VER EL VÍDEO

ENTREVISTA CON DAVID GARCÍA CANO, CYBER SECURITY SALES MANAGER SOUTHER EUROPE DE ARUBA

CLICAR PARA VER EL VÍDEO

ENTREVISTA CON ALON ROTHCHILD, PRE SALES INGENIEER DE BACKBOX

CLICAR PARA VER EL VÍDEO

Infinity Total Protection es un modelo de consumo que permite a las empresas tener acceso a todas las herramientas de seguridad de Check Point por un coste fijo por usuario

Todo el mundo habla de Inteligencia Artificial, en todas las industrias. Para Stephen Hawking “el desarrollo de una inteligencia artificial completa podría significar el fin de la raza humana”, una opinión muy similar a la de Steve Wozniak, quien asegura que no hay duda de que “los ordenadores van a tomar el relevo a los humanos”, o a la de Vladimir Putin, cuando dice que “los países que lideren la IA serán los que gobiernen el mundo”. Para Elon Musk, la Inteligencia Artificial “será la causa más probable de la tercera guerra mundo”. Tal Eisner prefirió referirse a la Inteligencia Artificial como “la próxima

Check Point Infinity es una arquitectura de seguridad que unifica la mejor protección, la mejor inteligencia y la mejor gestión a través de redes, nube y dispositivos móviles

MARIO GARCÍA, DIRECTOR DE CHECK POINT PARA ESPAÑA Y PORTUGAL

revolución industrial, una revolución en la que los músculos serán sustituidos por el cerero".

La capacidad de almacenar petabytes de información con lo que alimentar el machine learning; la capacidad de cómputo con la que digerir y analizar la información almacenada y la capacidad de enfocarse en los algoritmos matemáticos que extraigan valor es lo que está impulsando la adopción de la Inteligencia Artificial, algo cada vez más presente en nuestras vidas, tanto en previsiones como en soluciones de búsqueda de imágenes o en el reconocimiento del habla a través de asistentes como Siri, Alexa y otras grandes amigas.

Lo decía el directivo de Check Point antes de preguntar si hay magia en la Inteligencia Artificial y enumerar algunos ejemplos de cómo se está aplicando y dejar claro que lo que necesita una buena solución de IA son datos. "Cuando no hay datos y no hay suficiente experiencia se generan veredictos oscuros que afectan a la tasa de detección", decía el Product Marketing Manager de Check Point antes de asegurar que la Inteligencia Artificial está revolucionando la ciberseguridad "porque permite crear procesos mecanizados para detectar malware y amenazas".

Check Point ya ha desarrollado y evolucionado motores basados en IA en su plataforma de prevención de amenazas, consiguiendo mejorar la detección de malware hasta un 600% gracias a ellos. Las herramientas que ha desarrollado son, entre otras, Campaign Hunting, Huntress y Context-Aware Detection (CADET).

Seguridad cloud, Check Point Cloudguard SaaS

El 70% de las empresas están utilizando algún tipo de aplicación en la nube, según datos de Gartner. El gran reto del cloud es cómo proteger los datos que ahora se encuentran en aplicaciones que salen de nuestros control, como puede ser un Office 365, un Salesforce, un Dropbox…

Check Point afronta el reto de securizar este entorno aplicando tecnologías que la compañía ha estado aplicando en el firewall, o en el endpoint, pero ahora aplicado al mundo cloud. Se presta mucha atención al robo de credenciales, identificado como

Grandes amenazas de seguridad móvil

Probablemente WannaCry es el malware más conocido de los últimos tiempos e infectó a menos de un millón de ordenadores y generó un negocio de dos millones de dólares. El mundo móvil es más rentable, aseguraba Francisco Arcia, Threat Prevention Sales Manager Iberia en Check Point, durante la celebración del CPX España 2018.

Durante su ponencia sobre las últimas amenazas se seguridad móvil el experto de Check Point hacía referencia a algunos ejemplos de malware para plataformas móviles. Nombraba a HummingBad, con el que sus creadores llegaron a ganar más de 300.000 dólares al mes tras infectar unos diez millones de dispositivos.

También descubierto por Check Point, CopyCat infectó más de 14 millones de dispositivos Android alrededor del mundo, y generar negocio por valor de más de 16 millones de dólares por anuncios fraudulentos.

