Internet y nuevas tecnologías

Roberto Plá
Coronel de Aviación
http://robertopla.net/

SEGURIDAD

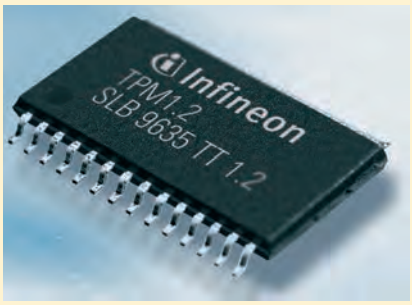
ENCRIPTAR O NO ENCRIPTAR

En el imaginario colectivo, la agencia de seguridad nacional norteamericana (NSA) se ha convertido en la versión real del "Gran Hermano" imaginado por Orwell. Los largos tentáculos de omnipresente escrutador se extienden a través de la red, accediendo a los registros de nuestras redes sociales, a la información almacenada en la nube o a nuestras conversaciones por mensajería o correo electrónico. Podríamos pensar que nuestro disco duro, el del ordenador de nuestra casa, está a salvo. Pero para estar seguros de ello, tenemos la posibilidad de cifrar nuestros datos. El disco completo. Al cambio solo perderemos un poco de la capacidad de proceso de nuestra máquina, ya que cada operación de acceso o grabación de información en el disco requerirá una operación previa de descifrado o cifrado.

Hay utilidades de software libre que nos permiten realizar esa operación, pero las versiones profesionales de Windows disponen de una herramienta que permite encriptar un disco o partición enterita de una forma más o menos transparente para el usuario. Hay dos pesadillas que persiguen a los usuarios que encriptan sus datos. Una de ellas es que se pierda la clave que protege sus datos y la otra que el cifrado sea ineficaz y sus secretos sean examinados por extraños.

En el primer caso, se recomienda leer atentamente el manual. El gran secreto es tener la clave que Bitlocker crea cuando se encripta el disco. Esta clave de 48 dígitos debe ser guardada celosamente. Su olvido puede acarrear una pérdida de datos. Por ejemplo, si falla el sistema operativo y hay que reinstalarlo, el setup no permitirá hacerlo en un disco cifrado con Bitlocker si no disponemos de la clave.

En el segundo caso, es posible que hayamos oído historias sobre vulnerabilidades de los programas de encriptado. Fallos de programación que permiten a los hackers curiosos examinar nuestros preciados datos. Aunque Bitlocker es software propietario y por tanto su código es secreto y no puede ser examinado, hasta el momento las vulnerabilidades que se conocen requieren tener acceso físico al ordenador y que este haya permanecido encendido después de introducir la clave de descifrado. Programas especiales rebuscan en la memoria del ordenador para encontrar el rincón donde guardó la clave. Pero como comentaba un bloguero: "si cogemos a una persona y le obligamos a decirnos la combinación de la caja fuerte, no parece que la culpa sea del fabricante de la caja fuerte".



Por eso se aconseja apagar completamente los ordenadores después de usarlos en lugar de dejarlos simplemente 'hibernando' y también usar sistemas de seguridad de doble llave, donde además de la clave sea necesario introducir una tarjeta inteligente o una memoria USB para desbloquear el ordenador.

Aun así, se sabe que el FBI presionó a Microsoft en 2005 para que introdujera una puerta trasera por la que las fuerzas de la Ley pudieran entrar en los secretos de los presuntos criminales. "Se dice" que no cedió. En el estado de la Ley actual en Estados Unidos, si Microsoft conoce la forma o dispone de un método para romper el cifrado de Bitlocker, a petición de la policía debería proporcionarlo.

Entre las revelaciones del antiguo analista de la CIA, esa agencia estaba muy interesada en Bitlocker y su apoyo en el chip TPM que 'vigila' los cambios de configuración en un ordenador previniendo la instalación de malware avisando al programa de cifrado de cualquier cambio sospechoso, con lo que el descifrado del disco no se efectuaría.

¿Tuvieron éxito? Si lo supiéramos, ya no sería un secreto. Microsoft no hace comentarios al respecto.

Entonces, aunque esté cifrado, ¿Puede leer el "Gran Hermano" nuestro disco duro? No se sabe, pero en cualquier caso, cifrar o no cifrar, es su decisión.

http://delicious.com/rpla/raa849a

CIBERGUERRA

UN PASO ADELANTE

Recientemente se ha producido una esperada noticia: el Ejército del Aire

ha puesto en marcha su Centro de Operaciones de Seguridad de Ciberdefensa (COS-EA). Aunque no alcanzará su capacidad operativa final hasta finales de septiembre de 2016, supone un importante hito en la incorporación de nuestro ejército a la forma de guerra más moderna y a la asunción de unas capacidades que son ya vitales y decisivas para cualquier potencia.

