SEGURIDAD INFORMÁTICA. SITUACIÓN ACTUAL Y BUENAS PRÁCTICAS

En los últimos años todo lo relacionado con la seguridad informática suscita un gran interés. Las empresas y particulares están más concienciados de los riesgos que conlleva su actividad electrónica. Esto es un hecho. También lo es que el desconocimiento general sobre estos temas todavía es demasiado grande.

La situación actual

Cada día se publican decenas de nuevos fallos en el software que utilizamos habitualmente. Hay cientos de sitios en Internet que ofrecen información, herramientas y métodos para vulnerar sistemas informáticos. Cada mes se publican nuevos libros con información sobre seguridad. Somos decenas de miles las personas que nos dedicamos en todo el mundo a la seguridad informática. Muchos lo hacemos porque es nuestra profesión y aplicamos estrictas normas éticas a nuestro trabajo. Pero otros están en el "lado oscuro" y tienen intenciones menos amigables.

Hasta hace poco la mayoría de las pesadillas sobre seguridad informática de un usuario típico tenían que ver con los virus. Ya casi no nos acordamos de ellos, ahora tenemos nuevas palabras para jugar: *phishing*, *spamming*, *pharming*, *hacker*, *cracker*, *adware*, *spyware*, etc. El mundo de la seguridad informática y los medios de comunicación han creado todo un mar de terminos en los que el usuario normalmente acaba ahogándose.

Pero los "chicos malos" si conocen todo esto a la perfección. A un atacante con conocimientos medios le resulta relativamente sencillo introducirse en la mayoría de sistemas informáticos. Se asombraría de lo fácil que es entrar en su router de conexión a Internet o en la base de datos de su sitio Web.

Tomemos como ejemplo el *phishing*. Este ataque consiste en conseguir mediante engaño información sensible de las víctimas, como contraseñas de banca online o números de tarjeta de crédito. Hay varias modalidades pero la más habitual consiste en el envío masivo e indiscriminado de correos electrónicos que simulan provenir de entidades bancarias y en los que se nos solicita esta información. Hay informes publicados que señalan que solo en EE.UU. el número de usuarios que han recibido este tipo de mensajes ha pasado de 57 millones en 2004 a 109 millones en 2006. Las perdidas provocadas por el *phishing* han superado ya los 2.800 millones de dólares.

La información sobre seguridad informática es muy amplia, hace mucho tiempo que este tema se convirtió por derecho propio en una rama específica de la

informática. Para estar al día de todos los posibles riesgos es necesario especializarse y dedicar mucho tiempo al estudio. Obviamente, todo este esfuerzo no puede exigirse al común de los usuarios. Entonces ¿como puede protegerse?. Le ofreceré un pequeño consejo. Usar el sentido común.

El sentido común

En nuestra vida cotidiana aplicamos constantemente conceptos de seguridad: no dejamos las llaves de nuestra vivienda en cualquier sitio, no le decimos el PIN de nuestra tarjeta de crédito o nuestros datos personales a cualquiera que nos los pida, ponemos cerraduras y alarmas en nuestras casas y empresas, etc. Constantemente aplicamos el sentido común en nuestra vida cotidiana, de la misma forma deberíamos hacerlo en nuestra vida informática: usar contraseñas complejas y mantenerlas en secreto, no responder a correos que nos piden datos personales, no abrir cualquier fichero que nos llegue por correo, usar sistemas de protección de intrusión, etc.

Volviendo a nuestro ejemplo del *phishing* debe saber que su banco nunca le pedirá información confidencial por Internet. De hecho, ninguna empresa seria lo hará. Si recibe un mensaje de este tipo no responda.

La solución mágica

Tengo un antivirus y un *firewall* (cortafuegos), estoy protegido. Pues no. Esta es una de las presunciones más habituales y más peligrosas. ¿Sabe que su antivirus y su cortafuegos tienen fallos?. Todos los tienen. ¿Lo ha actualizado últimamente?.

Desconfíe de quien le ofrezca estas soluciones milagrosas, la seguridad informática es algo más complejo. Estos software también tienen vulnerabilidades, todos los fabricantes tienen problemas de seguridad, está en la naturaleza humana, mientras el software lo sigan construyendo humanos seguirá conteniendo errores.

Es cierto que como usuarios podríamos exigir a los fabricantes un mayor esfuerzo en seguridad. De hecho la mayoría de ellos hace tiempo que se toman el asunto muy en serio. El caso de Microsoft es significativo, esta empresa ha pasado de casi no preocuparse por el tema, de ahí la merecida fama que se ha ganado, a construir productos cada vez más seguros, en muchos casos bastante más que sus competidores, aunque como todos sigue teniendo problemas.

Tampoco nos protegen las leyes cada vez más estrictas sobre lo relativo a la seguridad informática. En nuestro país, el legislador está desarrollando últimamente leyes que castigan cualquier acto de *hacking*, sea de la naturaleza que sea, e incluso la simple posesión de programas de seguridad se convierte en delito. Esto nos sitúa a

los investigadores en seguridad informática en una difícil posición. Pero al usuario no le protege. Recuerde que si sus sistemas están conectados a Internet, su atacante puede estar en cualquier parte del mundo, esto incluye países con escasa o nula legislación al respecto, podemos presuponer que a un *hacker* de Corea, Nigeria, Irán o Indonesia nuestras leyes no le causarán mucho miedo.

No deberíamos depositar toda nuestra confianza en que solo el software de seguridad o las leyes nos protejan. Le ofreceré otro consejo. Sea desconfiado, muy desconfiado.

Protegiéndose

Entonces ¿qué puede hacer el común de los mortales para protegerse?. Alguien muy drástico le diría que no use Internet y que apague todos sus ordenadores. Evidentemente no queremos volver al pasado, así que le ofreceré una humilde lista de buenas prácticas encabezada por los dos consejos anteriores:

- Use el sentido común.
- Sea desconfiado.
- Manténgase todo lo informado que pueda.
- Consiga apoyo y asesoramiento de expertos.

No todo es negativo. El inmenso conocimiento acumulado sobre seguridad informática sirve para crear sistemas cada vez más robustos. La propia cultura general de los usuarios sobre estos temas hace que los atacantes tengan que idear métodos cada vez más complejos. La implantación de sistemas de autenticación y certificación digital ofrece nuevos mecanismos de seguridad. Las empresas dedican más recursos a esta área y cada vez hay más profesionales cualificados.

Para las empresas es muy importante contar con asesoramiento experto que les guíe en los procesos de implantación de mecanismos de seguridad. Si su empresa cuenta con asesor financiero y legal, ¿por qué no tener un asesor informático que le ayude también con la seguridad?.

Del mismo modo que en la vida cotidiana la seguridad es parte de nuestro comportamiento, con el tiempo también lo será en nuestro quehacer informático. La seguridad informática ha entrado en nuestras vidas impetuosamente, y está para quedarse. Acostúmbrese a vivir con ella.

Jose Manuel Cejudo Gausi (jmcejudo@multitrain.es)
Desarrollador e investigador en seguridad informática