

LOS EXPERTOS EN SEGURIDAD INFORMÁTICA ESTÁN CADA VEZ MÁS COTIZADOS EN LAS EMPRESAS

Atacantes y defensores

TEXTO: ALBERTO MARTÍN

Para muchas empresas, más de las que se pudiera pensar, es más importante para su negocio que nadie entre en su red informática sin su permiso a que les roben una buena suma de dinero. Tanto es así, que tanto empresas como instituciones cada vez dedican mayores recursos a la seguridad de sus redes, lo que ha convertido a los especialistas en seguridad —que normalmente antes han sido consumados *hackers*— en unos de los profesionales de la informática mejor remunerados.



Quien accede de manera ilícita a una red informática no sólo puede robar información, sabotearla, introducir virus o troyanos, sino que incluso, por ejemplo, puede usurpar identidades y delinquir en nuestro nombre. ¿Es posible evitarlo? "La verdad es que en un porcentaje elevado sí —responde Javier García Villalba, director del curso "Seguridad práctica en redes"—. En la mayoría de los casos, sobre todo cuando hablamos de evitar que accedan al ordenador de nuestra casa, basta con adquirir una serie de hábitos. Son cosas sencillas, de sentido común, como abrir sólo los correos electrónicos conocidos, no abrir nunca los ficheros adjuntos si no sabemos quién nos los envía, instalar *antispam*, que mucha gente no lo hace porque a veces falla y nos elimina correos importantes; escribir la dirección completa de nuestro banco en lugar de redireccionarnos, incluir en la contraseña de nuestro equipo signos de puntuación y no sólo números o letras que es como si no pusiéramos contraseñas... En suma, con mucho sentido común y con alguna regla básica se pueden evitar el 90 por ciento de los ataques", concluye García Villalba, que dirige en la Facultad de Informática el Grupo de Investigación de Análisis, Seguridad y Sistemas.



J. DE MIGUEL

El diez por ciento restante de ataques se divide en tres grupos. Unos, la mayoría, proceden de organizaciones delictivas muy organizadas que cuentan con informáticos de contrastado nivel. Un segundo grupo, por desgracia cada vez más numeroso, proviene de los propios Estados y sus agencias de seguridad y sus ejércitos, que con Estados Unidos a la cabeza, dedican ingentes cantidades de dinero y recursos para acceder a cuanta información gustan. "Contra este tipo de ataques es prácticamente imposible hacer nada, ya que dedican potentes supercomputadores a descifrar cuantas trabas se les quiera poner", señala el profesor García Villalba. El tercer grupo es el más curioso de todos, ya que lo forman *hackers* aficionados, cuya única intención es "presumir" de haber entrado en una o en otra red. "Existen blogs en los que cuentan hasta dónde han sido capaces de entrar e incluso se organizan congresos semiclandestinos en los que cuentan sus experiencias". Lo curioso es, como ya ocurriera en Estados Unidos en los 70 cuando alguno de los principales

COMO OCURRIERA EN ESTADOS UNIDOS EN LOS 70 CUANDO ALGUNO DE LOS PRINCIPALES ESTAFADORES BANCARIOS FUERON FICHADOS POR LOS PROPIOS BANCOS PARA MEJORAR SUS SISTEMAS DE SEGURIDAD, HOY SON ESTOS HACKERS LOS QUE SON FICHADOS POR LAS EMPRESAS PARA CONFIARLES LA MEJORA DE SUS SISTEMAS DE SEGURIDAD INFORMÁTICOS

estafadores bancarios fueron fichados por los propios bancos para mejorar sus sistemas de seguridad, hoy son estos *hackers* los que son fichados por las empresas para confiarles la mejora de sus sistemas de seguridad informática.

Los veintisiete estudiantes en el curso matriculados que dirige García Villalba no son, que se sepa, consumados *hackers* y sí estudiantes o titulados del ámbito de la informática que quieren dirigir su futuro profesional a este ámbito de la seguridad de redes o, sencillamente, quieren ampliar sus conocimientos en este área. Como subraya el profesor García, se trata de un curso eminentemente práctico, aunque por supuesto introducido con unos mínimos conocimientos teóricos. Participan no sólo profesores del Grupo de Investigación de Análisis, Seguridad y Sistemas, sino incluso de la Universidad de Basilea (Suiza) o profesores formados en el SegLab de la Universidad de Davis (California), uno de los más prestigiosos del mundo. Precisamente las prácticas del curso están inspiradas en una de las prácticas más famosas de este labo-

OTROS CURSOS

◆ SISTEMAS DE INFORMACIÓN GEOGRÁFICA: ARC/GIS

El profesor Javier García Puebla dirige este curso que se adentra en el uso de las principales aplicaciones de los sistemas de información geográfica, así como de los sistemas ráster y vectoriales. Curso eminentemente práctico, que se viene impartiendo desde la primera edición de la ECV, y que en esta ocasión se desarrolla en las aulas de informática de la Escuela Universitaria de Estudios Empresariales.

ratorio, la que enfrenta a los estudiante de Davis con los del Laboratorio de Seguridad Nacional de Los Alamos, también de Estados Unidos, para ver quién es capaz de vulnerar la red del otro. "Hemos creado dos subredes y dividido a los estudiantes del curso para que unos se defiendan de los ataques de los otros. El problema es que a veces encontramos alguna traba al creer alguien de la facultad que tenemos motivos belicistas en vez de académicos", concluye