Internet y nuevas tecnologías

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

SEGURIDAD

EL ATAQUE A HACKINGTEAM

La empresa italiana HackingTeam es, por decirlo en terminología 'física' un fabricante de armas. En realidad se trata de sistemas de seguridad, que pueden ser utilizados con carácter defensivo, pero también 'ofensivo'. La naturaleza de estos recursos informáticos hace que su fortaleza se base en información secreta o al menos discreta, entre la que se encuentra el propio código de los programas y aplicaciones.

Pues bien, el día 6 de julio de 2015 unos intrusos hackearon los servidores de la empresa, apoderándose de su cuenta de twitter y posteando desde ella un enlace a una web de almacenamiento en la nube donde habían ubicado un gigantesco archivo con información de las relaciones de la empresa con sus clientes y código fuente de sus aplicaciones. Esta situación plantea diversos aspectos cuando menos incómodos.

En primer lugar, los clientes de la empresa son gobiernos y servicios de seguridad. Aún cuando sus contratos sean completamente legales, como es el caso en España del CNI, a ningún organismo oficial le gusta que se conozcan sus técnicas y recursos contra el crimen, y menos cuando se trata de operaciones 'discretas'.

En segundo lugar, está la polémica que ya rodeaba anteriormente a HackingTeam sobre la naturaleza de sus clientes, ya que mientras algunos activistas afirmaban que facilitaba herramientas de espionaje, incluso a gobiernos de dictaduras que las usarían para limitar los derechos de sus oponentes políticos, desde la empresa se desmintió antes y después del ataque, pero los documentos desvelados parecen demostrar que mentían antes y ahora.

En tercer lugar y según la propia nota publicada en la página de HackingTeam, el código desvelado puede comprometer las operaciones de sus clientes, a los que la empresa ha aconsejado dejar de utilizar sus programas hasta que sean convenientemente protegidos por nuevas versiones.

Y en cuarto lugar, la tecnología de seguridad de HackingTeam ha pasado en cierto modo a ser pública. Según su nota, "la capacidad de controlar quién utiliza la tecnología se ha perdido. Terroristas, extorsionistas y otros pueden desplegar esta tecnología a voluntad si tienen la capacidad técnica para hacerlo".

Estas implicaciones que se me ocurren en este momento sin duda no son las únicas. Los programas de 'monitorización' de HackingTeam se anunciaban como 'no detectables por los antivirus' y demás medidas de protección, un “escudo de invisibilidad” que es posible que ahora hayan perdido, por lo que muchos de los objetivos de estos programas de "monitorización" pasarán a ser conscientes de que eran monitorizados y actuarán en consecuencia, para consternación de aquellos que sigilosamente los monitorizaban.

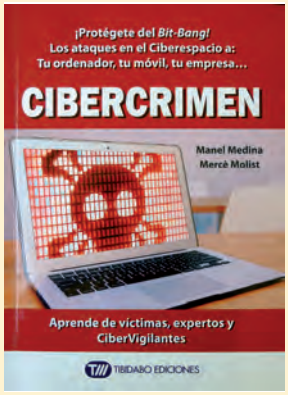
http://delicious.com/rpla/raa846a

LIBROS

CIBERCRIMEN

Aún a riesgo de invadir otras secciones de la revista, voy a hacer en esta el comentario de un libro. Trata de cuestiones prácticas, que afectan a nuestra vida diaria y se titula "Cibercrimen", una guía sobre los riesgos y peligros que podemos encontrar en nuestras actividades digitales, escrito con precisión de experto que aporta Manuel Medina y con textos muy asequibles a cualquier nivel escritos por la periodista y divulgadora de temas de seguridad informática Mercé Molist.

No es un recurso al tópico decir que se trata de un manual de lectura imprescindible, que resulta ameno para leer en casa y riguroso, además de útil para su estudio en las aulas.



Tal y como se dice en la presentación, "La seguridad no es un producto, sino un proceso en el que participa todo el mundo, por el cual garantizamos la robustez y la resistencia de la información".

Su índice abarca desde consejos básicos a la forma de actuar de los ciberdelincuentes y sus principales técnicas, así como la forma de protegernos de ellas. Es cierto que en cada sistema la parte más débil suele ser el usuario y este libro resulta sumamente útil para disminuir esa vulnerabilidad.

La idea que se repite una y otra vez a través de la metodología empleada, que resulta sumamente didáctica, es que tradicionalmente nuestros padres, nuestros maestros e incluso nuestros amigos nos han advertido de los peligros tradicionales de la vida real.

