Nueva ciberseguridad para nuevas amenazas

¿Te avisamos del próximo IT User?

Este es un documento producido por

www.ituser.es
www.itreseller.es

Accede a nuestras publicaciones digitales

CÓMO USAR ESTE DOCUMENTO

Con el fin de obtener la mejor experiencia de uso de esta revista, es **imprescindible** seguir estos sencillos pasos que te indicamos a continuación:

Paso 1. Asegúrate de disponer de las versiones más actualizadas de Adobe Reader y Flash Player. Si no las tienes instaladas, puedes descargarlas aquí:

Adobe Acrobat Reader y Adobe Flash Player

Paso 2. Accede al enlace de descarga y la publicación se abre en el visor del navegador.

Paso 3. Busca la opción guardar como que, dependiendo del navegador que utilices, podrá ser un icono o estar incluída en la barra de menú, y guarda la revista en la carpeta donde almacenes los documentos en tu equipo.

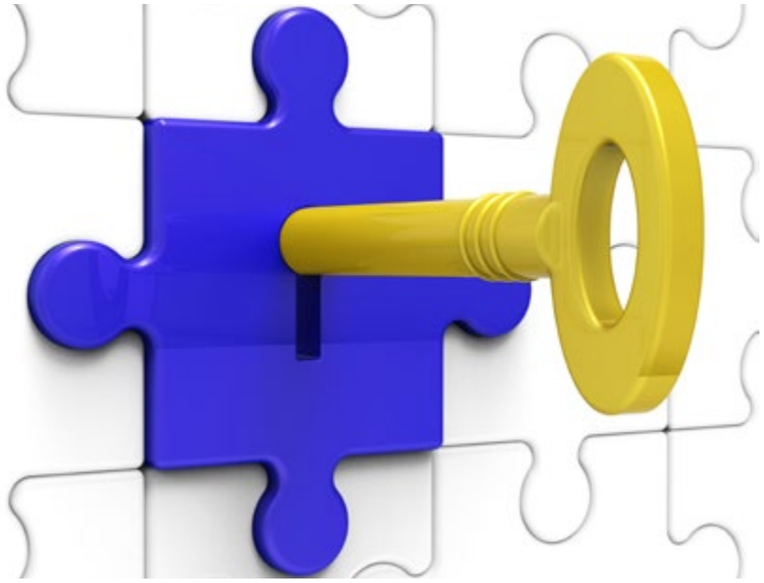
Paso 4. Accede a dicha carpeta y usa el botón derecho del ratón para hacer clic en el fichero de la revista.

Paso 5. Selecciona Adobe Reader como aplicación predeterminada para abrir este tipo de documentos.

Paso 6. Una vez abierta la revista, habilita la visualización a pantalla completa, y puedes iniciar la lectura de la revista con todas las capacidades interactivas disponibles.

Ciberseguridad
frente a las nuevas amenazas

Las amenazas han cambiado y, por tanto, la seguridad debe transformarse para dar respuesta a los nuevos retos a los que se enfrentan los negocios y los usuarios. Y este cambio debe basarse en la creación de una respuesta global y en la aplicación de inteligencia a cualquiera de los elementos que la componen.



Los smartphones y tabletas ofrecen acceso sin precedentes a la información crítica del negocio que necesitamos para trabajar con mayor rapidez y precisión. El poder ofrecer a los empleados acceso a toda esta información desde sus dispositivos móviles tiene muchas ventajas, pero también supone un riesgo para el negocio. Estos dispositivos y los sistemas empresariales en los que confía para administrarlos no pueden protegerlos frente a las amenazas móviles avanzadas. Como consecuencia, la información sensible, descargada y almacenada en los dispositivos, puede quedar vulnerable ante los ciberdelincuentes.

Las políticas estáticas, contenedores, PIN y contraseñas, ofrecen escasa protección frente a las sofisticadas ciberamenazas actuales, hasta el punto de que son incapaces de informar correctamente de cuándo se está produciendo un ataque. Una tecnología de detección de amenazas inteligente, como la de Check Point Mobile Threat Prevention, monitoriza más de un vector de ataque. Analiza todo un dispositivo al completo en su contexto, incluyendo su entorno, un componente clave de cualquier estrategia de seguridad móvil que se precie.

