Els casos més usuals de criminalitat informàtica i cibernètica

DANIEL R. NIELSEN*

Agent supervisor especial de l'FBI (Oficina Federal d'Investigació)
dels Estats Units d'Amèrica

1. ELS DELICTES RELACIONATS AMB ELS ORDINADORS

Actualment —això ho sabem tots—, ens trobem en el pas de l'era industrial a l'era de la informació. En el rol tradicional de la policia un dels objectius de la seva actuació consisteix en la preservació dels béns i els drets entesos o vinculats a elements materials. Amb el canvi d'era, aquests béns materials evolucionen cap a un concepte lògic, menys tangible físicament, però amb el mateix grau de rellevància pel que fa a la necessitat de protecció legal i actuació policial. Per aquest motiu, les idees i els serveis adquireixen molta més importància al costat de les coses materials en el sentit tradicional. Però, com a policia cal protegir les idees i els pensaments de la mateixa manera que es protegeixen els béns materials.

Per això, si tenim prou recursos i coneixements per valorar l'impacte de les noves tecnologies en la comissió dels delictes, podrem integrar-les també en la investigació i facilitar-ne l'adaptació als nous reptes que se'ns presenten.

Tot i així, a banda dels coneixements i de l'experiència professional de cadascú, de cada policia, és molt important que tots els cossos de policia del món treballin en comú per fer front a la criminalitat informàtica i cibernètica. La comissió dels delictes relacionats amb els ordinadors acostuma a tenir un caràcter transfronterer, per això els vull transmetre aquesta idea que, per mi, és fonamental, és a dir que la col·laboració internacional en aquest àmbit és imprescindible per dur a terme les investigacions.

Davant d'aquest tipus de delictes, primerament cal tenir en compte una doble

* Abans d'ingressar a l'FBI —ara fa dotze anys—, Nielsen havia treballat set anys com a oficial de la policia de Seatle. Al començament era membre de les unitats especialitzades en la lluita contra els grups organitzats; més endavant va treballar en l'anàlisi forense dels ordinadors. Actualment, és agent supervisor especial de les brigades d'investigació dels delictes comesos contra els ordinadors que es troben en l'àrea geogràfica del nord-est dels Estats Units.

perspectiva: d'una banda els ordinadors i les xarxes informàtiques poden ser el *mitjà* utilitzat per cometre els delictes i, de l'altra, poden ser l'*objecte* del fet il·lícit.

Pel que fa als sistemes informàtics, hem de considerar els seus punts vulnerables, que es poden classificar en quatre categories:

a) els punts vulnerables del mateix ordinador, com per exemple la utilització de paraules de pas poc sòlides;
b) els basats en la xarxa, com ara els punts d'entrada desprotegits;
c) els basats en el lloc d'instal·lació del sistema, com és el cas dels servidors situats en zones obertes, o l'accés franc a persones que no són prou conegudes;
d) els basats en les persones: per exemple, en els casos de personal amb contractes temporals i casos d'acomiadaments, suposa un gran risc comunicar a una persona que administra un sistema que d'aquí a trenta dies el despatxaran.

Aquests punts febles dels sistemes davant del que significa la nova era de la informació, comporten també amenaces noves amb les seves peculiaritats, que podríem resumir en els punts següents:

a) una gran facilitat per obtenir les eines necessàries per produir el dany (per exemple, els *hackers*[1] poden obtenir-les per via Internet);
b) aquestes eines estan molt distribuïdes i es poden utilitzar sense haver de tenir gaires coneixements ni gaire preparació tècnica;
c) la globalització de les infraestructures implica exposar-se més a un atac potencial;
d) la interdependència entre els sistemes fa que les conseqüències d'un atac siguin menys previsibles i més severes.

Per tot això, es pot dir que l'estructura de telecomunicacions és la principal víctima d'aquesta nova era de la informació.

Amb relació a la procedència de les amenaces, s'ha de dir que les més perilloses són les que provenen de l'interior d'una organització. Sovint és molt més perjudicial el dany que pot causar una persona que porta tot el control del sistema que no pas el dany procedent d'un atac exterior.

2. Els *hackers*

La figura del *hacker* es pot definir mitjançant un seguit de trets característics:

1. Inicialment, el mot *hacker* servia per definir una persona amb grans coneixements tècnics en informàtica, un expert tant en llenguatge informàtic com en programació, que passa moltes hores davant l'ordinador per intentar trobar els punts febles dels sistemes. Actualment, aquest terme té un sentit negatiu perquè s'utilitza per definir les persones que aprofiten els seus coneixements per aconseguir un accés no autoritzat o danyar o destruir els sistemes informàtics i les bases de dades.

— solen ser persones joves, majoritàriament de sexe masculí
— tenen molt poques relacions socials i estan obsessionats per la tecnologia
— l'ordinador és el substitut de les relacions interpersonals
— acostumen a tenir una actitud antisistèmica i delegen obtenir coneixements prohibits, impulsats per una curiositat insaciable

El *hacker* maliciós centra els seus objectius en ordinadors, xarxes i sistemes telefònics i pretén traficar amb codis de telèfon, programes informàtics piratejats, targetes de crèdit i dispositius de frau en sistemes de pagament.

