Internet y nuevas tecnologías

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

INTERNET

INTERNET DE LAS COSAS

Uno de los conceptos más repetidos en los foros tecnológicos es el del "Internet de las cosas". Se refiere al conjunto de dispositivos cotidianos a los que se ha dotado de un acceso a internet.

¿Qué utilidad puede tener esto?, enseguida se menciona el frigorífico o el horno conectados a internet, y para la mayoría de las personas esta posibilidad es una auténtica quimera carente de utilidad, pero no podemos olvidar que hace muy poco pensábamos lo mismo de nuestros televisores y hoy estos electrodomésticos son sencillamente ordenadores con forma de pantalla plana.

Una de las principales ventajas de mantener conectado un electrodoméstico a internet es permitir que su programación interna pueda ser actualizada sin intervención del usuario ni visita física del técnico, pero quizás lo más interesante para el usuario puede ser acceder a la información que el elemento puede proporcionarle y controlar su funcionamiento. No solo encender la calefacción poco antes de ir a casa, sino contar los productos que tenemos en la despensa o el frigorífico, comprobar como avanza el guiso programado en la olla robot de cocina, ver quién está llamando a la puerta de casa cuando no estamos y conversar con el visitante, quizás un repartidor, para pedirle que deje el paquete que compramos por internet en casa del vecino.

Un buen número de utilidades pueden parecer auténticas estupideces, pero deberíamos ser conscientes de que las estupideces mueven mucho dinero en los mercados de la tecnología. Las mascotas tipo 'Tamagochi', o la maceta que pone un mensaje en Twitter cada vez que la riegan, pueden parecer usos triviales o prescindibles, pero atraen a un buen número de gente, se convierten en tendencias,... y toman su vía de acceso a la red a través de nuestra conexión doméstica o de la red de datos móvil a través de nuestro *smartphone*, o de la propia tarjeta de datos que algunos aparatos llevan incorporada.

Todas esas vías de comunicación pueden ser vías de entrada de intrusos. Esclusas que hay que proteger. Todo dispositivo dotado de un *software* que esté conectado a una red de comunicaciones es vulnerable. ¿Qué pasaría si a través del sistema de riego del jardín un asaltante pudiera acceder a nuestro router y desde allí a las cámaras de seguridad de la vivienda? O las fotos privadas de nuestro ordenador, o acceder al frigorífico que compra en el supermercado virtual cuando se nos acaba la leche y robar los datos de nuestra tarjeta de crédito, por no mencionar claves o documentos profesionales que siempre son susceptibles de haber llegado a casa desde el trabajo por un descuido.

Otras posibilidades de asalto son mucho más sencillas y parecidas al molesto *spyware* que continuamente intenta introducirse en nuestros ordenadores. ¿Cuánto valen los datos sobre los hábitos de millones de personas? Tarde o temprano aparecerá el troyano que espiará nuestros hábitos televisivos, o las horas a las que estamos o no en casa, cuantas veces lavamos la ropa o rellenamos la nevera. Esos datos tienen un valor incalculable desde el punto de vista económico y comercial y no podemos ser tan inocentes de pensar que una prohibición legal va a impedir a los 'malos' intentar conseguirlos.

El internet de las cosas puede hacernos la vida más cómoda e interesante, pero abre nuevas puertas que debemos asegurar si queremos vivir tranquilos y mantener a salvo nuestra vida privada y patrimonio.

http://delicious.com/rpla/raa833a

SEGURIDAD

CUANDO SANGRA EL CORAZÓN

Una noticia de carácter técnico que habría pasado inadvertida a la mayoría de los usuarios resulta de suma importancia para la seguridad de la red. Por ello saltó a primeros de abril a la portada de muchos diarios.

El Proyecto OpenSSL hizo público el lunes 7 de abril un comunicado en el que avisaba de un grave fallo en algunas versiones recientes de OpenSSL, un paquete de herramientas y bibliotecas que utilizan dos terceras partes de los servidores de Internet, para cifrar sus comunicaciones y contenidos.

El fallo se encontraba en una librería denominada 'heartbeat' (latido de corazón) utilizada por los protocolos TLS (Transport Layer Security) y DTLS (Datagram TLS) de OpenSSL. Permitía mantener una comunicación cifrada abierta mediante señales (latidos), pero un fallo en el código hace que un atacante pueda obtener trozos de 64 Kb. de la memoria del servidor. Realizado de forma sistemática, puede llegar a obtener información muy importante, porque por la memoria del servidor pasa información que puede ser muy crítica en manos de un extraño. Además el 'asaltante' no deja ninguna huella. De forma muy acertada el fallo ha sido denominado 'corazón sangrante'.