Desde el "mira antes de cruzar" que nos repetía nuestra madre o el "no hables con extraños", hasta el comentario de un amigo sobre los lugares peligrosos o caros que debemos evitar en nuestras escapadas de ocio, hemos pasado una vida aprendiendo a identificar las situaciones de peligro a través de los consejos de nuestro círculo de confianza. Para muchos de los usuarios de las Tecnologías de la Información, esta experiencia no existe. De una forma vaga se mencionan en las noticias temas como: robo de identidad, fraude informático, virus, troyanos o malware, sin que nadie nos haya explicado claramente cuales son las implicaciones que tienen en nuestra vida y qué son y significan de forma práctica para nosotros estas amenazas.

"Cibercrimen" nos muestra en sus diferentes capítulos como identificar situaciones potencialmente peligrosas, explicando el peligro que comportan y las formas de actuación de los "malos", así como cual debe ser nuestra actuación para protegernos y a quién acudir en caso de convertirnos en víctimas de un ataque.

Espero que este libro sea un éxito, no solo para premiar el atrevimiento de autores y editor, sino porque de su popularización solo puede surgir un entorno más seguro y fiable para todos. Los riesgos más importantes para nuestros dispositivos y ordenadores se derivan de relacionarnos con personas cuyos dispositivos son vulnerables a los ataques pues, como en la medicina, las infecciones nos las pasan los que tenemos cerca.

http://delicious.com/rpla/raa846b

HACKING

CIBERATAQUE CONTRA LA COMPAÑÍA AÉREA LOT

En cualquier campo de la aviación, la Seguridad en Vuelo o Seguridad Aérea, es una condición imprescindible. En la aviación comercial hay una máxima que dice: "Si la seguridad te parece cara, prueba con los accidentes". Quiere decir que el mayor quebranto económico que puede sufrir una compañía aérea es un fallo de seguridad. A las pérdidas materiales provocadas por el siniestro y las posibles indemnizaciones a que diera lugar, se añadiría la pérdida de imagen, con el consiguiente descenso en las ventas. Son muchas las compañías que no se han recuperado de un accidente, viéndose abocadas al cierre o a la ruina.

Por eso, cualquier aspecto de las operaciones aéreas relacionado con su seguridad cobra una importancia enorme y obtiene una gran repercusión mediática. Y como casi toda persona sensata sabe, en el centro de un huracán mediático es muy difícil distinguir el polvo de la paja y sacar conclusiones técnicas fiables debido a la afición de los periodistas por los titulares dramáticos.


Wikimedia Commons

No obstante hay que mencionar un hecho que saltó a la prensa en el mes de junio: un hackeo de los ordenadores de la compañía aérea polaca LOT afectó a sus operaciones obligando a cancelar una serie de vuelos.

Los comunicados de la compañía aportaban poca información: primero un fallo en los sistemas de tierra, más tarde solo se reconoció haber estado en una situación de ataque a las TI. Mucha de la información que en la red se da por cierta son estimaciones de agencias de noticias.

Es probablemente la primera vez, o al menos la primera que se conoce, que un ataque informático afecta a las operaciones de una compañía aérea. Hace ya un tiempo que en congresos de seguridad se han presentado casos hipotéticos sobre posibles ataques a los sistemas de información en vuelo o a la red wifi interna de la aeronave. Los estudios de estos temas concluían que el ataque a sistemas vitales era un escenario improbable y que la posibilidad de obtener el control de un aparato en vuelo era inviable. El máximo daño posible consistía en crear la confusión suficiente para alterar el normal discurrir de algún vuelo.

Este caso real, a pesar del revuelo formado, no contradice estos análisis. El ataque se produjo sobre los sistemas que generan los planes de vuelo. A pesar de que la elemental prudencia impone una desesperante falta de detalles sobre el ataque; parece ser que no se llegó a obtener el control de la aplicación que confecciona los planes de vuelo, sino que mediante un ataque de denegación de servicio se saturó el servidor impidiendo la distribución de planes de vuelo. Al encontrarse bajo un ataque de este tipo, el sistema, incapaz de diferenciar entre las peticiones legítimas y las de los atacantes, no tiene otra alternativa que detener su funcionamiento para adoptar medidas defensivas y hacer un chequeo para determinar que no se trata de una cortina de humo para ocultar una intrusión en alguna parte del sistema. Estas medidas requieren tiempo y si el sistema no tiene alternativas que puedan suplir su función, se produce una alteración del ritmo normal de operaciones.

Esto es lo que se sabe hasta ahora del ciberataque que produjo retrasos en las salidas de varios vuelos de la compañía LOT. Es de esperar que cuando el incidente haya sido analizado podamos estudiar su desarrollo completo con la misma finalidad que se hacen todos los análisis e informes de Seguridad Aérea: aprender de lo ocurrido para corregir los procedimientos, haciéndolos más seguros.

http://delicious.com/rpla/raa846c

Enlaces

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