Seguridad en comunicaciones inalámbricas y dispositivos móviles

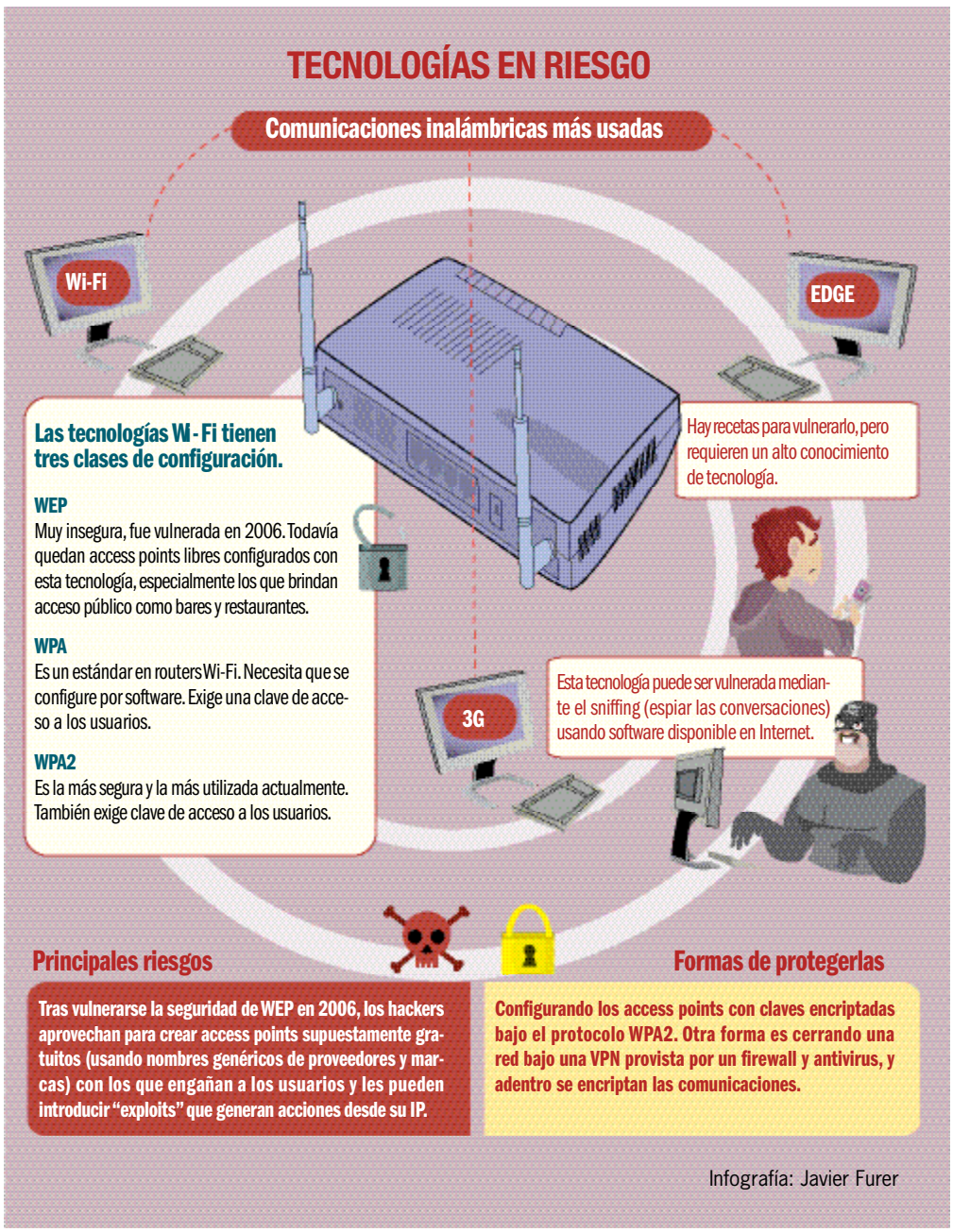
Inseguridad en el aire

Para asegurar el entorno corporativo ya no alcanza con antivirus, firewall y claves. Cuáles son las amenazas sobre redes inalámbricas y celulares. Cómo protegerse.

