Departamento de Seguridad Informática MINSAP

Julio 2017

Volumen 1, nº 1

Boletín de Seguridad Informática

Contenido:

Puntos de interés especial:

-El mercado de seguros ha estimado que las pérdidas que podría causar un ciberataque a nivel mundial estarían entre los 53.100 millones y los 121.400 millones de dólares.

-**BackBox Linux** es una distribución basada en Ubuntu a la que se han añadido un gran número de paquetes y aplicaciones relacionadas con la seguridad informática

-Windows cuenta con una serie de funciones de monitorización, control y **auditorías** que registran absolutamente todo lo que ocurre en el equipo

Un ciberataque a nivel mundial podría causar pérdidas de 53.100 millones de dólares

Casos como los de WannaCry y NotPetya han despertado la preocupación de muchas empresas e instituciones en torno a la ciberseguridad. Cada vez estamos más interconectados a través de Internet, y eso supone más posibilidades de recibir un cibertaque o bien dar medios para realizar uno, como por ejemplo los necesarios para la creación de una botnet.

Con la ciberseguridad en primer plano debido a la cada vez mayor capacidad de los cibercriminales y hackers para lanzar potentes ataques, el mercado de seguros británico **Lloyd's of London** ha publicado un informe que intenta predecir las pérdidas máximas que puede ocasionar un potente ciberataque.

El mercado de seguros ha estimado que **las pérdidas que podría causar un ciberataque a nivel mundial estarían entre los 53.100 millones y los 121.400 millones de dólares**. Este daño, debido a que está totalmente basado en software, sería puramente económico, a pesar de que las cuantías parecen más bien propias de un desastre natural.

Para estimar esas cuantías tan elevadas, Lloyd's ha planteado dos posibles escenarios de ataques:

-Ataque hacker contra un proveedor de servicios en la nube: La nube está concentrando cada vez más secciones y departamentos de las empresas. Un ataque contra un proveedor de servicios en la nube podría ser llevado por activistas que podrían realizar una modificación maliciosa de un hypervisor que controla la infraestructura cloud. En caso de realizarse contra servidores cloud utilizados por empresas, el servicio acabaría interrumpido y se forzaría a detener la actividad, generando así

pérdidas.

-El segundo escenario sería **algo muy parecido a lo visto a través de WannaCry**. Windows es un sistema operativo muy utilizado, por lo que una vulnerabilidad grave que le afecte podría causar grandes daños a las empresas en caso de ser explotada. Los informes sobre las vulnerabilidades que afectan a los sistemas operativos podrían ser vendidos a través de la dark web y acabar en menos de ciberdelincuentes que crearían exploits y diseñarían ataques específicos contra empresas vulnerables para obtener un beneficio económico.

Lloyd's ha calculado las posibles pérdidas para cada uno de los posibles escenarios. Para el primero ha estimado unas cuantías que van desde los 4.600 millones hasta los 53.100 millones de dólares, mientras que para el segundo ha estimado unas posibles pérdidas de entre 9.700 millones y 28.700 millones de dólares.

Los expertos de Lloyd's dejan entrever en su informe que es muy difícil estimar las posibles pérdidas económicas causadas por un ciberataque de grandes dimensiones, ya que por un lado dicen que **las cuantías podrían ser mucho menores si se toman todas las precauciones necesarias**, sin embargo, por otro dicen que en un caso extremo de interrupción de los servicios cloud las pérdidas podrían ascender hasta los 121.400 millones de dólares.

Sobre ataques que ya se han producido, Cyence ha estimado que WannayCry ha podido provocar unos 8.000 millones de dólares en total, mientras que NotPetya habría causado daños que ascenderían a 850 millones.

BackBox Linux 5, disponible la nueva versión de esta distribución de hacking ético

En los últimos años han ganado una gran popularidad las distribuciones Linux para hacking ético y auditorías de seguridad. Este tipo de distribuciones suelen contar con una serie de aplicaciones, paquetes y configuraciones específicos de manera que puedan utilizarse para auditar la seguridad de todo tipo de sistemas y redes. Existen muchas distribuciones para hacking ético, aunque una de las más conocidas es BackBox Linux.

BackBox Linux es una distribución basada en Ubuntu a la que se han añadido un gran número de paquetes y aplicaciones relacionadas con la seguridad informática de manera que los usuarios puedan tener un sistema Linux rápido, fiable y muy sencillo de usar para poder auditar sistemas y redes sin tener que preocuparse de nada más.

A lo largo de este fin de semana, los responsables de esta distribución han lanzado una nueva versión de la misma, **BackBox Linux 5**, una versión que, aunque a simple vista no trae grandes cambios y novedades, sí se trata de una actualización necesaria para que esta distribución pueda seguir creciendo y ganándose la confianza de los usuarios.

Novedades de BackBox Linux 5

La verdad es que esta versión ha tardado bastante en llegar, tal como aseguran sus responsables, por una serie de problemas que se han encontrado durante el proceso de desarrollo, pero finalmente ya está aquí.

