Nº 3 - MARZO DEL 2011

www.autoes.es

En este número vamos a centrarnos en la seguridad informática.

La necesidad de que nuestro sistema informático goce de buena salud está ligado a un conjunto de factores a los que no siempre les prestamos la atención que merecen.

Internet se utiliza hoy en día para todo y algunos de los usuarios de la red tienen muy claro que pueden sacar provecho de ese tráfico multitudinario.

El objetivo fundamental de los creadores de virus, gusanos, troyanos,... tiene ahora un objetivo muy claro: obtener dinero.

Agradeceremos cualquier comentario, sugerencia, aportación,… que nos hagáis llegar.

Contacto: comercial@autoes.es

INTERNET : ¿UN PELIGRO NECESARIO?

I.- ¿De donde proceden los programas maliciosos?

Los creadores de programas malintencionados se han profesionalizado y los ataques a nuestro sistema informático pueden venir de los sitios más insospechados.

Durante años la parte más importante de estas amenazas ha venido introduciéndose a través del correo electrónico; la descarga de programas gratuitos, películas, música, …; el acceso a páginas de contenido sexual, …

Ahora el peligro se ha extendido a cualquier página de Internet que reciba muchas visitas y ahí podemos incluir: páginas de uso cotidiano (periódicos,...), redes sociales como "Facebook", "Tuenti", … o páginas superconcurridas como "yotube", "ebay", … o de juegos en red.

El objetivo de estos "programadores" ha perdido cualquier tipo de romanticismo que pudiera haber tenido en el pasado. Ya no se trata de demostrar lo mucho que saben o de dejar en evidencia los agujeros de seguridad de grandes empresas o de la administración estatal. De lo que se trata ahora es de conseguir un beneficio económico.

II.- ¿Que armas utilizan?

Su arma fundamental es el engaño. Los grados de sofisticación y de encubrimiento con el que desenvuelven su labor no ha hecho más que aumentar.

Aunque la mayoría de los usuarios se cree protegido, simplemente por el hecho de tener instalado un antivirus, han sido muchos los que han picado al recibir un aviso parecido a este:

"Tu ordenador esta infectado.
Hemos detectado muchos bichejos,
Bajate nuestro programa y los mataremos".

El ordenador no estaba infectado realmente, pero al aceptar la invitación lo que realmente se instalaba era un gusano molesto y pertinaz que impedía trabajar.

Otra variante de lo mismo puede ser:

"Tenemos un premio para ti.
Pincha aquí y verás que bien".

Más sofisticado es el caso del gerente de una empresa que habia estado en Brasil, por cuestiones comerciales, y al volver se encontró con un correo del "Ministerio de Justicia de Brasil", a cuya pagína web tenia que conectarse para bajarse un "requerimiento judicial" (en realidad un gusano).

También han proliferado los bichejos que retocan los protocolos de red impidiendo la salida a Internet o que inutilizan el antivirus instalado, o impiden que se actualize, u otros que permiten el acceso a la red local pero impiden la conexión a Internet, …

III.- ¿Como defenderse?

Las precauciones a adoptar para evitar contaminaciones innecesarias son:

1) Utilizar un Sistema Operativo legal, que permita actualizarse con todos los parches de seguridad necesarios en cada momento.

2) Utilizar un buen antivirus que detecte cualquier intento de intrusión e impida el acceso a los programas malintencionados.

3) No instalar programas que no se necesiten y no abrir correos de remitentes desconocidos.

4) No instalar ActiveX, a no ser que proceda de sitios de confianza.

5) Periodicamente entrar en el Internet Explorer, "Herramientas", "Opciones de Internet" y solicitar el borrado de archivos temporals, cookies, historial, formularios y contraseñas, …. o si se utiliza Mozilla Firefox, "Herramientas", "Limpiar datos privados".

6) Restringir al máximo la utilización de llaves USB, CDROMS, disquets, … porque pueden transmitir su propia infección (cogida en otros ordenadores) al sistema con el que estamos trabajando.

7) Los móviles de última generación y las PDA's, o los ordenadores portátiles pueden ser otra buena fuente de infecciones de las que hay que resguardarse.

8) La protección de las redes inalambricas para que no puedan acceder a ella cualquier extraño que se encuentre cerca fisicamente.

9) La utilización de contraseñas seguras para acceder a las aplicaciones que contienen información sensible de ser utilizada con fines ilícitos.

10) Establecer una política de seguridad que promocione la conectividad y la disponibilidad, pero sin saltarse la seguridad.

En cualquier caso, el mayor peligro es siempre el propio usuario que está dentro de una organización, que no tiene porque ser malintencionado, pero que por torpeza o por desconocimiento puede abrir las puertas a una infección y a una fuga de datos.

Palabras técnicas relacionadas

Malware.- Del ingles "**mal**icious soft**ware**", es cualquier programa que tiene como objetivo infiltrarse en un sistema informático sin el conocimiento de su dueño, con finalidades muy diversas.

Spam.- Son mensajes de correo no deseados, habitualmente de tipo publicitario, enviados en grandes cantidades.

Adware.- Es cualquier programa que se ejecuta automaticamente y muestra publicidad no deseada de manera persistente.

Scam (estafa).- Correo electrónico o página fraudulenta que persigue obtener dinero ofreciendo cualquier cosa previo envio de dinero.

Pharming.- Redirección de un dominio a un servidor preparado para suplantar la página original .

Phising.- Intento fraudulento de obtener contraseñas o información detallada de los códigos que permiten realizar operaciones bancarias a través de internet.

Spyware.- Es un "programa espia" que se apodera de datos (direcciones de correo, ficheros de nuestro ordenador, …) y que pueden monitorizar nuestros accesos a Internet.

Botnet.- Conjunto de ordenadores infectados por un mismo gusano que permite a su creador utilizar las computadoras de otros para sus propios fines.

Cookie.- Huella que se almacena en el disco duro del visitante de una página web a petición del servidor de la página.