Internet y nuevas tecnologías

Roberto Plá
Teniente coronel de Aviación
http://robertopla.net/

SEGURIDAD

XII JORNADAS DE SEGURIDAD DE LA INFORMACION EN DEFENSA

Como otros años, han tenido lugar en Madrid a mediados de abril, las Jornadas de Seguridad de la Información organizadas por el Ministerio de defensa y que este año alcanzaron su edición número doce.

Esta actuación, que pone el acento en la seguridad en el campo de las tecnologías de la información (TIC), representa una importante inversión enfocada a la formación de una adecuada conciencia de seguridad entre los profesionales que prestan sus servicios en el Ministerio y es la excusa perfecta para la convivencia y mutuo conocimiento entre profesionales de reconocido prestigio en el campo de la seguridad informática.

La edición del año 2013 se ha articulado como en otras ocasiones en sesiones de mañana y talleres por la tarde durante cuatro días, de los cuales dos estaban reservados para profesionales del Ministerio y los otros dos de libre acceso para profesionales del sector y personal interesado.

En ellas se han desarrollado charlas sobre las consecuencias derivadas de la aparición y persistencia de amenazas y riesgos por medio de ciberataques, presentando las novedades e iniciativas que en el campo de la ciberdefensa militar se están adoptando centrándose, por una parte en la ampliación del escenario y del campo de actuación de la seguridad CIS, desde un punto de vista tecnológico, organizativo y jurídico, y por otra de la seguridad de la información en su modelo más tradicional.

Cabe destacar el interesantísimo taller programado para la primera jornada sobre "Técnicas de *hacking* en Ciberdefensa" coordinado por los representantes del EMACON.

El ministerio valoró muy positivamente la inestimable colaboración de importantes empresas del sector que ha permitido aumentar la oferta de mesas redondas.

http://delicious.com/rpla/raa824a

INTELIGENCIA

MANUAL DE ESPIONAJE EN INTERNET

Uno de los medios de obtención de inteligencia son las llamadas fuentes abiertas. Se trata de información que está ahí, al alcance de cualquiera, en publicaciones comerciales o a veces incluso gratuitas, en información comercial o en noticias de prensa, publicada por gobiernos, por ONG o por los departamentos de estadística de instituciones y organizaciones diversas.

El adecuado análisis de esta información es lo que produce la Inteligencia de fuentes abiertas, OSINT en sus siglas inglesas. La CIA reconoce que el 85% de la información que procesa procede de fuentes abiertas.

Hoy en día Internet es la mayor fuente de datos abiertos. Y existe una interesante colección de documentos que explican cómo buscar y recopilar estos datos. La mayor parte de estos datos corresponden a información que antes se publicaba en papel y hoy podemos tener en nuestra mesa a través de la pantalla del ordenador. Lo más interesante de la red es que además de los datos 'evidentes', contiene otros datos que incluso su propietario no es consciente de que están prácticamente a disposición pública. Las páginas *web* muestran una información a través de un navegador, pero su código puede encerrar otro tipo de datos, como el nombre del autor o el *software* con el que fue creado. Este tipo de informacion también puede buscarse a través de Google, y existen libros como Google Hacks (Tara Calishain y Rael Dornfest, O'Relly, 2003) que explican como exprimir Google hasta el último dato, utilizando las herramientas que el propio Google nos proporciona, o los despistes de los usuario y autores de la información, que pueden dejar archivos en lugares a los que no creen que llega el buscador o con datos que no creen que vayan a ser leídos por el mismo. Resulta sorprendente como años después de la publicación de estas técnicas sigue siendo posible acceder a claves de acceso y otros datos sensibles simplemente usando las herramientas que proporciona Google.

Otras veces los servidores *web* que envían la información a través de la red y los navegadores que la reciben y presentan, pueden tener fallos que expongan información que en principio no iba destinada al usuario. Esto ocurre frecuentemente porque recursos, como las páginas de error, ofrecen demasiados datos sobre las interioridades del servidor. Esta información que en periodo de

desarrollo puede ser usada por los programadores para localizar rápidamente donde se ha producido el fallo, si no es retirada al ponerse la aplicación a disposición del público puede ser usada por visitantes curiosos para obtener pistas sobre vías de acceso a las partes que no deberían estar expuestas al publico. De nuevo la información sobre cómo explotar estas vulnerabilidades también podemos encontrarla en la red, quizás a través de la "Google Hacking Data Base" o de páginas y publicaciones en forma de manual con detalladas instrucciones.

