Internet y nuevas tecnologías

ROBERTO PLÁ
Teniente coronel de Aviación
http://robertopla.net/

SEGURIDAD

SEGURIDAD PARA DISPOSITIVOS MOVILES

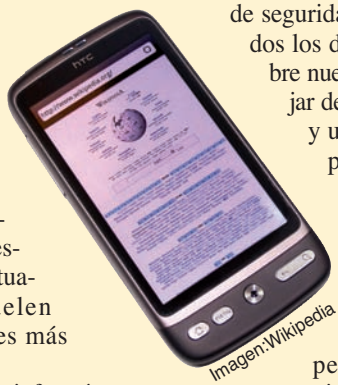
Imagen:Wikipedia

En deportes de riesgo, los peores accidentes suelen ocurrirles a los expertos. Los novatos suelen prestar mucha atención a las situaciones comunes y no suelen involucrarse en actividades más complejas.

En nuestra relación con la informática pueden pasar cosas muy parecidas. Cuando consideramos las normas de seguridad una rutina aburrida y exagerada, estamos creando una vulnerabilidad que puede llevarnos a ser víctimas de incursiones, robo de información, destrucción de datos o estafas y pérdidas económicas.

Para mantener a salvo nuestros dispositivos y nuestra información es tan importante crear hábitos saludables como mantenerse informado de los peligros que les acechan. Como ciudadanos particulares, nuestros datos pueden ser codiciados por ciberdelincuentes para suplantar nuestra identidad y enmascararse con ella para la realización de delitos, para privarnos de nuestro patrimonio o usar nuestros recursos y conexiones a la red para realizar acciones poco éticas o ilegales.

Como profesionales de la defensa, tenemos acceso a información y redes de comunicación que pueden ser codiciadas tanto por ciberdelincuentes como por potencias extranjeras. Como entre nuestras obligaciones se encuentra la de mantener reserva sobre los asuntos que conocemos por razón del servicio, la práctica de rutinas de seguridad que impidan la exposición de esta información a la que tenemos acceso, es una obligación reglamentaria cuyo incumplimiento puede llevarnos a numerosos quebraderos de cabeza.

El peor enemigo de la seguridad de la información es la falta de conciencia de los depositarios de la misma en materia de seguridad. A fuerza de ver todos los días datos sensibles sobre nuestra mesa podemos dejar de valorar la importancia y utilidad que puede tener para los curiosos del 'lado oscuro'. Cualquier dato puede ser interesante para componer la imagen de un escenario y facilitar pistas para perpetrar un acceso no autorizado a información quizás más relevante.

Los teléfonos y dispositivos móviles actuales pueden ser un arma con más valor para los curiosos indiscretos que la que tuvo el famoso caballo de los griegos en Troya.

Un teléfono o una tableta pueden recopilar información en forma de imágenes, mensajes, datos de posición, listas de direcciones o datos almacenados en el mismo como en cualquier otro ordenador, ya que un teléfono moderno es un potente y minúsculo ordenador y centro de comunicaciones.

Los ataques en forma de virus y *malware* a teléfonos móviles han aumentado y seguirán aumentando en los próximos tiempos, por la gran popularidad de estos aparatos y los beneficios que pueden proporcionar a los delincuentes.

Una aplicación maliciosa puede tener acceso a cualquiera de las funciones de nuestro móvil, a los datos almacenados en el mismo o a la redes a las que accedemos desde ese dispositivo, y reenviar esos datos al controlador de la aplicación que, de esta forma, podría espiar desde nuestros mensajes a nuestras fotos, seguir nuestros movimientos o espiar las contraseñas introducidas en nuestras cuentas al acceder a ellas desde el teléfono.

El Jefe de Seguridad de Datos de Stonesoft, una importante empresa de servicios informáticos, publica en la *web* de la compañía una serie de consejos para el uso seguro de dispositivos móviles. Me he permitido una versión propia corregida y ampliada. La lista queda expresada en estos doce puntos:

1. La primera norma de seguridad con un dispositivo móvil es no perderlo de vista. Al peligro de robo se suma la posibilidad de que un extraño haga un uso inadecuado de nuestro dispositivo o pueda acceder a la información que contiene.
2. Actualizar los programas y el sistema operativo del dispositivo móvil con regularidad. La actualización automática de aplicaciones puede ser una vulnerabilidad y debería ser desactivada para realizarse únicamente en redes de confianza.
3. Cuando se adquiere un nuevo dispositivo móvil, conviene elegir el que pueda usar la última versión del sistema operativo y de una marca con una política de actualizaciones adecuada, así la desactualización del sistema operativo no será un motivo de obsolescencia que nos obligue a cambiar de dispositivo.
4. Como en cualquier otro ordenador, hay que tener instalada y activa una versión actualizada de un programa antivirus de probada eficacia.
5. Solo instalar programas de fuentes confiables. Las tiendas electrónicas de aplicaciones en línea propias de cada marca puede que sean más caras, pero ofrecen la seguridad de realizar controles de seguridad de las aplicaciones que venden. Como en todo, cuidado con los chollos, podrían ser una fuente de *malware*.
6. Cuidado con los costes intra-aplicaciones. El uso de algunas aplicaciones puede acarrear gastos y otras pueden ofrecer la adquisición de ventajas en el


Imagen por digitpedia en Flickr

juego, personajes o características que implican un pago. Los niños especialmente pueden verse tentados de obtenerlos sin comprender bien su coste.

