

Los ingenieros alertan de que las redes inalámbricas son vulnerables

Advierten de que muchos usuarios no configuran bien la protección de equipos. Cortafuegos, antivirus y claves ayudan a decidir quién tiene acceso

Las redes inalámbricas domésticas no siempre son seguras. Al menos eso es lo que afirma el Col.legi Oficial d'Enginyers de Telecomunicació de Catalunya en una nota hecha pública ayer. El organismo advierte de tres problemas: los usuarios no configuran bien las redes 802.11b y .g, no instalan un cortafuegos (firewall) y se exceden los límites de potencia de los equipos. En el mismo sentido se han pronunciado antes otros grupos de usuarios, como la celebración de la gincama de la Xarxantoni, celebrada el pasado febrero.

Si desea ver el gráfico en PDF haga click en la imagen.

"Existe un riesgo potencial de la seguridad de la información en el ámbito doméstico y empresarial debido a la falta de rigor en la ejecución de las instalaciones", asegura la nota. Los ingenieros advierten de los peligros más habituales, que no son sólo que alguien utilice una conexión ajena, sino que a través de ella "tenga acceso a los datos de su ordenador y pueda manipularlos libremente". Y el siguiente paso puede ser, advierten, usurpar la identidad.

Los ingenieros aconsejan que "los usuarios sometan sus sistemas a alguna revisión de seguridad a fin de evitar accesos indeseados a su intimidad". y que exijan "que las instalaciones sean homologadas" en potencia radioeléctrica; "no dejar las redes abiertas a otros usuarios", y "seguir una política estricta de protección de la información, al igual que se realiza en el caso de los virus".

"Los equipos actuales ofrecen un nivel de protección del 85%, que es mucho, lo que ocurre es que mucha gente se olvida de blindar el ordenador. La conexión se puede compartir, pero la máquina hay que protegerla", señala Josep Comulada, de la empresa Grubit y miembro de la red libre Barcelona Wireless.

¿Cómo? "Desactivar el compartir el disco duro, instalar un buen antivirus y un cortafuegos, y tenerlos actualizados, no bajarse cosas raras de internet y vigilar si la máquina empieza a hacer cosas que no se le han pedido", asegura Comulada.

"La mayoría de equipos incluyen medidas de seguridad como cortafuegos y protocolos de encriptación, pero como algunos no son muy intuitivos, los usuarios no los instalan", admiten en el fabricante D-Link.

"Los usuarios están acostumbrados a que instalan el equipo en cinco minutos y funciona, y entonces se ponen a navegar y se olvidan de proteger la red", explica Javier Gómez, responsable para España de Linksys, la rama de productos inalámbricos de Cisco Systems. "Para un usuario doméstico, con ocultar la red y eliminar el control de direcciones MAC, ya es suficiente. Aunque se puede añadir claves WPA y WPA más encriptación PKIP, si lo permiten los equipos", dice.

[El Periodico](#)

Fecha artículo: mié 30 mar 2005 07:32:54 CEST

Cristino Martos, 4
28015 Madrid

Tel 91 540 92 82 Fax 91 548 28 10
comfia@comfia.ccoo.es