EN INTERNET

SEGURIDAD EN INTERNET
¿Hackers, el principal peligro en la WEB?

Klaus Hartung Sabugo *

Introducción.

Problemas para la e-Banca española. El 41% de los usuarios españoles de la banca electrónica por Internet desconfía, y pone en duda la seguridad de las comunicaciones", una noticia así apareció hace 4 años en todos los periódicos españoles, y viene a aclarar un concepto muy importante: la desconfianza que los usuarios tienen en la seguridad de Internet. Solamente cuando piensan que la información que sobre ellos se pueda obtener no es relevante, no tienen inconvenientes en "navegar" a través de la red. En la conciencia popular se considera que el principal agente que pone en peligro la seguridad en Internet son los denominados Hackers o Piratas, sin embargo éstos son sólo una porción de todos los entes peligrosos que pueden vulnerar la amplia información de todo tipo disponible en la web.
El presente artículo tiene como objetivo fundamental, describir todos aquellos agentes que pudieran afectar la seguridad informática de nuestra organización, de manera tal de adoptar las medidas pertinentes antes que sea demasiado tarde.

La E-Confianza.

La mayoría de los visitantes requieren reserva respecto de la información personal que ofrecen "*on-line*". Por esta razón, los sitios web deben proveer a los navegantes confianza cuando envíen sus datos personales, haciéndoles saber claramente que no se va a vender o distribuir su información a ninguna otra compañía y ello supone una diferencia entre la competencia. Desgraciadamente muchas web tienen malas políticas de privacidad de datos. Muchas páginas web publican políticas inadecuadas con respecto a la privacidad de los datos de los visitantes. La Universidad de Mc Donough en Georgetown, ha realizado un estudio para determinar si las páginas web están siguiendo los consejos de los gobiernos para respetar la privacidad de los visitantes. El estudio examinó 364 web del tipo ".com" que se escogieron de forma aleatoria entre los 7.500 votos recibidos en la encuesta previa al estudio.
El 93% de las 364 web examinadas, recopilaban información personal identificable, incluyendo nombres, números telefónicos y direcciones postales y electrónicas, además de datos financieros o demográficos. Asimismo, se observó que aunque el 65.7% de las web tiene políticas de privacidad o avisan de que la información personal se transmite con seguridad, tan sólo el 9,5% de los sitios tenían una política de privacidad "*adecuada*".
Con la explosión que ha sufrido el uso de Internet, los abogados de muchas asociaciones en todo el mundo han estado intentando averiguar cómo darles a los usuarios los derechos adecuados para proteger sus datos de la mejor forma. Al respecto es interesante destacar que la política de privacidad de las web europeas, en general, es bastante más estricta que la norteamericana, la cual es menos restrictiva.
"Construir la e-confianza" y asegurar que ésta llega al cliente, y ser consciente de que la seguridad en las TI (Tecnologías de Información) es un reto que, al igual que sucede con los desafíos que plantea cualquier otra rama de la Ciencia y de la Técnica, es mucho más complejo y multidisciplinario de lo que parece. Aparte de la faceta estrictamente tecnológica, que es imprescindible, las facetas más importantes de dicho reto son:

- La socioeconómica.
- La cultural.
- La ético-legal.
- La política.

Todas ellas están estrechamente relacionadas entre sí. Ello implica la utilización de un enfoque socio-tecnológico, es decir, aquel en el que la Tecnología en general, y las TI en particular, se contemplan en su contexto social y se consideran como medios muy importantes destinados a coadyuvar a la consecución de fines deseables por la comunidad y sus miembros.

Tipos de Seguridad.

La inseguridad en la Red es uno de los fenómenos que más problemas y pérdidas económicas ha originado en los últimos años en gobiernos, administraciones y empresas. Resulta, incluso, complicado establecer los parámetros fundamentales que rigen o esquematizan el mundo de la seguridad en las redes. Podemos simplificar la seguridad informática descomponiéndola en dos grandes bloques: la seguridad por máquina o por *host* (sistema anfitrión), y la seguridad por *red*. La mejor forma de llevar a cabo un proyecto de seguridad es precisamente implementando la seguridad bajo la combinación de ambas aunque muchas veces resulte complicado, especialmente en grandes organizaciones.

La seguridad por host incluye el conjunto de técnicas y herramientas que permiten que un ordenador se encuentre seguro: sistema operativo correctamente configurado, políticas de copia de seguridad (backup), encriptado de ficheros, programas antivirus, programas de auditoría del propio sistema, etc. Aparte de las técnicas y herramientas criptográficas es importante recalcar que un componente muy importante para la protección de los sistemas es la atención y vigilancia sistemática y continua de los gestores de la red.

La seguridad por red, se plantea para el conjunto de sistemas interconectados.

Entran entonces a formar parte aspectos tales, como el tipo de autenticación en red, los sistemas cortafuegos o firewalls, los programas de detección de intrusos (Intrusion Detection Systems o IDS), los programas de auditoría en red, etc.

Además, dentro del sistema de seguridad por red podemos identificar dos tendencias principales:

Protección de los sistemas de transferencia o transporte.

En este caso, el administrador de un servicio asume la responsabilidad de garantizar la transferencia segura de la información de forma bastante transparente al usuario final. Ejemplos de este tipo de planteamientos serían el establecimiento de un nivel de transporte seguro, o la instalación de firewalls que defiendan el acceso a una parte protegida de una red.

Aplicaciones seguras extremo a extremo.

Es el caso de un documento firmado digitalmente o de un correo electrónico cuyo contenido haya sido asegurado previamente mediante algún procedimiento.