7. Controlar cuidadosamente los derechos que se otorgan a redes sociales o aplicaciones para hacer uso de nuestra información o de las características de nuestro dispositivo. Algunas aplicaciones pueden desvelar nuestras ubicación o las imágenes que subimos a determinadas redes pueden otorgar a otros derechos sobre ellas.

8. Usar claves de acceso seguras. Cambiar con frecuencia el código de acceso y el código PIN de la tarjeta SIM. Configure el dispositivo para que solicite la contraseña o un patrón secreto cada vez que se utilice.

9. Si el dispositivo admite el cifrado de datos, activar esta función.

10. Prever las circunstancias de pérdida o robo antes de que ocurran. Anotar a parte los números de teléfono o las acciones a realizar para obtener la localización de nuestro dispositivo en caso de robo, desactivar la cuenta de teléfono o borrar remotamente los datos. Actuar rápidamente.

11. Antes de desechar un equipo, devolverlo a la configuración de fábrica y realizar un borrado de seguridad de toda la información que contiene en la memoria, en las tarjetas SIM y las tarjetas de expansión.

12. Hacer copias de seguridad de todos los datos en su dispositivo móvil. Almacenarlos en un servicio de almacenamiento en linea (en "la nube") puede ser práctico, pero es menos seguro. No debe usarse este sistema para datos personales sensibles y jamás para datos de carácter profesional.

http://delicious.com/rpla/raa820a

CIBERGUERRA

LA PROXIMA GUERRA

El pasado año 2012 ha presenciado una consolidación del concepto de ciberguerra. Esta técnica se ha convertido en una realidad para las fuerzas armadas de las principales potencias mundiales que ya no dedican tímidos esfuerzos en la organización de equipos experimentales; crean mandos específicos en sus estructuras de fuerza, analizan la doctrina existente, se aprestan a dotarse de las armas

Imagen: Ministerio de Defensa

adecuadas y de los elementos de desarrollo de las mismas y definen perfiles de carrera para captar los recursos humanos indispensables y decisivos en esta guerra que está muy lejos de ser una guerra entre máquinas.

Ya nadie duda de que Stuxnet ha sido, tal y como lo define la editorial del número de "Air&Space Power Journal" dedicado a la ciberguerra, "el primer episodio de una nueva era en los anales de la guerra moderna". Un episodio que rápidamente se ha convertido en historia para dejar paso a la propagación de "miniFlame" el virus más preciso de los vistos hasta el momento, derivado en tan solo unas semanas del virus "Flame" detectado en mayo.

Estos virus no son ejercicios académicos o travesuras de estudiantes aburridos, tampoco son herramientas de ciberdelincuentes ávidos de desvalijar cuentas bancarias. Se trata de sofisticados sistemas de armas, vectores capaces de transportar armas de guerra sofisticadas y sorprendentemente especializadas que pueden ensamblarse con los recursos necesarios para cada misión en forma de módulos de infiltración, camuflaje, ataque, autodestrucción, encriptación....combinados según las necesidades de la operación y reutilizables o actualizables por sus operadores.

Permanecer impasibles ante esta escalada armamentística resulta impensable, pero limitarse al papel de meros observadores o aún al de usuarios de las herramientas desarrolladas por otros es simplemente, suicida.

La seguridad en el campo cibernético solo puede ser mantenida por el personal propio con ideas propias y desarrollos autónomos. En un tablero donde se lucha con las ideas, pretender usar las de otros es simple vasallaje y una dejación de soberanía.

La buena noticia es que la ventaja en este campo no está supeditada a la disposición de grandes recursos económicos. Esto puede ser incómodo para los poderosos, que preferirían mantener la ventaja que les otorga su riqueza material. Contra las reglas que han regido la guerra y las relaciones internacionales en el transcurso de la historia, la "Tierra Corazón" no es de acceso exclusivo a los ricos; los medios materiales ceden en importancia ante una doctrina y unos recursos humanos, con mayor incidencia en su calidad que en su cantidad.

¿Sabremos elegir y motivar a nuestros jóvenes más capacitados para dirigir nuestra defensa?, ¿Sabremos liberarnos de la costumbre que lleva a todo ejército a preparar la guerra anterior en lugar de la siguiente?. El pensamiento y la capacidad de reacción deben moverse a una velocidad acorde con la naturaleza del campo de trabajo. Si "cada uno piensa a la velocidad a la que se mueve", en la guerra cibernética hay que moverse a la velocidad de la luz. Esto implica que incluso estas mismas palabras, cuando sean impresas en la Revista de Aeronáutica y Astronáutica ya estarán algo obsoletas; confiemos en que más que a meditar sobre el pasado o el presente irremediable, se lean como una invitación a interpretar el futuro según nuestra propia determinación.

http://delicious.com/rpla/raa820b

Enlaces

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