El primer cambio visible que podemos encontrar en ella es que BackBox ahora cuenta con **un nuevo logo y una nueva identidad** que demuestra cómo los responsables de este proyecto quieren tomarse en serio su crecimiento.

Además de este cambio, esta nueva versión está basada en Ubuntu 16.04.2 LTS e incorpora en su interior la última versión del **Kernel Linux 4.8**, con todos sus parches de mantenimiento y seguridad y otras mejoras desarrolladas por Canonical para Ubuntu, como, por ejemplo, una serie de mejoras en los gráficos y en el rendimiento general de Ubuntu (y, por lo tanto, de BackBox). Además, los responsables también han **actualizado todas las herramientas de hacking** a sus versiones más recientes de manera que los usuarios puedan tener a mano las últimas versiones de sus herramientas listas para utilizar.

El nuevo BackBox Linux 5 es compatible con procesadores de 32 y 64 bits y necesita para funcionar tan solo 1 GB de memoria RAM y 10 GB de espacio de almacenamiento en el disco duro y una gráfica capaz de procesar imágenes a una resolución de 800×600. El sistema operativo puede instalarse tanto desde un DVD como desde una memoria USB.

Cómo ver quién inicia sesión en Windows 10 y cuándo lo hace.

La principal forma de proteger los datos de nuestro sistema operativo es mediante el bloqueo de inicio de sesión. De esta forma, para poder utilizar nuestro ordenador será necesario iniciar sesión en él con nuestro usuario y nuestra contraseña, sin embargo, esto abre la puerta a que otros usuarios también puedan hacerlo, o intentarlo al menos, y, por defecto, Windows no nos permite saber si alguien ha

intentado iniciar sesión en el equipo, si lo ha conseguido ni cuándo lo ha hecho.

Windows cuenta con una serie de funciones de monitorización, control y **auditorías** que registran absolutamente todo lo que ocurre en el equipo, desde errores en el software hasta problemas de seguridad. Como no podía ser menos, Windows también cuenta con una opción que nos va a permitir **registrar todos los inicios de sesión que se realizan en nuestro sistema operativo**, sin embargo, esta opción viene desactivada por defecto, por lo que para poder utilizarla lo primero que debemos hacer es activar esta auditoría.

A continuación, os vamos a explicar cómo indicar a Windows que guarde los registros de inicio de error de inicio de sesión y cómo ver todos estos valores desde el visor de eventos del sistema operativo. Antes de empezar queremos indicar que, al tener que utilizar las directivas de grupo de Windows, **este truco solo funcionará en las versiones "Pro"** de Windows y no en las "Home".

Cómo habilitar el registro de inicios de sesión en Windows 10

Para que Windows guarde un registro de los inicios de sesión que se realizan en el sistema operativo, lo primero que debemos hacer es habilitar dicha característica. Para ello, lo primero que debemos hacer es escribir en Cortana "**gpedit.msc**" para abrir la ventana de directivas de grupo y, allí, desplazarnos hasta el directorio:

- Configuración del equipo > Configuración de Windows > Configuración de seguridad > Directivas locales > Directiva de auditoría

Y, una vez allí, localizamos la opción "**Auditar eventos de inicio de sesión**".

Hacemos doble clic sobre esta directiva y nos aseguramos de marcar las dos opciones que aparecen en el programa para poder registrar todos los intentos de inicio de sesión, incluso los erróneos.

Una vez marcadas estas opciones ya podemos cerrar las directivas de grupo ya que Windows empezará a controlar esta opción.

Cómo ver todos los inicios de sesión en Windows 10

Todos los intentos de inicio de sesión, tengan éxito o no, quedarán registrados en el visor de eventos de Windows. Por ello, para poder verlos todos ellos, el siguiente paso será buscar en Cortana "Visor de eventos" y abrir la aplicación que nos aparece.

Una vez en ella, nos desplazamos hasta la ruta "**Registros de Windows > Seguridad**" donde veremos todos los registros relacionados con la seguridad de nuestro sistema operativo.

Como Windows guarda un montón de registros dentro de esta categoría, el que nos interesa a nosotros, el de inicio de sesión, podemos encontrarlo fácilmente por su ID, que será 4624. Una vez localizado el evento podemos verlo en detalle haciendo doble clic sobre él.

Gracias a esta función vamos a poder tener nuestro sistema operativo siempre controlado ya que, con una simple vista, vamos a poder ver quién ha intentado iniciar sesión en el ordenador, cuándo lo ha hecho y si lo ha conseguido con éxito o, de lo contrario, no ha podido al equivocarse con la contraseña.

Firefox Focus 1.1, el navegador privado para Android se actualiza con interesantes novedades

Cada vez utilizamos más nuestros dispositivos móviles para conectarnos a Internet. Igual que cuando navegamos desde un ordenador, cuando lo hacemos desde dispositivos móviles existen distintos scripts que intentan identificarnos y seguirnos por la red, reduciendo al mínimo nuestra privacidad. Por suerte, algunas desarrolladoras, como Mozilla, se preocupan realmente por la privacidad de los usuarios, y una muestra de ello es Firefox Focus.