Su motor de riesgo de comportamientos (BRE - Behavioral Risk Engine), basado en la nube, aplica algoritmos propios, sandboxing y análisis estadísticos para detectar y establecer prioridades en las amenazas. Evalúa el comportamiento, metadatos y firmas de dispositivos, apps y redes, analizando cualquier violación o exploit en los sistemas operativos, roots y jailbreaks, así como configuraciones maliciosas para determinar el verdadero nivel de riesgo de un dispositivo. BRE emplea esta información para determinar las respuestas adecuadas que aseguren la protección de los datos y dispositivos hasta la eliminación de la amenaza. Toda esta inteligencia puede exportarse a otros sistemas de empresa para ampliar su valor y mejorar los tiempos de respuesta ante incidencias.

Análisis avanzado de apps

Un administrador puede confiar en sus empleados para que accedan a la información sensible de la empresa, ¿pero puede confiar de igual forma en sus apps?

Las políticas estáticas, contenedores, PIN y contraseñas, ofrecen escasa protección frente a las sofisticadas ciberamenazas actuales

Esta solución intercepta las apps al descargarse en los dispositivos, enviándolas al BRE para descompilarse y ser examinadas. Allí cada app se ejecuta en un entorno virtual basado en la nube para analizar el comportamiento antes de ser aprobada o marcarse como peligrosa, lo que evita su instalación en el dispositivo. Además, los informes de análisis, exportables y de fácil comprensión, proporcionan a los profesionales de seguridad la información que necesitan para asegurar que las apps que utilizan los empleados, tanto para el trabajo como para el ocio, son seguras.

Ataques basados en la red

Los lugares públicos suelen estar repletos de redes Wi-Fi abiertas, lo cual hace difícil saber qué redes son seguras y cuáles no. Los cibercriminales pueden servirse de estas redes para secuestrar smartphones y tabletas, asumiendo el control de los dispositivos y obteniendo valiosos datos como mensajes, archivos y credenciales de red. Esta solución detecta comportamientos y condiciones maliciosas de la red, desactivando automáticamente redes sospechosas para salvaguardar la seguridad de los dispositivos y los datos.

Al mismo tiempo, los ciberdelincuentes tratan de sondear los puntos débiles de seguridad antes de actuar. Esto incluye a menudo debilidades tanto de sistemas operativos como de apps, que otras soluciones de seguridad pueden no detectar. Check Point Mobile Threat Prevention analiza continuamente los dispositivos para descubrir vulnerabilidades y comportamientos utilizados por los cibercriminales para atacar a los dispositivos y robar la información. Con una mejor visibilidad de las amenazas a las que se enfrentan los dispositivos móviles, puede reducir su superficie de ataque general y su riesgo.

Respuesta dinámica a cada amenaza

Cada amenaza es diferente, por lo que es importante una reacción a medida si se quiere mantener la seguridad de dispositivos y datos. Check Point Mobile Threat Prevention ejecuta respuestas calculadas para amenazas conocidas y desconocidas, para impedir que los dispositivos comprometidos tengan acceso a las redes de la organización. Con la flexibilidad para crear políticas para diferentes umbrales, o para distintos individuos o grupos de usuarios, estará preparado para cumplir cualquier requisito.

Cuando se identifica una amenaza, la solución controla automáticamente cualquier riesgo hasta que se elimine la misma. Si puede eliminarse inmediatamente una amenaza en un dispositivo, se notifica a los usuarios y se pide aplicar una acción, como eliminar las apps maliciosas o desconectarse de redes hostiles. La integración con su MDM (Mobile Device Management) permite a la solución restringir el acceso al contenedor seguro, o aplicar en tiempo real, ajustes de políticas basados en riesgos en los dispositivos comprometidos, que los MDM no pueden aplicar por su cuenta. Check Point Mobile Threat Prevention puede también activar túneles VPN bajo demanda y preservar el tráfico de datos de los cibercriminales evitando la extracción de los datos mientras los usuarios siguen conectados.

