ESTILS

El 'hacking' ètic, una pr

L'hàbit d'avaluar els riscos informàtics a través de tècniques 'hacker' compta cada vegada amb més professionals i clients

NEREIDA CARRILLO
BARCELONA

Diuen que la millor defensa és un bon atac. D'aquesta filosofia beu, en certa manera, el *hacking* ètic, una pràctica empresarial que consisteix a examinar els errors de seguretat d'un sistema informàtic mitjançant tècniques *hacker*, és a dir, simulant-hi atacs. En els últims temps s'ha incrementat el nombre de professionals que s'hi dediquen i el nombre de clients que ho demanen. Administracions, empreses i organitzacions volen que els *hackers* ètics, també coneguts com a *hackers de barret blanc*, els descobreixin els seus forats a internet. I poder-los tapar abans que hi entrin els *hackers* que volen robar o destruir dades, els coneguts com a *hackers de barret negre*.

Tot i el ressò d'alguns atacs recents, els professionals lamenten que la seguretat informàtica encara no sigui prioritària. "No s'actua de manera proactiva", es queixa Kenneth Peiruza, director de tecnologia a la consultora GNU Networks i professor d'administració de sistemes. Peiruza afegeix que sovint es busca un consultor de seguretat després d'un incident.

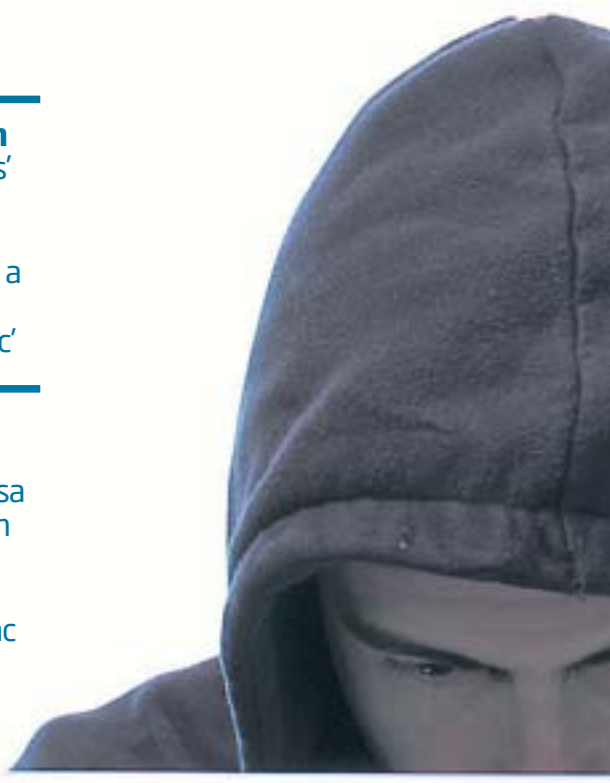
Els bancs, els més auditats

Els que més demanen aquests tests de seguretat són els bancs, però també grans corporacions, administracions públiques i partits polítics. No és estrany, ja que són també els que figuren més sovint en el punt de mira dels delinqüents informàtics. Però ningú és invulnerable i la responsabilitat no hi entén de mides. La llei obliga a tothom a vigilar per la seguretat de les dades personals, també a internet.

El test de seguretat comença amb un pacte de confiança amb el *hacker*, com explica Toni Haro, soci de Neotica Solutions i professor de *hacking* ètic al Cibernàrium: "Has d'estar d'acord amb l'empresa, saber fins on arribaràs, quina do-

Sobrenom
Als 'hackers' ètics se'ls coneix també com a 'hackers de barret blanc'

Reactius
Sovint una empresa només pren mesures després de patir un atac



Canvis legals el 2010

El Codi Penal preveu penes d'entre 1 i 3 anys de presó per als que robin, destrueixin o alterin dades electròniques de sistemes informàtics aliens. Però la llei orgànica 5/2010 hi va introduir canvis per castigar també el fet d'obstaculitzar o interrompre el funcionament d'un sistema informàtic sense autorització. Alguns veuen bé aquest canvi perquè penalitza atacs com ara el que va llançar Anonymous per tombar les webs de la SGAE i el ministeri de Cultura, un atac de denegació del servei (DDoS) que no comporta robar dades, sinó saturar una web intentant accedir-hi de manera massiva. D'altres ho critiquen, com Peiruza, perquè també penalitza els atacs informàtics que, malgrat que es fan sense permís, no tenen com a objectiu robar, sinó, en ocasions, notificar els errors que s'han d'esmenar per protegir dades personals.