Firefox Focus es un navegador desarrollado por Mozilla centrado principalmente en mejorar la seguridad y la privacidad de los usuarios que se conectan a Internet desde dispositivos Android. El funcionamiento de este navegador es muy simple, y es que, a diferencia de las versiones estándar de otros navegadores como Firefox o Google Chrome, Focus se centra en navegar, borrar todos los datos generados, y volver a navegar en una sesión limpia.

Este navegador, además, cuenta con una serie de **funciones especialmente diseñadas para preservar la privacidad** de los usuarios tales como **Private Browsing y Firefox Tracking Protection**, bloquea cierto contenido que puede resultar perjudicial e impide que las cookies de sesión se guarden en el dispositivo.

Con el fin de hacer de Firefox Focus un navegador un poco más práctico a la vez que mantiene su elevada privacidad, Mozilla acaba de lanzar la **versión 1.1**, una versión que trae una serie de interesantes cambios y novedades muy interesantes para los usuarios.

Novedades de Firefox Focus 1.1

En total, el nuevo Firefox Focus 1.1 ha llegado con 3 grandes novedades importantes para este sistema operativo. Además de las típicas correcciones de errores de todas las aplicaciones que se actualizan, la primera de ellas es la posibilidad de **reproducir vídeo en**

pantalla completa, mejorando así las capacidades de este navegador a la hora de reproducir este tipo de contenido en plataformas como, por ejemplo, YouTube. En segundo lugar, otra de las novedades se encuentra en las **notificaciones** del navegador que, en vez de ser solo informativas, ahora son interactivas y nos permiten trabajar con ellas.

Por último, y probablemente la novedad más importante, es que ahora **Firefox Focus soporta la descarga de cualquier tipo de archivo**, pudiendo utilizar ahora este navegador para descargar cualquier tipo de fichero desde Internet directamente a nuestro smartphone.

Ya puedes descargar el nuevo Firefox Focus 1.1

Esta nueva versión ya se encuentra disponible para todos los usuarios a través de la Play Store, y podemos descargarla en nuestro dispositivo desde el siguiente complemento. Si aún no aparece en la Play Store la nueva versión, también podemos descargarla directamente desde GitHub.

Como podemos ver, una actualización muy interesante que dota de mayor funcionalidad a este navegador web que no debe faltar en los dispositivos de todos aquellos usuarios que realmente se preocupan por su privacidad. Mozilla se está tomando en serio el desarrollo de su navegador web y, sin lugar a dudas, en las próximas semanas, a medida que la compañía vaya actualizando su navegador, seguramente podamos ir viendo nuevas e interesantes características que solo le harán seguir ganando popularidad y ganándose la confianza de la comunidad.

Las funciones, responsabilidades y obligaciones del Especialista de Seguridad Informática son:

- Organizar y controlar la actividad de seguridad informática.
- Evaluar el estado de cumplimiento y aplicación de la base legal vigente en la materia.
- Proponer medidas ante violaciones de la base legal vigente establecida en la materia.
- Controlar que se implemente y cumplan las medidas de seguridad informática que se establece en el Plan, informando de las violaciones por escrito al Jefe de Departamento de Seguridad y Protección.
- Mantener actualizado el Plan de Seguridad Informática y elaborar los procedimientos indispensables para garantizar la seguridad de los sistemas informáticos en uso en la entidad.
- Apoyar el trabajo de la Dirección, en cuanto al estudio y aplicación del Sistema de Seguridad Informática establecido, valorando permanentemente su efectividad y proponiendo las modificaciones que se requieran ante el surgimiento de nuevas amenazas o la variación de la probabilidad de ocurrencias de algunas de las existentes.
- Planificar, coordinar y participar en las inspecciones y auditorías a la seguridad informática
- Habilitar y llevar los registros que se indican en el Sistema de Medidas y aplicar los procedimientos que se incluyen como parte de este Plan de Seguridad Informática.
- Velar porque se apliquen los productos de protección actualizados y certificados.
- Establecer el chequeo previo y posterior de todo soporte informático que participe en eventos, ferias, exposiciones u otras actividades similares de carácter nacional e internacional, con el objetivo de evitar la posible propagación de algún virus informático o programa maligno y sus consecuencias.
- Registrar los virus o programas malignos que aparezcan en la Entidad y tratar de determinar quienes los introducen y cómo, sea de forma intencional o no.
- Someter todo nuevo software al proceso de cuarentena que se detalla en el Sistema de Medidas.
- Implementar el control a la resolución 127/2007.
- Implementar el plan de medidas para enfrentar y prevenir violaciones de seguridad informática.
- Controlar que el plan de seguridad informática este elaborado por la nueva metodología.
- Implementar el procedimiento para el control a las cuentas de informed y multipop.