Inteligencia integrada con los sistemas existentes

El análisis de amenazas genera un flujo de inteligencia en tiempo real sobre la estrategia de seguridad de los dispositivos móviles soportados, la cual puede alimentar sistemas de empresa existentes, como las plataformas de información de seguridad y gestión de eventos (SIEM). Esto incluye registros detallados y otros indicadores de compromiso, que pueden filtrarse para desencadenar acciones de respuesta, que ayuden al equipo de seguridad a aplicar correcciones rápidamente para controlar y neutralizar el riesgo.

Check Point SandBlast ZeroDay Protection usa una tecnología exclusiva que realiza la inspección a nivel de CPU para detener los ataques antes de que tengan oportunidad de iniciarse

Asimismo, se integra con los sistemas empresariales existentes para proporcionar sin esfuerzo seguridad avanzada para los dispositivos móviles. El diseño está pensado también para no resultar intrusivo, facilitando a los usuarios la posibilidad de mantener los datos del trabajo seguros sin tener que preocuparse de la privacidad.

Independientemente del número de dispositivos, integrar la solución con un MDM es rápido y sencillo. La implementación y gestión pueden efectuarse automáticamente, directamente desde el MDM, acelerando la adopción y reduciendo en su conjunto los costes operativos. La solución crece con el MDM, protegiendo a la perfección los dispositivos móviles que incorpora y eliminando las funciones de aquellos que elimina. El resultado es que puede descansar tranquilo sabiendo que dispone de las capas de seguridad necesarias, tanto para gestionar como para proteger dispositivos móviles, incluso en un entorno altamente dinámico.

Check Point Sandblast Zero-Day Protection

Se trata de una solución que detecta y bloquea malware no conocido, llevando la defensa contra amenazas a un nuevo nivel, dando una respuesta a otra de las tendencias en el mundo de la ciberseguridad.

Y es que la ciberguerra sigue en auge, y los cibercriminales modifican continuamente sus estrategias y técnicas para evitar ser detectados y conseguir sus objetivos. Dentro del ecosistema hacker de hoy en día, los ciberdelincuentes pueden compartir fácilmente código de exploits, vulnerabilidades identificadas recientemente e incluso el propio talento y conocimientos con sus cómplices. Incluso los ciberdelincuentes más novatos pueden aprovechar estos recursos para identificar vulnerabilidades y organizaciones susceptibles de ser atacadas, y crear fácilmente ataques de día cero desconocidos usando variantes personalizadas del malware ya existente.

Los antivirus, los cortafuegos de nueva generación (Next Generation Firewalls), y otras soluciones de seguridad se centran únicamente en las amenazas conocidas, aquellas que tienen ya firmas o perfiles bien conocidos. Pero cada hora aparecen 106 nuevas formas de malware, así que ¿cómo puede protegerse frente a algo que desconoce?

Las soluciones de sandbox tradicionales identifican malware “nuevo” que es desconocido, pero tardan en hacerlo, poniendo en serio riesgo la red frente a una infección antes de que se produzca su detección y bloqueo. Desgraciadamente, también son vulnerables a las técnicas de evasión, que son capaces de superar la tecnología de detección de los sandboxes tradicionales.

Frente a esto, Check Point SandBlast Zero-Day Protection emplea las funcionalidades de Threat Emulation y Threat Extraction para elevar la defensa frente a amenazas a un nuevo nivel, con la capacidad de detectar malware que utilice técnicas avanzadas de evasión y una protección completa contra los ataques más peligrosos, garantizando al mismo tiempo la entrega rápida de contenido seguro a sus usuarios.

Threat Emulation realiza una inspección en profundidad a nivel de CPU, deteniendo incluso los ataques más peligrosos antes de que el malware tenga una oportunidad para desplegarse y evitar la detección. SandBlast Threat Emulation usa la inspección a nivel de SO para analizar una gran variedad de tipos de archivos, incluyendo ejecutables y archivos de datos. Con estas fun-

ciones de inspección únicas, SandBlast Threat Emulation proporciona la mejor tasa de captura posible de amenazas, y es prácticamente inmune a las técnicas de evasión de los atacantes.