Otro ejemplo de malware móvil con pretensiones es Gooligan que generó el mayor robo de credenciales de la historia. El malware comprometió un total de un millón de cuentas de Google que se encuentran en nuestros dispositivos móviles. Según Check Point, Gooligan se encontró en 86 aplicaciones infectadas en varios mercados de aplicaciones de terceros.

Las aplicaciones son un coladero de malware, y si el ejemplo de Gooligan no es suficiente añadía Francisco Arcia el de Dreesscode, un malware que se coló en 40 aplicaciones alojadas en Google Play, un malware que además interactuaba sólo cuando el dispositivo se conectaba a la wifi de la empresa para establecer una comunicación y hacer una copia de todos los datos y ficheros.

SandBlast Mobile es la propuesta de Check Point, una solución que protege los dispositivos de las amenazas en el dispositivo, en las aplicaciones y en la red, para iOS y que se integra con casi todos los MDMs del mercado.

el mayor problema a nivel de aplicación, junto con el malware, pero además se incorpora un motor de DLP porque según Francisco Arcia, Threat Prevention Sales Manager Iberia en Check Point, “otro de los grandes problemas que estamos viendo son las fugas de información. El resultado es Check Point Cloudguard SaaS para aplicar la seguridad sobre múltiples aplicaciones en la nube y con una manera de comercialización por la que el cliente que quiera este tipo de soluciones sólo tiene que saber cuántos clientes quiere proteger y le vamos a dar todas esta tecnología para todas las aplicaciones que quiere proteger.

CloudGuard SaaS utiliza la tecnología ID-Guard para identificar el acceso de usuarios ilegítimos y evitar que los usuarios no autorizados accedan a las aplicaciones SaaS. Además, CloudGuard SaaS permite crear políticas coherentes entre dispositivos móviles, PC e incluso gateways, y una monitorización de seguridad unificada que se aplica en forma generalizada.

Check Point Cloudguard SaaS incorpora diferentes tecnologías, como de la sandboxing, Threat Extraction, motores antiphishing y DLP, protección de identidad, etc., y todo ello basado en una consola cloud sin coste adicional para los clientes y fácil de utilizar, con integración vía API con todas las aplicaciones.

“Para evitar el robo de credenciales hemos hecho algo único”, decía Francisco Arcia: poder validar que un usuario se está conectando desde un dispositivo verificado y seguro. “Podemos combinar dispositivos, nivel de riesgo, usuarios y en muchos casos geolocalización”, decía Arcia.

Check Point está en el móvil, está en las redes, en el cloud, en el puesto de trabajo, y eso significa que, si un usuario accede a una página que se califica como maliciosa, esa información pasa a formar

La Seguridad es Infinity

Ponencias CPX España 2018

TAL EISNER, PRODUCT MARKETING MANAGER DE CKECK POINT

IS AI THE SILVER BULLET IN CYBER SECURITY? — CLICAR PARA VER EL VÍDEO

MAYA HORROWITZ, THREAT INTELLIGENCE GROUP DE CHECK POINT

CYBER ACADEMY AWARDS 2017 – LEADING TRENDS IN THE THEATS LANSDCAPE — CLICAR PARA VER EL VÍDEO

DAVID GARCÍA CANO CYBER SECURITY SALES MANAGER SOUTHENR EUROPE DE ARUBA

CYBERTALK: PROTÉGETE DE LAS AMENAZAS INTERNAS CON ARUBA SECURITY Y CHECK POINT — CLICAR PARA VER EL VÍDEO

EUSEBIO NIEVA, DIRECTOR TÉCNICO DE CHECK POINT ESPAÑA Y PORTUGAL

LA NUEVA ARQUITECTURA DE SEGURIDAD CONSOLIDADA: INFINITY — CLICAR PARA VER EL VÍDEO

ALON ROTHCHILD, PRE SALES INGENIEER DE BACKBOX

CYBERTALK: INTELLIGENCE AUTOMATION FOR SECURITY OPERATIONS — CLICAR PARA VER EL VÍDEO

JAVIER HIJAS, CHECK POINT; MARIOLA DE LOPE, MICROSOFT Y VICENTE PÉREZ, VMWARE

TECNOLOGÍA CLOUD EN ESPAÑA, RETOS Y OPORTUNIDADES DE SEGURIDAD — CLICAR PARA VER EL VÍDEO

parte de una base de datos que comparten todos los productos de la compañía. “Por lo tanto para ser buenos en seguridad no sólo basta con tener buenos productos, sino también tener información, y gracias a ese enfoque que nosotros llamamos Infinity hoy en día tenemos los mejores datos”, decía Francisco Arcia.