Encuadrado en la Dirección de Ciberdefensa de la JSTCIS (Jefatura de Servicios Técnicos y de Sistemas de Información y Telecomunicaciones) del Ejército del Aire, está ubicado en el Cuartel General del Ejército del Aire. Mantiene, además, una relación funcional con el Equipo de Respuesta ante Emergencias Cibernéticas (CERT) del Ministerio de Defensa.

Un CERT (del inglés Computer Emergency Response Team) es un centro de respuesta a incidentes de seguridad en tecnologías de la información. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. Un CERT estudia el estado de seguridad global de redes y ordenadores y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, publica alertas relativas a amenazas y vulnerabilidades y ofrece información que ayude a mejorar la seguridad de estos sistemas.

Cuando hablamos de defensa aérea, terrestre o naval, resulta relativamente fácil visualizar el esfuerzo que representa un despliegue de medios materiales, de infraestructuras y sensores. Comprender las actividades de la ciberdefensa no siempre es fácil porque con frecuencia se mueven en ámbitos lógicos, en el corazón de los sistemas de comunicaciones y las redes interconectadas, en lo que se ha dado en llamar “el mundo virtual” aunque en realidad es una parte de nuestro mundo real en el que se guarda nuestra información y se producen procesos lógicos que nos ayudan a controlar procesos y sistemas físicos.

El COS-EA realizará sus cometidos a través de la observación y control del tráfico de información y funcionamiento de los procesos en los sistemas de información mediante sofisticadas herramientas compuestas por aplicaciones y equipos específicos. Esta actividad permite detectar intentos de intrusión, puntos en los que se produce una situación vulnerable que podría constituir una puerta para un ataque y en caso de que este se produjera, tomar medidas para proteger los sistemas, neutralizar el ataque, analizar su origen, evaluar los daños si llegan a producirse, conseguir que los sistemas vuelvan a funcionar normalmente en el mínimo tiempo posible y analizar lo ocurrido para determinar sus causas y extraer enseñanzas para evitar el fallo o mejorar la respuesta al mismo en el futuro.

La ciberguerra tiene interesantes coincidencias con la guerra aérea, como la continuidad del medio, que en el caso de la ciberguerra hace aún menos relevante el terreno, aunque tiene una componente física importante en la topología de las redes y el uso del espectro electromagnético, la flexibilidad en el ataque y la respuesta, así como la capacidad de llevar la guerra hasta el corazón de la organización del adversario.

Sin duda alguna, si tuviéramos la ocasión de oír a Giulio Douhet analizando este nuevo ámbito de enfrentamiento nos diría con toda seguridad que "sin la superioridad cibernética es imposible obtener la victoria".

Necesitamos personal altamente cualificado, medios complejos y técnicamente sofisticados y sobre todo una doctrina que surja de un análisis inteligente del medio. Nuestros compañeros se han incorporado a esa tarea, pero necesitamos la ilusión, la sabiduría y el trabajo de muchos jóvenes que encuentren en la ciberdefensa, su vocación de servicio a España.

http://delicious.com/rpla/raa849b

TERRORISMO

COMUNICACIONES ALTERNATIVAS

Tras los criminales atentados producidos en Francia el pasado día 13 de noviembre, se produjeron varios arrestos en Bélgica. Al parecer una furgoneta con matrículas belgas había sido vista cerca de alguno de los lugares de los atentados.

Bélgica es el país europeo que más terroristas ‘per cápita’ ha aportado al DAESH, el grupo terrorista que se sospecha está tras los atentados. Según publicó la prensa, las detenciones han servido para confirmar a la policía que los terroristas utilizaban para comunicarse con la organización y entre ellos consolas Play Station 4 de la casa Sony.

Dias antes de los atentados el Ministro de Interior belga ya había hablado de la dificultad que suponía para los servicios de inteligencia occidentales interceptar y descifrar las comunicaciones realizadas a través de las mencionadas cónsolas. Se ha calificado como “más difícil de interceptar que WhatsApp”.

Todas las consolas modernas se conectan a internet y además de jugar a través de la red con otros jugadores, permiten conectarse con ellos, enviándoles mensajes de texto o hablando directamente cuando comparten una partida y están ‘agregados’ como amigos del usuario. El elevado número de jugadores sería una dificultad más para localizar conversaciones esporádicas entre sospechosos.

http://delicious.com/rpla/raa849c

Enlaces

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