Aunque el acto de aportar seguridad a un mensaje cae bajo la responsabilidad del usuario final, es razonable pensar que dicho usuario deberá usar una herramienta proporcionada por el responsable de la seguridad de su organización.

Prioridad de la Seguridad en E-Commerce.

A pesar de que cada vez se hace más alusión a la seguridad electrónica, la mayoría de los negocios tienen grietas importantes que facilitan las intrusiones no autorizadas. Desgraciadamente, estas lagunas en seguridad se deben a la ausencia de planificación o a no tomarse en serio las amenazas. El mejor consejo consiste en estar preparado para los violentos ataques que se avecinan.

Los ataques del tipo delegación de servicio, debidos esencialmente a una saturación de servidores Internet causada por una inundación coordinada de mensajes inútiles entrantes, ponen de relieve la necesidad de ir con precaución y de protegerse cuando se trata de hacer negocios en la WEB. La disponibilidad de la línea, la protección de la privacidad de los usuarios y la confidencialidad otorgan una importancia capital a la seguridad de los negocios electrónicos.

Hay que considerar algunos de los retos que deben afrontar actualmente las empresas establecidas en la Red. Utilizando tan sólo unos cuantos mandatos muy primarios de bases de

datos, Strategy LLC, una firma rusa de ingeniería de software para la Web, ubicada en Yaroslavl, pudo obtener números de las tarjetas de crédito de los clientes, contraseñas, datos de los empleados y sus números de seguridad social. Tal como informó el *E-Commerce Times* en enero de 2000, Anatoliy Prokhoroy, director ejecutivo de Strategy LLC, afirma que las empresas, tanto grandes como pequeñas, olvidan instalar las defensas más simples, como proteger el software servidor mediante una contraseña e instalar las actualizaciones de seguridad, para impedir que los *hackers* accedan a sus sistemas.
La seguridad electrónica es un tema candente, debido a las espectaculares noticias que se han generado recientemente.
No han sido menos espectaculares los accesos ilegales y los robos perpetrados por algunos delincuentes.
Un ejemplo claro de ello podría ser CDUniverse, un detallista de música a través de Internet. Unos *hackers* accedieron a su sistema y obtuvieron los datos de los códigos de las tarjetas de crédito de sus clientes. Ahora, tanto ellos como sus clientes, se hallan expuestos a un importante riesgo económico, aparte de estar sometidos a chantaje para poder recuperar esta información.

¿Dónde Yace el Peligro?
El Centro Nacional de Protección de infraestructuras (NIPC) del FBI se encarga de detectar, impedir, analizar, emitir advertencias de peligro, responder e investigar las intrusiones informáticas y los actos ilegales. En respuesta a la última oleada de ataques tipo denegación de servicio, el NIPC ha apuntado hacia sedes de "*terceros*" que, sin ser conscientes de ello, apoyan de una forma activa los ataques de este tipo, las que al no instalar, actualizar o mantener tecnología Web de alta seguridad, estas sedes, sin saberlo, apoyan el lanzamiento de futuros ataques a través de Internet.

A pesar de que se informe a las organizaciones en materia de seguridad, las empresas que relegan la seguridad a menudo olvidan prestar atención a las advertencias. En pocas palabras, si la mayoría de sus vecinos *on-line* se olvidan de mantener una protección adecuada, pueden convertirse en los cómplices de los robos *on-line*, de modo que hay que estar atentos: *Uno tiene que preocuparse por sus propios huecos de seguridad y por los de los servidores http de los demás que, sin quererlo, sirven de plataforma de lanzamiento para ataques contra la propia sede*

.

Especialistas con motivaciones externas a las propiamente tecnológicas.
Existe un tercer tipo de atacantes externos, aunque éstos sólo suelen realizar ataques sobre grandes instituciones. Es el caso de los grupos criminales y de los piratas recompensados por organizaciones en competencia. Este suele ser el más peligroso de todos los perfiles de atacantes de un sistema informático, aunque por suerte, también el menos usual. Este tipo de ataques suelen buscar el robo de información muy valiosa para terceras partes o incluso el daño contra la imagen pública del atacado. La mayoría de los profesionales dedicados a realizar ataques a máquinas en Internet son efectivos gracias a limitaciones de los sistemas, errores de política, agujeros en las aplicaciones, etc. Comprender cuáles de estos elementos pueden incidir en un aumento de la seguridad es vital de cara a conseguir cerrar puertas a visitantes no deseados. A continuación se exponen algunos de estos factores, muchos de ellos completamente obvios.

Conclusiones.
Como se ha observado en el presente artículo, los peligros respecto a la información disponible en la web, como en los propios sistemas de información de una organización, están más cerca de lo que normalmente se piensa, y por consiguiente, su solución está al alcance de la mano, debiendo como primera medida tan sólo adoptar dentro de la organización, las acciones conducentes a restringir el uso de la información a aquellas personas idóneas tanto

profesional como personalmente, y cuya moral asegure que en el tiempo otorguen la seguridad de que la información disponible no será utilizada para otros fines que los realmente necesarios.

* Teniente 1° AB. Diplomado en Comercio Electrónico y Logística Empresarial U.V. Universidad Técnica Federico Santa María.

BIBLIOGRAFÍA

- Universidad Virtual Universidad Técnica Federico Santa María, Diplomado en Comercio Electrónico y Logística Empresarial, Los Procesos y Tecnologías del Comercio Electrónico y su Logística, Profesor Pedro Bravo Zehnder, MBA. E-Bussines.

*** * ***