àctica en auge a la xarxa

cumentació aportaràs del que trobis i signar clàusules de confidencialitat". L'empresa auditada proporciona informació tècnica, com ara noms de domini i quines xarxes té. "I a partir d'aquí –explica Peiruza– fas cerques a internet per veure si trobes res més i comences a verificar els noms de domini per veure si els hi pots robar".

Els experts recomanen que es facin una o dues auditories a l'any, en funció de la mida de la companyia. Però, si canvia molt la web o els productes en línia, s'aconsella una periodicitat de tres mesos. La forquilla de preus pot oscil·lar entre els 1.000 euros o menys per a una empresa petita i els 150.000 que pot costar el servei a una gran corporació, on sol caldre un equip de quatre persones que hi treballin durant tres mesos.

Auditories
Els 'hackers' ètics signen contractes de confidencialitat abans de començar

Preus
Una auditoria pot costar des dels 1.000 euros fins als 150.000 per a grans empreses

Riscos causats per la imprudència

Atacar un ordinador o sistema no és tan fàcil com han retratat les pel·lícules de Hollywood, però, malgrat això, sovint es troben errors. Peiruza explica que en alguna auditoria només li van caldre 48 hores per accedir a dades sensibles i modificar-les. Hi ha webs que tenen problemes des de bon principi, però també riscos a causa del poc manteniment i de la imprudència: xarxes internes en què el nom d'usuari i la contrasenya són públics o són dades d'accés relativament fàcil, com el DNI d'algú, o tan intuïtives com *1234*.

Un altra pràctica de risc consisteix a llistar de manera pública els ordinadors, tot i que això s'ha corregit molt últimament. Tot plegat no ho posa difícil per als *hackers*, que, amb algun d'aquests errors, poden accedir fàcilment a dades personals com ara multes, llistes de morosos o dades de vols. Malgrat tot, quan obtenen els resultats de l'auditoria, la majoria d'empreses arreglen tots els errors crítics, però només una petita part de la resta de vulnerabilitats menys greus.

En contra del que puguem pensar, la majoria d'atacs provenen dels mateixos treballadors de l'empresa. "És gent que intenta accedir a llocs on no els toca accedir", explica Haro. De totes maneres, cada vegada es pren més consciència que estar connectats no és tan pràctic ni tan divertit si no és també segur. I les empreses hi aposten perquè la seguretat, valora Paco Sánchez, també soci de Neotica, "és una cursa de fons".

Els particulars tampoc no s'escapen de patir atacs en comptes de correu electrònic i xarxes socials amb diversos enganys i enllaços perniciosos. Els tècnics demanen sentit comú: "Hem d'analitzar-ho com si fos un fax o una trucada més –explica Haro–. La meva àvia, quan li trucaven per dir-li que li havia tocat alguna cosa, sempre responia que era impossible perquè no havia jugat a res". ▬

'Hackers' de tots colors: blanc, negre i gris

El concepte *hacker* no tenia anys enrere una connotació negativa. Es diferenciava entre els *hackers*, que intentaven colar-se com a repte i sovint notificaven o resolien els errors, i els *crackers*, que, per contra, atacaven per perjudicar. Amb el temps, la paraula *hacker* s'associa també a delictes i ara es parla de *hacking* ètic per tornar a diferenciar-ho.

En argot, però, les intencions es classifiquen per barrets i colors. El *hacker de barret blanc* (anomenat *white hat*) vol examinar punts febles i tapar-los, i ho fa amb permisos. Els *hackers de barret negre* són els considerats criminals, els *crackers*, que busquen notorietat a través de la malícia informàtica. I els *hackers de barret gris*, segons explica Haro, estan "en una zona indeterminada", és a dir, no perjudiquen a ningú però entren sense permís.

Els consultors de seguretat informàtica es consideren *hackers de barret blanc*, però sovint també hi ha qui quan arriba a casa deixa el barret blanc al penja-robes i agafa el gris. La majoria de *hackers* al món, de fet, porten barret gris. També hi ha *hackers de barret negre* reconvertits al blanc.