SandBlast Threat Extraction complementa esta solución entregando rápidamente contenido seguro, o versiones limpias y reconstruidas de archivos potencialmente maliciosos, manteniendo de esta forma el flujo de trabajo ininterrumpido. Gracias a la eliminación de los retrasos inaceptables que producen los sandboxes tradicionales, Threat Extraction hace posible la implementación de un sistema de prevención del mundo real, no solo generando alarmas, sino bloqueando el contenido malicioso para que nunca llegue a los usuarios. Check Point SandBlast Zero-Day Protection proporciona detección completa, inspección y protección frente a los peligrosos ataques dirigidos y de día cero.

Al contrario que otras soluciones, Check Point SandBlast ZeroDay Protection usa una tecnología exclusiva que realiza la inspección a nivel de CPU para detener los ataques antes de que tengan oportunidad de iniciarse.

Existen miles de vulnerabilidades y millones de implementaciones de malware, pero hay muy pocos métodos que los ciberdelincuentes utilizan para aprovechar estas vulnerabilidades. El motor de Check Point SandBlast Threat Emulation monitoriza el flujo de instrucciones de la CPU en busca de exploits que intenten superar los controles de seguridad del hardware y el sistema operativo.

Al detectar los intentos de aprovechar una vulnerabilidad en la etapa de pre-infección, el sandboxing de Check Point SandBlast Threat Emulation detiene los ataques antes de que tengan posibilidad de evadir la detección del sandbox.

Reconocer e identificar más amenazas

Check Point SandBlast Zero-Day Protection lleva a cabo una investigación más profunda con la emulación de amenazas a nivel de SO interceptando y filtrando los archivos entrantes y ejecutándolos en un entorno virtual. El comportamiento de los archivos es inspeccionado simultáneamente en múltiples sistemas operativos y versiones. Los archivos que aparecen involucrados en actividades sospechosas, habitualmente asociadas con el malware, como por ejemplo la modificación del registro, las conexiones de red y la creación de archivos nuevos, son marcados y analizados más en profundidad. De esta forma se evita que los archivos maliciosos penetren en su red.

Por cada archivo que se emula y resulta malicioso se genera un informe detallado. El informe, de fácil comprensión, incluye detalles del archivo e información sobre cualquier intento de actividad anormal o maliciosa originada al ejecutar el archivo. Además, proporciona capturas reales del entorno mientras se ejecuta el archivo en todos los sistemas operativos en los que se ejecute la simulación.

Ecosistema ThreatCloud

Las nuevas amenazas descubiertas se envían a la base de datos de inteligencia de ThreatCloud y se distribuye al ecosistema para proteger otros gateways de Check Point conectados. Esto permite que los gateways conectados puedan bloquear la nueva amenaza antes de que pueda extenderse. Esta colaboración constante hace de ThreatCloud la red de inteligencia contra amenazas más actualizada y avanzada disponible.

Facilidad de instalación

Check Point SandBlast Threat Extraction se instala como un Software Blade adicional en el gateway, y puede aplicarse en toda la organización o implementarse únicamente para personas, dominios o departamentos específicos. Los administradores pueden configurar los usuarios y grupos incluidos basándose en sus propias necesidades, facilitando de una forma sencilla su implementación gradual en la organización.

Check Point analiza el estado actual de la seguridad en Cyber Day 2016

Check Point Software Technology ha celebrado en Madrid la primera edición del Cyber Day, un evento que quiere convertir en una cita de referencia para el mundo de la seguridad. Aprovechando el marco de este evento, la firma ha dado a conocer una vulnerabilidad encontrada en Facebook Messenger.

De la mano de jugadores como IDC, INCIBE y empresas como Mapfre, Cepsa y Repsol, Check Point ha celebrado en Madrid Cyber Day 2016, un evento pensado para dar a conocer el momento que vive la seguridad. Y si una cosa ha quedado clara en este evento es que las amenazas para el entorno móvil son cada vez mayores y que las viejas apuestas para combatir el malware han quedado superadas.