Por Darío Laufer

En seguridad informática, el límite entre precaución y paranoia es muy difuso. Firewall, antivirus, encriptación, hardware dedicado. Todas las tecnologías entran en juego al momento de asegurar el entorno corporativo. "Hay que tratar de no dejar ninguna puerta abierta, ya que puede ser un riesgo potencial para una intrusión", aconseja Julio Ardita, director de Cybsec, consultora que desde hace cinco años realiza un estudio para saber cuáles son las medidas de seguridad en los accesos Wi-Fi públicos.

La técnica que utiliza es tan simple como conocida: recorre en auto el centro porteño en busca de señales Wi-Fi emitidas por routers inalámbricos y clasifica los niveles de protección en base a los protocolos de seguridad que utilizan, los nombres que dan a las redes, y el tipo de contraseñas que usan. "Cada vez hay menos accesos con protocolo WEP, que fue vulnerado en 2006. La mayoría está configurado con WPA y WPA2, pero muchos accesos tienen como nombre la marca del equipo, o del proveedor de acceso, y utilizan la numeración correlativa del uno al nueve como contraseña. Esos equipos son una puerta de entrada para intrusos, y es posi-



Infografía: Javier Furer

ble que desde allí se ejecuten exploits (programas que explotan una vulnerabilidad del software) para enviar spam", ejemplifica Ardita.

Y hay algo que es aún peor: la mayoría de los ataques no son dirigidos hacia una persona o una empresa en particular. Se trata de pruebas realizadas por principiantes (rookies, en la jerga), pichones de hackers que prueban aplicaciones disponibles en Internet como Karmetasploit o Airbase-ng, que permiten crear access points que simulan los de una empresa, y de esa forma toman el control de la PC de un usuario a través de su placa de red. "Este tipo de ataque es bastante común y es el que hacen los chicos que empiezan a probar herramientas de hacking disponibles en la Red", apunta Iván Arce, CTO de Core Security Technologies.

No es casual que los estudios sociológicos sobre el riesgo se preocupen tanto por explicar la noción de heurística, tan afín al mundo de la seguridad informática. "La metodología para evaluar riesgos es muy eficaz para entender por qué un experto es capaz de provocar calamidades en un sistema con riesgo usando software de simulación. Porque incluso las personas más capacitadas tienden a fijar la atención en problemas aislados en lugar de analizar los fenómenos que son sistémicos y que son los que van a traer problemas", define el teórico Cass Sunstein en su libro "Riesgo y razón", publicado poco tiempo antes de su asunción como administrador de la Oficina de Información y Asuntos Regulatorios de la Administración Obama en Estados Unidos.

Este sociólogo de la Universidad de Chicago, que se hizo conocido por su obra Republica.com, remarca que la metodología heurística permite tomar en cuenta sucesos aparentemente inconexos, y vincularlos de tal modo que permitan encontrar una solución ante un riesgo potencial. "A partir de esta metodología, es necesario evaluar los riesgos potenciales de cada acto, con el objetivo de entender si el sistema en su conjunto está en peligro o no", analiza.

Foto: Gustavo Fernández

"Encriptamos las comunicaciones en grupos de celulares"

Hugo Scolnik,
director de Encriptel

El cuento del tío

En los últimos tiempos, la cuestión de la seguridad informática fue tomando una relevancia cada vez mayor, junto a la definición del rol del CISO (Chief Information Security Officer). Si bien aún son pocas las empresas que crearon el puesto dentro de su organigrama, cualquier empresa con un volumen importante de información se preocupa por la integridad de sus datos. "Debe haber un responsable por la seguridad de la información, que puede tener también el apoyo de consultores externos. En muchos casos, esto recae en el gerente de seguridad física", explica Gustavo Aldegani, profesor de Seguridad Informática de la Universidad de Belgrano y consultor de empresas. "Pero, como muchas amenazas provienen de Internet, quien administra ese recurso dentro de la empresa también influye a la hora de tomar decisiones", agrega.