Los servicios de inteligencia son más conscientes que nadie del inmenso tanque de pesca que supone internet y han sido los primeros en recopilar técnicas de rastreo y recogida de información. Recientemente se ha desclasificado un interesante documento elaborado para la Agencia Nacional de Seguridad de Estados Unidos (NSA) y que puede bajarse libremente de la red. Se trata de un tomo de 645 páginas y corresponde a la versión de 2007.

También existen otras herramientas, como el buscador Shodan especializado en la búsqueda de dispositivos conectados a la red, Shodan permite encontrar teléfonos móviles, frigoríficos, reactores nucleares o sistemas de regulación de tráfico si están conectados a internet.

En una ponencia presentada en la Defcon del año pasado, el experto en seguridad Dan Tentler demostró cómo se puede usar Shodan para encontrar sistemas de control de evaporadores industriales, calentadores de agua a presión, y puertas de garaje.

Creo que no es arriesgado afirmar que la mayoría de los incidentes de seguridad ocurren porque los recolectores de información saben más del sistema que su propio administrador o bien este es descuidado o perezoso. Para los espías laboriosos no faltan, ni oportunidades, ni técnicas para aprovecharlas fácilmente accesibles en la red.

http://delicious.com/rpla/raa824b

SOFTWARE

EL FIN DE WINDOWS XP

Víctima de una práctica que debería ser calificada como criminal, denominada 'obsolescencia programada' Windows XP verá su final en abril de 2014. Microsoft ha anunciado que a partir de esa fecha no ofrecerá actualizaciones de seguridad ni soporte para ese sistema operativo que hace muy poco ha dejado de ser el más usado, en beneficio de su hermano Windows 7.

A pesar de que Microsoft dice en su comunicado que la medida se adopta porque "un sistema operativo presentado hace más de diez años limita a las organizaciones el acceso a las ventajas que ofrece la tecnología de última generación", lo cierto es que puedo garantizar que las máquinas que uso con Windows XP funcionan perfectamente y satisfacen mis necesidades. ¿Por qué entonces me obligan a cambiar? Naturalmente, porque hay que dar de comer a las fábricas de *software*. La economía moderna se basa en el consumo y si las cosas duran demasiado, la engrasada máquina de hacer dinero tiene que frenar su avidez de ventas.

Hay que recordar que el sucesor de Windows XP no fue Windows 7 sino Windows Vista, uno de los fiascos más grandes de la empresa de Redmond, una pifia incluso mayor que Windows ME, una actualización que casi sólo aportaba nuevos fallos.

Naturalmente es poco probable que si instalamos Windows 7 o Windows 8 en la máquina que hasta ahora funcionaba perfectamente, lo siga haciendo con igual rendimiento. Es probable que necesitemos ampliar la memoria o directamente cambiar de ordenador. Y por eso precisamente, los fabricantes de ordenadores están encantados de suministrar sus máquinas nuevas con sistemas operativos que cada cierto tiempo "caducan": Ellos también quieren una parte del pastel.

Por mi parte como usuario prefiero que tantas ganancias no sean a mi costa, y esa es la principal razón por la que uso *software* libre: hace lo mismo, cuesta menos o directamente es gratis y me ofrece más opciones a la hora de gestionar mi parque de ordenadores.

Ovum, una prestigiosa empresa dedicada al análisis de decisiones corporativas ha publicado un estudio en el que ofrece tres posibles soluciones para bajarse de la rueda del consumo de sistemas operativos con fecha de caducidad que obliga a pasar por caja.

Las propuestas de OVUM son la virtualización del escritorio, es decir pasar de tener ordenadores independientes a usar terminales de un ordenador central, en el que se ejecutan las aplicaciones y residen los datos, lo que disminuye los costes de *hardware* y los de mantenimiento de aplicaciones. Otra opción similar es el uso de un sistema operativo basado en el navegador, como Chrome OS, y el acceso a las aplicaciones y los datos a través de las tecnologías propias de la web. Por último la propuesta quizás más atrevida es la de sustituir los ordenadores, especialmente los portátiles, por tabletas con sistema operativo Android que podrían realizar con eficacia las funciones requeridas por la mayor parte de los usuarios corporativos a un precio mucho menor.

Los gobiernos y las grandes corporaciones son conservadores a la hora de tomar decisiones que afecten a sus estructuras, pero en tiempos de crisis el factor económico puede ser determinante y un importante ahorro puede suponer un estímulo decisivo para explorar nuevos horizontes.

http://delicious.com/rpla/raa824c

Enlaces

Los enlaces relacionados con este artículo pueden encontrarse en las direcciones que figuran al final de cada texto