SEGURIDAD INFORMATICA

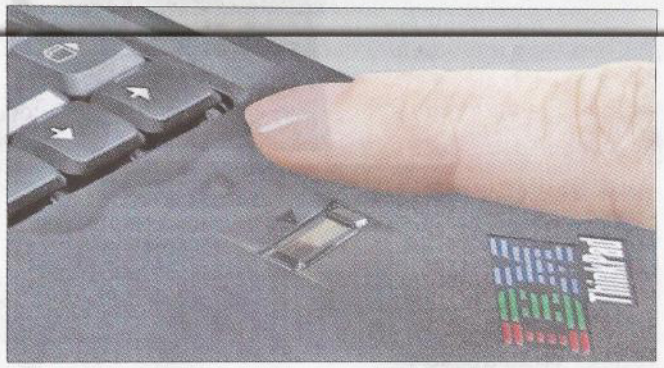
Los virus son un problema para el universo digital, pero sin dudas, la aparición de intrusos a través de Internet se ha convertido en un inconveniente aun mayor para los navegantes individuales y corporativos.

Hay un espía en mi PC

Los usuarios de computadoras en el mundo entero por la ola de inseguridad informática. Hasta hace un tiempo, su gran preocupación se centraba en los virus que podían infectar su sistema operativo. En la actualidad, a esa inquietud se suma otra mayor: los espías.

Estos intrusos se meten en las máquinas ajenas a través de programas Spyware que permiten a otras personas ingresar en un equipo sin permiso por medio de Internet y conocer toda su información, páginas que visita y preferencias. Los más utilizados son el Adware, Malware, Keylogger, Algunos abren avisos pop-up con publicidades y los más dañinos modifican las preferencias del navegador web, agregan sitios en la lista Favoritos del Internet Explorer y transmiten información confidencial. También, hacen más lento el sistema y pueden llegar a inutilizar la máquina.

A pesar de su peligrosidad, algunas personas no le dan la importancia que merece el tema. Un estudio realizado por America Online y la organización National Cyber Security Alliance destaca que "la mayoría de la gente cree que estos ataques no ocurren". Cuando los expertos visitaron sus casas, detectaron que "no contaban con la protección adecuada y que el 80 por ciento tenían programas espías instalados clandestinamente".



Este problema ha superado los hogares y se está tornando un dolor de cabeza para las empresas. La intromisión en las máquinas ha comenzado a poner en jaque su seguridad informática.

El 67 por ciento de las compañías consultadas por Ernst & Young en 51 países considera el tema como muy importante. Sin embargo, el 80 por ciento coincidió en que "la seguridad informática no se encuentra dentro de las prioridades de los CEO".

Contra el espionaje

El gran dilema de las empresas es cómo combatir las intromisiones en sus redes internas. "Primero deben conocer la exposición real que tienen y después concien-

Incidentes que ocasionaron una interrupción inesperada de sus sistemas*

Incidente	Ocurrencia	Origen		
		Interno	Externo	Desconocido
Falla de hardware	72%	87%	9%	4%
Virus, Trojan Horse o Worms	68%	21%	76%	3%
Falla de telecomunicaciones	64%	26%	72%	2%
Falla de software	57%	78%	16%	6%
Falla de terceros, ej. proveedor del servicio	47%	9%	87%	4%
Cuestiones de capacidad del sistema	46%	91%	6%	3%
Errores operativos, ej. carga de software erróneo	42%	91%	6%	3%
Falla de infraestructura, ej. incendio, corte de luz	42%	49%	49%	2%
Mala conducta de empleados actuales o anteriores	24%	84%	12%	4%
Ataques de Denegación de Servicio	23%	10%	85%	5%

*Encuesta realizada entre 1235 empresas en 51 países. **Fuente**: *Ernst & Young*

tizar a los usuarios sobre los daños que pueden generar – dice Gabriel Agnoli, gerente de Technology & Security Risk Services de Ernst & Young -. Para eso, es necesarios capacitar a los empleados".

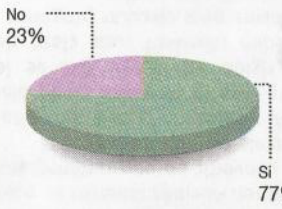
La lucha contra los espías no tiene límite. La solución es actualizarse para contrarrestar los nuevos embates. Una compañía necesita contar con personas que controlen los equipos y atiendan cualquier falla. A su vez, deben tener alguna protección: programa y equipamiento.

Los sistemas más famosos son los llamados firewall que bloquean el acceso de los Spyware a los puertos de salida cuando están instalados en una máquina. Estas barreras evitan que accedan a Internet y envíen información a otras personas.

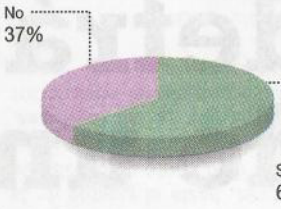
Existen programas que limpian la computadora de intrusos. Los anti-spyware y ad-aware detectan los espías y cookies, y los eliminan. El Bugnosis revisa las páginas visitadas y detecta la presencia de los Web Bugs.

Cuánto se protegen las empresas*

¿Tienen un plan de respuesta ante incidentes?



¿Realizan evaluaciones de vulnerabilidad y penetración en forma regular?



*Encuesta realizada entre 1235 empresas en 51 países.

Fuente: *Ernst & Young*

"Lo mejor que se puede hacer es tener actualizado el Windows, el antivirus, el firewall y los programas para la limpieza de la máquina", aconseja Patricio Dlin, especialista técnico de Hewlett Packard (HP).

Otra forma de protegerse es con tecnología diseñada especialmente para evitar ingresos de extraños en las computadoras. Estos dispositivos ofrecen métodos de bloqueo y tornan más seguras las máquinas.

Digital-Persona cuenta con un Automatizador Total de Contraseñas que utiliza las huellas digitales para permitir el acceso a los datos guardados. Así, sólo ingresan en el sistema las personas registradas Esto sirve para defenderse contra ataques externos, evitar la vulnerabilidad de las contraseñas y cuidar el correcto funcionamiento interno de las PC.

IBM también implementó esta modalidad para sus notebook. En cambio, HP, optó por un doble cerrojo. Sus nuevos modelos cuentan con una Smart Card que sirve para habilitar el inicio del Windows.

A su vez, incluye un chip de seguridad que permite a los usuarios encriptar la información que desee a través de un hardware. Esto la torna invulnerable. El dispositivo fue desarrollado en conjunto entre AMD, HP, IBM, Intel, Microsoft, Sony y Sun Microsystems.

Los espías están en todas partes y han comenzado a generar problemas en las máquinas y redes internas de las empresas y los hogares. Sólo hay una forma de prevenirlos: invirtiendo en seguridad informática.

"Es imposible evitar los ataques por completo porque los propios sistemas operativos aún son vulnerables –concluye Agnoli–. Tomar medidas de seguridad los va a ayudar a minimizar los riesgos".

Por Hernán Dobry