Es una lástima que esta posición sea aún menos popular que la del CISO. Pero en plan de usar siglas para todos los cargos, se podría imaginar que ese rol lo cumpliría el ChInO (Chief Internet Officer), un experto en comercio electrónico, reputación online, seguridad informática e ingeniería social, algo bastante improbable por el momento. "Una compañía puede haber comprado la mejor tecnología de seguridad, entrenado a su personal y vigilar su comportamiento, y sin embargo seguir siendo completamente vulnerable. El punto flojo siempre es la ingeniería social, el lugar por donde pasan todos los ataques", desalienta Kevin Mitnick, un hacker rehabilitado en las clínicas del FBI y la CIA norteamericanas, desde su libro "The art of deception" (El arte del engaño). En sus conferencias por el mundo —cobra unos U$S 20.000 por una hora de exposición— disfruta avisando a los CIOs que, además de asegurar sus sistemas, preparen a su gente contra los engaños más habituales de la vida real.

Celulares blindados

Con el auge de los celulares inteligentes, los ataques a la plataforma móvil empiezan a tener mayor frecuencia. Una forma de asegurar las comunicaciones consiste en crear una red privada virtual (VPN) donde se realizan las comunicaciones seguras. Este esquema es usado en las empresas, que colocan un firewall y dispositivos de hardware. Basada en ese esquema se encuentra la tecnología de Encriptel, que realiza el cifrado de las comunicaciones celulares dentro de un entorno VPN utilizando un ser-

vidor propio. “Encriptamos las comunicaciones en grupos de celulares, a los cuales asignamos un número corto que permite la comunicación gratuita por voz y chat entre los aparatos dentro de una misma red”, explica Hugo Scolnik, director de Encriptel. Esta empresa fue formada en partes iguales por Firmas Digitales, de Scolnik, y Primary, que provee software para servicios financieros.

“Desarrollamos este modelo, que utiliza muy poco ancho de banda de la red 3G, con el fin de generar entornos seguros para empresas y áreas de gobierno que necesitan usar canales cerrados que no puedan ser espiados por un eventual hacker”, detalla Matías Castellani, CTO de Primary, que aportó parte de los $ 500.000 que demandó la creación de la empresa.

Para que estas tecnologías sean útiles es necesario establecer pautas de seguridad, como la creación de un comité de crisis. “Ante la posibilidad de robo de información las comunicaciones pueden pasar a un canal encriptado y los principales ejecutivos se comunican entre ellos de esa forma”, explica Aldegani.

“Hay algunos antivirus para celulares, pero lo cierto es que hoy hacen que pierda rendimiento. El principal problema con los celulares es que hay una tendencia muy fuerte por parte de los usuarios hacia el ‘jailbreaking’, que consiste en quebrar la seguridad de los sistemas operativos de los celulares y las tablet PCs para poder instalar aplicaciones que no están permitidas por el fabricante o que tienen un costo para el usuario, como en el caso de los juegos”, destaca Arce, de Core Security Technologies.

A eso hay que sumarle que cuando un usuario recibe un smartphone, más allá del uso corporativo, también se lo apropia culturalmente y comienza a darle nuevos usos, algunos de ellos potencialmente riesgosos para las empresas. “Algunos ataques son de instalación de malware, hay robos de credenciales de autenticación online y de esa forma pueden acceder a redes de las empresas. Esos ataques se dan en celulares con Wi-Fi, que en el perímetro del hogar se conectan al access point, que quizás no tiene los niveles de seguridad de una empresa. Se están viendo ataques y problemas de seguridad en los teléfonos”, alerta Arce.

> “Cada vez hay menos accesos con protocolo WEP, que fue vulnerado en 2006”
>
> **Julio Ardita,**
> director de Cybsec

Lo cierto es que los dispositivos móviles se volvieron cada vez más vulnerables a todo tipo de ataques, ya que a los nuevos smartphones los usuarios los utilizan como agenda, directorio y cliente de correo electrónico, debido a las capacidades de computación que poseen, más cercanas a una PC que a ese aparato que sólo permitía hablar a través de él. ■