José Antonio Lorenzo, director general de IDC España, fue el encargado de dar comienzo a las exposiciones con una ponencia titulada Estado de la Ciberseguridad en España. En ella, Lorenzo señalaba que la seguridad no es solo una cuestión del departamento de TI, “es una cuestión de todos”.

Mirando las prioridades de las empresas para este año, Lorenzo destaca que la primera es la seguridad y la protección, mientras que la tercera es el cumplimiento normativo. Asimismo, este responsable ponía sobre la mesa las principales tendencias en el mundo de la seguridad. La primera de ellas es la Transformación Digital, que debe ser empleada no sólo como motor del negocio, sino como motor de la seguridad; la segunda sería el cumplimiento normativo, algo que afecta a la totalidad de las empresas; la tercera, la necesidad de responder, no sólo a los clientes, sino ante las amenazas, en cualquier momento (24x7).

Un paso por delante de los ataques

Y sobre esta capacidad de respuesta, incluso antes de que se produzca el ataque, es sobre lo que habló Thierry Karsenti, vicepresidente técnico y de Nuevas Tecnologías de Check Point Europa, en una presentación que, bajo el título, One step ahead of cyberattacks, mostraba la necesidad de estar preparado ante ataques desconocidos, cada vez más frecuentes.

Tal y como mostró Karsenti, se van a invertir en seguridad empresarial en 2016 un total de 86.000 millones de dólares, cifra que podría elevarse a 101.000 millones

en 2018. Y eso en un contexto en el que el 72% de los CIOS creen que sus infraestructuras TI no están protegidas y son vulnerables a amenazas avanzadas y donde el 57% de las empresas carecen de las capacidades necesarias para bloquear ataques modernos.

“Se van a invertir en seguridad empresarial en 2016 un total de 86.000 millones de dólares, cifra que podría elevarse a 101.000 millones en 2018”

Thierry Karsenti, vicepresidente técnico y de Nuevas Tecnologías de Check Point Europa

Mario García, director general de Check Point para España y Portugal, repasa las claves de Cyber Day 2016 Clicar para ver el vídeo

Frente a esto, Check Point propone una seguridad basada en la aplicación de la inteligencia y en adelantarse y estar preparado ante posibles amenazas.

El punto de vista del cliente lo puso de manifiesto Javier Espasa, gerente de arquitectura de infraestructuras de Repsol, quien habló sobre cómo implementar la seguridad en el nuevo paradigma del centro de datos.

Sobre servicios para la ciberseguridad de las empresas habló Elena García, responsable de contenidos e investigación del INCIBE, que reconocía que, el económico es una de los motivos que explican el cibercrimen. De hecho, este cibercrimen representa el 8% del PBI mundial, aunque existen otros motivos como la notoriedad o el perjuicio de la imagen.

Por tanto, la seguridad debe verse como un motor generador de confianza.

Una movilidad segura, otra gran tendencia actual

La inseguridad en la movilidad fue el tema que centró la ponencia de Michael Shaulov, director de gestión de

“En movilidad la propuesta de Check Point pasa por una tecnología de detección de amenazas inteligente, como la de Check Point Mobile Threat Prevention”

aplicaciones en las tiendas móviles estén infectadas y, con ello, se infecten los dispositivos que las descarguen y ejecuten.

Frente a esto, la propuesta de Check Point pasa por una tecnología de detección de amenazas inteligente, como la de Check Point Mobile Threat Prevention, que monitoriza más de un vector de ataque. Analiza todo un dispositivo al completo en su contexto, incluyendo su entorno, un componente clave de cualquier estrategia de seguridad móvil que se precie.