El error se introdujo en OpenSSL en diciembre de 2011 y se ha mantenido en el código de OpenSSL hasta la versión 1.0.1 liberada el 14 de marzo 2012. La versión secundaria OpenSSL 1.0.1g liberada el 7 de abril de 2014 fija (elimina) este error.

Desde marzo de 2012 hasta abril de 2014, esas dos terceras partes de servidores de internet que utilizaban las librerías han sido vulnerables, de forma que hipotéticos atacantes habrían podido desvelar todo tipo de datos cifrados en los mismos, incluidas contraseñas, datos bancarios, o cualquier otro tipo de información. Y lo que es peor, prácticamente sin dejar rastro de haberlo hecho. A partir del anuncio, las principales compañías de la red se han lanzado a un análisis de los posibles daños y a advertir a sus usuarios que sus datos podrían haber quedado expuestos, recomendando cambios de contraseñas. Los expertos lo califican como el mayor fallo de seguridad producido en la red.

En términos cotidianos, es como si nos hubiéramos ido de vacaciones dejándonos la puerta trasera cerrada, pero con la llave debajo de la alfombra. Si nadie buscó ahí la llave, puede que no nos hayan robado. Ha sido un gran peligro, pero no quiere decir que nos haya afectado. Sin embargo, si en casa teníamos algún secreto, puede que este haya quedado desvelado sin necesidad de que echemos en falta algún objeto de valor, por no mencionar el hecho de que pueden haber hecho copias de las llaves que estaban colgadas a la vista. Por tanto puede que nadie haya entrado en nuestra casa o puede que nuestros secretos y nuestras llaves estén en manos de desconocidos. Se impone un inventario y un cambio de cerraduras...

El fallo no afecta a los ordenadores o el *software* que puedan utilizar el usuario, sino en el *software* del servidor. Por eso han sido las compañías que poseen estos servidores en internet los que han tenido que actualizarlos para eliminar las versiones defectuosas. A los usuarios se les ha recomendado que después del cambio actualicen sus contraseñas, que podrían haber quedado expuestas y en poder de alguien que hubiera realizado una intrusión. Si no lo han hecho ya, es muy recomendable hacerlo, especialmente aquellos que para realizar un menos esfuerzo de memoria, usan siempre la misma clave en varios servicios.

http://delicious.com/rpla/raa833b

CIBERGUERRA

PRIMERAS JORNADAS DE CIBERDEFENSA

El Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD) organizó la primera edición de las jornadas de ciberdefensa, que se desarrollaron entre los días 31 de marzo y el 3 de abril en el Centro Superior de Estudios de la Defensa (CESEDEN)

El lema elegido en la primera edición de las Jornadas de Ciberdefensa, "Construyendo la Ciberdefensa en España", refleja la firme voluntad de que estas jornadas sirvan de manera efectiva al propósito de crear un punto común para construir una sólida conciencia nacional de ciberdefensa, contando para ello con la participación de cuantos tienen alguna responsabilidad en la materia: las Fuerzas Armadas, las Fuerzas y Cuerpos de Seguridad del Estado, la Administración Pública en general, la Industria Nacional, el sector académico español y, como pieza clave de todo ello, las personas.

Las jornadas fueron inauguradas por el ministro de Defensa acompañado por el jefe del Estado Mayor de la Defensa, almirante general Fernando García Sánchez y el director del Centro, teniente general Alfonso de la Rosa. Durante las palabras de inauguración, Pedro Morenés resaltó que "la ciberdefensa es imprescindible porque el ciberataque es una de las agresiones más brutales que puede recibir una sociedad", y ha asegurado que "es fundamental la capacidad industrial para desarrollar nuestros propios mecanismos de seguridad en ciberdefensa".

Las jornadas se estructuraron de manera temática, con cada uno de los días dedicado a un aspecto distinto de la Ciberdefensa. De esta manera, el día 31 de marzo se trataron los aspectos generales, En la primera sesión de las jornadas, intervino el general de brigada, Carlos Gómez López de Medina, jefe del Mando Conjunto de Ciberdefensa (MCCD), presentando el mismo y haciendo un desarrollo de sus funciones.

El día 1 de abril se trataron las acciones de ciberdefensa, el 2 de abril cuestiones relacionadas con la Explotación (ciberinteligencia), y el 3 de abril fue el día dedicado a la respuesta (Acciones ofensivas).

Las mesas redondas fomentaron la participación de todos los participantes, entre los cuales hay que mencionar especialmente al sector industrial, que expuso conceptos relacionados con distintos escenarios y amenazas, tratando las posibles formas de abordarlas mediante demostraciones concretas, esencialmente prácticas y muy participativas, desarrolladas por las tardes.

Tras el éxito de estas primeras jornadas cabe esperar que la convocatoria se repetirá en los proximos años.

http://delicious.com/rpla/raa833c

Enlaces

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