2.1 Els mètodes utilitzats

Per entrar als sistemes informàtics, els *hackers* recorren a diversos mètodes, com són els següents:

— Intenten utilitzar els *codis per defecte*, que són els que tothom coneix i entén perquè són els que apliquen els fabricants d'origen.
— També poden penetrar en els sistemes mitjançant els *ports de manteniment*, utilitzats per les grans companyies per gestionar els seus sistemes a distància sense que s'hagin de desplaçar els seus tècnics.
— Un altre mètode, molt prosaic però molt efectiu, és l'anomenat *dumpster diving*,[2] que consisteix a remenar els llistats i els manuals d'empreses que els han deixat per obsolets, però que poden ser útils per aplicar aquells coneixements a d'altres sistemes.
— En darrer terme, però no per això menys important, hi ha tota una sèrie de mitjans que anomenem *atacs tècnics*, que poden consistir a emprar les *portes posteriors*,[3] amb què simulen ser ordinadors amb accés autoritzat, o bé a utilitzar *sniffers*[4] per obtenir paraules de pas.

A banda dels mètodes tècnics, els *hackers* tenen un altre recurs que es coneix amb el nom d'*enginyeria social* i que es basa en la seva habilitat personal per fer-se passar per experts de les organitzacions utilitzant el llenguatge tècnic i especialitzat característic d'aquell col·lectiu, i arriben a fer creure a l'interlocutor que realment són persones de confiança.

2. Traduït literalment, vol dir capbussar-se dins les deixalles.
3. Les portes posteriors (de l'anglès, *back doors* o *trap doors*) són un mecanisme secret del programari i del maquinari que pot fer saltar els sistemes de protecció i, així, evitar-los. S'activa d'una manera aparentment innocent, perquè els programadors sovint instal·len portes posteriors en els seus codis per connectar-se amb el sistema i fer algunes funcions.
4. Traduït literalment vol dir ensumadors. En realitat són uns petits programes que busquen una cadena numèrica o de caràcters en els paquets informàtics quan travessen un node amb el fi d'aconseguir informació. Normalment, el seu ús és il·legal.

2.2 La resposta a l'amenaça

Cal destacar que l'èxit dels *hackers* és el fet de *compartir la informació*. Per aquesta raó, la clau de l'èxit policial en la lluita contra aquest tipus de delictes rau també, com a premissa bàsica, a compartir la informació amb la mateixa facilitat.

Tot i que hem parlat de *hackers* que actuen per interès propi i de manera individual, s'ha de tenir present la possibilitat que actuïn per encàrrec de governs que vulguin atacar les infraestructures del nostre Estat.

En el cas dels atacs fets pels *hackers*, la corba de cost/benefici o esforç/resultat tradicional perd el seu sentit, ja que amb molt poc esforç i amb un cost molt baix poden arribar a causar danys considerables.

Entre les amenaces més freqüents, cal tenir en consideració aquestes quatre:

— l'ús maliciós de la informació
— el bloqueig dels serveis
— la publicació d'informació reservada
— el canvi o l'alteració de la informació

Al mateix temps, s'ha de tenir en compte que les amenaces poden tenir diversos graus d'intensitat: poden passar de ser simples problemes o incidències sense gaire transcendència a convertir-se en delictes. En el grau més elevat, fins i tot poden constituir seriosos problemes d'espionatge o de terrorisme, amb la possibilitat de desencadenar un veritable estat de guerra (naturalment, electrònica, en el terreny que ens ocupa). Però, en cas d'un hipotètic estat de guerra electrònica, no s'identifica l'enemic de forma visible com en la guerra convencional, en què es vesteix un uniforme característic.

Ara bé, per a cada grau d'amenaça hi ha diferents organismes que se'n fan càrrec. D'acord amb l'escala dels exemples del paràgraf anterior, correspondria resoldre'ls a la policia, els serveis de contraespionatge i a l'exèrcit, respectivament.

No obstant això, en un exercici realitzat als Estats Units dissenyat per l'exèrcit, en què l'FBI tenia un paper de suport, es va veure que a la pràctica era el cos policial qui realment representava la primera línia de defensa davant d'un atac electrònic, mentre que l'exèrcit hi tenia un paper subsidiari.

D'altra banda, actualment una de les dificultats més grans per a la investigació i la persecució dels delictes és la utilització de la criptografia en les comunicacions a través de l'ordinador. Tanmateix, és un pas més en la utilització de la tecnologia, com ja va passar primerament amb l'aparició del telèfon i, més tard, amb la telefonia mòbil. És cert, però, que la criptografia representa un gran obstacle a l'hora de desxifrar els missatges interceptats, i més considerant que hi ha eines d'*encriptació*[5] gratuïtes i prou robustes.

5. Transformació d'un text original en un de xifrat o convencional, incomprensible per a una persona que no en posseix la xifra o la clau.

3. Conclusió

Després de tractar els aspectes més controvertits de la criminalitat informàtica i cibernètica, vull acabar la meva exposició encoratjant els membres dels diferents cossos policials a utilitzar Internet —si és que no ho han fet ja— de manera particular i individual perquè podran comprendre molt més bé el potencial i les dimensions reals que ofereix. És important, per això, perdre la por a la tecnologia.

Al mateix temps, els animo a conèixer més de prop i a aprofundir en els delictes relacionats amb la tecnologia; de fet, es tracta de tenir en compte certes variacions i uns matisos tecnològics específics i incorporar-los a la investigació tradicional.