Michael Shaulov, director de gestión de productos de movilidad de Check Point

productos de movilidad de Check Point. Este responsable desgranó las diferentes amenazas para los entornos móviles y cómo han evolucionado estas amenazas, incluyendo, entre otras, la posibilidad de que incluso

Eusebio Nieva, director técnico de Check Point analiza las últimas tendencias de amenazas y las tecnologías para combatirlas

Clicar para ver el vídeo

Mesa Redonda Cyber Day 2016: La amenaza del secuestro digital

El broche al Cyber Day 2016 organizado por Check Point fue una mesa redonda que, bajo el título La amenaza del secuestro digital, abordó las nuevas tendencias de seguridad en el mundo de la empresa actual.

La cita contó con la participación de Andrés Peral Plaza, director de Seguridad en Sistemas de Información de Mapfre; Rafael Hernández, responsable de Seguridad de Sistemas de Información, CISO Infraestructuras Críticas de CEPSA; Galo Montes, services line manager de Hewlett Packard Enterprise; y Juantxu Mateos, director de desarrollo de negocio de Nextel, moderados por José Antonio Lorenzo, director general de IDC España.

El encargado de romper el hielo fue Andrés Peral, que comentaba que la seguridad "es algo integral que debe hacer frente a las amenazas del mundo lógico y el mundo físico".

"La seguridad no puede depender solo del departamento de seguridad"

Andrés Peral Plaza, Mapfre

Rafael Hernández destacaba que la seguridad "es un servicio para dar soporte al negocio. Buscando siempre la máxima seguridad, tanto lógica como física, tratamos de ser un facilitador", y recordaba que la securización no puede ser la misma que para un castillo, "tenemos que facilitar el acceso de la forma más eficiente".

"El eslabón más débil de la cadena es el usuario final"

Rafael Hernández, CEPSA

“Es necesario evaluar cómo transformarse de forma segura”

Galo Montes, Hewlett Packard Enterprise

Para Peral, “en la relación entre algo seguro y algo que se puede hacer, intentamos enfocarnos hacia las amenazas y dejar claros los riesgos, pero sin olvidar que es necesario hacer negocios de forma segura, cumpliendo con las normativas”.

Y es que, como señala Rafael Hernández, “sea donde sea, tenemos que dejar claro lo que se puede y lo que no se puede hacer”.

Galo Montes reconocía que “los clientes se están transformando a gran velocidad”, lo que genera “un escenario de incertidumbre donde es necesario evaluar cómo transformarse de forma segura”.

Juantxu Mateos, por su parte, destacaba que “no podemos banalizar la seguridad, sobre todo cuando cualquiera puede acceder al Hacking as a Service, y solo es una cuestión de dinero”. De ahí que la propuesta de su empresa pase por “aportar, con inteligencia, un valor más allá de las herramientas, buscando ofrecer soluciones en tiempo real”.

Diversidad en el cliente

Tanto Galo Montes como Juantxu Mateos coinciden al afirmar que hay dos tipos de clientes, los de la gran cuenta, que sí están “a la última” en seguridad, y las empresas de menor tamaño y recursos, donde todavía hay mucho que hacer. Eso sí, tal y como resume Mateos, “estamos avanzando, pero la seguridad al 100% no existe”.

Por otra parte, Andrés Peral destaca que IoT es una oportunidad, pero tiene sus retos. Por la LOPD, “la seguridad debe estar presente en cualquier iniciativa desde el primer momento. Siempre tiene que estar seguridad trabajando con negocio”.

“Estamos avanzando, pero la seguridad al 100% no existe”

Juantxu Mateos, Nextel

De una opinión similar es Rafael Hernández, que destaca que “el abanico de soluciones que tenemos que cubrir es muy amplio, con soluciones que han llegado para quedarse, como las de movilidad o las de cloud computing. Los entornos son, cada día, más volátiles”.

Para ello, Peral afirma que “tenemos que usar en la seguridad lógica algunos paradigmas que han funcionado en la seguridad física”, pero recalca que la seguridad “no puede depender solo del departamento de seguridad”.

Recuerda para finalizar Hernández que “el eslabón más débil de la cadena es el usuario final”, y añade que, “por mucha labor de concienciación que realices, siempre hay un porcentaje de usuarios al que no vas a alcanzar”.

Enlaces relacionados

- Movilidad (Mobile Threat Prevention)
- APT (SandBlast)