De forma que con el apoyo de la arquitectura Infinity de Check Point, CloudGuard SaaS proporciona protección contra amenazas de quinta generación para aplicaciones SaaS, desde dondequiera que se acceda, a través de un solo panel.

Seguridad móvil, Check Point SandBlast

Más de la mitad del tráfico de internet está generado por dispositivos móviles. Ya en 2014 había más suscripciones a líneas móviles que a personas a nivel mundial. Cada día se envían por 65.000 millones de mensajes por WhatsApp. Está claro que el mundo es móvil y que las empresas empiezan a tomar medidas: en Estados Unidos el 50% de las compañías ya adoptaron el BYOD, han permitido a los empleados que utilicen sus móviles en los entornos laborales, y esta cifra se duplicará el próximo años. Para Francisco Arcia, Threat Prevention Sales Manager Iberia en Check Point, es ahí donde está el reto, no sólo en proteger el móvil

La Seguridad es Infinity

Ponencias CPX España 2018

ALBERTO MAESTRE, SOLUTION ARCHITECT DE TUFIN

CYBERTALK: INCREMENTAR LA AGILIDAD DE NEGOCIO, REDUCIR COSTES Y RIESGOS CON LA AUTOMATIZACIÓN

CLICAR PARA VER EL VÍDEO

ESTIBALIZ EGUIDAZU UGALDEA, BETSAIDE E IÑIGO VALLEJO, NEXTEL

BETSAIDE: UN CASO REAL DE TRANSFORMACIÓN EN ENTORNO INDUSTRIAL

CLICAR PARA VER EL VÍDEO

FRANCISCO ARCIA, THREAT PREVENTION SALES MANAGER IBERIA EN CHECK POINT

ÚLTIMAS AMENAZAS DE SEGURIDAD MÓVIL

CLICAR PARA VER EL VÍDEO

ANTONIO DELGADO, SENIOR SOLUTIONS ARCHITECT EN AWS

CYBERTALK AWS: AUTOMATION IS THE NEW BLACK, X BY ORANGE

CLICAR PARA VER EL VÍDEO

JAVIER CASTILLO, IP/SDN ARCHITECT EN X BY ORANGE

CYBERTALK ORANGE: AUTOMATION IS THE NEW BLACK, X BY ORANGE

CLICAR PARA VER EL VÍDEO

FRANCISCO ARCIA, THREAT PREVENTION SALES MANAGER IBERIA EN CHECK POINT

SECURIZANDO LAS APLICACIONES SAAS: UNA APROXIMACIÓN PRAGMÁTICA

CLICAR PARA VER EL VÍDEO

que te da la empresa sino de cómo hacer que el móvil personal, con el que muchas veces se accede a los recursos de la empresa, tenga la seguridad adecuada.

Decía el directivo durante el CPX España 2018 que seguimos pensando que es más importante proteger un portátil que un móvil, pero que este último es un vector que cada vez está siendo más atacado. “WannaCry no llegó a infectar más de un millón de portátiles y sin embargo todo el mundo lo conoce, mientras en el mundo móvil estamos viendo muestras de malware para móvil que han llegado a infectar 14 millones de terminales, como CopyCat”.

Estamos tan enfocados en proteger las redes, el endpoint, el cloud… que nos dejamos cosas tan importantes como es la seguridad en el móvil. Una solución antivirus no es suficiente porque ha de tenerse en cuenta la conexión a redes inalámbricas abiertas y la complicación que supone el poder comprobar que esa red pueda estar haciendo un ataque man in the middle. “Con SandBlast Mobile nuestro objetivo es entender qué está ocurriendo a nivel de conectividad en ese móvil, a nivel de wifi, a nivel de bluetooth, a nivel de aplicaciones”, aseguraba Francisco Acacia.

Check Point lleva trabajando más de tres años en un producto que se llama Sandblast Mobi-

Compartir en RRSS

le, donde tenemos módulos que protegen estos vectores. Vamos a ver conexiones, aplicaciones, qué hay en ese mensaje de WhatsApp. Bluetooth, WiFi, SMS… es una aplicación que tiene muy poco impacto en el dispositivo, tanto en el consumo de batería como de ancho de banda y que se integra con casi todos los MDMs del mercado

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.

Enlaces de interés...

- Check Point Infinitve
- Check Point SandBlast
- Check Mates
- Check Point CloudGuard SaaS
- Check Point Seguridad Cloud