CIÈNCIA I MEDI AMBIENT

El delicte informàtic provoca bilions de pèrdues a tot el món

Delinqüents a distància

La informàtica ha propiciat l'aparició d'un nou tipus de delinqüent. Amb afany de diners, per espionatge o per simple diversió, pot causar vertaders desastres econòmics i socials.

Un nou tipus de delinqüent està d'actualitat des de fa un temps. No actua amb els mètodes convencionals. Necessita tenir grans coneixements, però també pot obtenir molts beneficis amb els seus delictes o bé causar desastres importants. Es tracta del delinqüent informàtic, una figura òbviament inexistent fa uns quants anys, però que ara, amb la proliferació d'ordinadors, representa un perill com més va més important.

El delicte informàtic pot ser de tipus molt diversos. De la mateixa manera, les motivacions de cada un també ho són. En el cas del delicte informàtic, això pot ser especialment vàlid.

En la societat d'avui, la informàtica domina l'organització. No es pot concebre una empresa sense cap ordinador. I no cal explicar les necessitats dels bancs i caixes d'estalvis. Al voltant dels ordinadors gira tota l'organització d'empreses grans i no tan grans. I el nombre d'ordinadors domèstics va augmentant any per any.

L'ordinador no ha facilitat només la feina a les empreses i institucions. També ha proporcionat noves maneres de delinquir. La lluita contra aquest delicte és essencial, perquè amenaça de manera greu no sols l'economia de moltes empreses, sinó la mateixa seguretat de la societat.

El delicte informàtic més senzill i més estès deu ser la còpia il·legal de programes. Aquest fet varia a cada país. Una manera d'observar si el nombre de còpies il·legals és molt elevada seria comparar el nombre de microordinadors venuts amb el de programes venuts. Si la diferència és molt gran, molta gent treballa amb còpies il·legals.

A Anglaterra, la diferència és molt petita. Només hi ha un 15% més d'ordinadors venuts que de programes. L'augment és progressiu si estudiem Suècia, Suïssa, França, Bèlgica, Alemanya Federal, Holanda i Itàlia. I arriba a un punt màxim

La delinqüència informàtica amenaça la seguretat de moltes empreses.

a l'estat espanyol, on sembla que hi ha una proporció d'1 a 4 entre programes venuts i ordinadors.

ENCARIMENT DEL PRODUCTE

Aquesta xifra és molt aproximada, perquè a l'estat espanyol no hi ha un control sobre ordinadors venuts, que poden serne uns 300.000. Com la majoria són importats, sembla que no costaria gaire establir aquest control de xifres. Peró no s'ha fet.

La causa que a Anglaterra hi hagi poques còpies il·legals pot provenir del fet que la gent sigui més respectuosa, però els programes també són més barats. Aquí, el mercat és més petit i, en canvi, una empresa que produeix *software* —programes— ha de tenir la mateixa estructura. Això encareix el producte i porta a un cercle viciós, es fa pirateria perquè el producte és car i és car perquè les empreses tenen pèrdues a causa de la pirateria.

Per a Lluís-Ferran Martín, secretari general de l'Associació Espanyola d'Empreses de Software, un dels culpables de la infravaloració del *software* és l'administració: «Compra les màquines que necessita i només un programa o molts menys dels necessaris. No compra un programa per cada màquina i les grans empreses tampoc».

Correus, per exemple, va convocar un concurs públic. El guanyador va rebre la següent proposta: comprarien cent màquines, un programa i demanarien l'autorització per fer-ne còpies. Això és força difícil, per no dir impossible, ja que un programa conté alguns sistemes d'altres programes. Per tant, el creador no pot autoritzar la còpia d'un producte que conté alguns sistemes que no li pertanyen.

Un altre tipus de delicte és el virus i les bombes lògiques. Els virus són programes que s'introdueixen en els ordinadors i que poden *infectar* de diverses maneres, provocant que l'ordinador faci coses estranyes o bé destruint programes i dades. Es poden introduir a través d'un programa contaminat expressament, amb *software* legal, contaminat accidentalment o per xarxa telemàtica —de connexió entre ordinadors—. Les bombes lògiques són més perilloses. Destrueixen tota la informació. I finalment hi ha els cucs, que entren per via telemàtica i mengen fitxers.

MILERS DE MILIONS DE PÈRDUES

Les pèrdues per aquests fets són elevades. A l'estat francès, per exemple, es pro-

duïren pèrdues declarades per més de 150 milions de franc —uns 3.000 milions de pessetes— per virus i bombes lògiques. Però això no és més que una petita part de les pèrdues reals. Precisament, un dels problemes de la lluita contra el delicte informàtic és que moltes empreses no el denuncien, per por a perdre credibilitat davant el públic. No volen que la gent conegui la seva vulnerabilitat.

Per a Lluís-Ferran Martín, «la promiscuïtat causa la proliferació dels virus». Això vol dir que canviar disquets d'un ordinador a un altre pot fer estendre les infeccions per virus. El senyor Martín recomana que la gent només utilitzi disquets dels quals en conegui la procedència.

Moltes empreses tenen cura amb la contaminació. Algunes preveuen sancions molts dures per els treballadors que portin un disquets de fora. D'altra banda, amb la contaminació es crea un altre negoci fraudulent. S'anuncien vacunes o detectors de virus que en realitat no tenen aquests efectes. La gent pensa que protegeix l'ordinador, però en realitat està gastant diners per a res.

Sortosament, també hi ha vacunes eficients. Contra el famós Divendres 13, l'Associació Espanyola d'Empreses de Software va repartir 10.000 còpies de la vacuna anomenada Dissabte 14. Va tenir una gran demanada d'institucions públiques i privades, des de ministeris i conselleries fins a universitats, empreses multinacionals i empreses petites. Fins i tot és demanava des d'instituts i escoles, ja que a molts les notes es posen per ordinador. És una mostra que la informàtica està present a tot arreu.

Però tampoc els virus són la causa de les pèrdues degudes a delicte informàtic d'uns 3.900 milions de francs.

Les previsions encara són pitjors. D'aquí al 1991 es calcula que el delicte causarà el 60% de les pèrdues informàtiques globals. Cal pensar que hi ha molts riscos accidentals, com incendis o altres sinistres que afecten els ordinadors, robatori de maquinària o errors en la fabricació, en la connexió o en la realització de programes. Els sinistres d'aquest tipus són molt més que els delictes, però les pèrdues ocasionades per aquests darrers són molt més grans.

ELS OBJECTIUS DEL DELINQÜENT

Les motivacions del delinqüent informàtic, com hem dit abans, són molt diverses. Un autor francès, Philippe Rosé, doctor en ciències econòmiques, n'assenyala set de principals. El primer seria el dels *amateurs,* que cometen delictes per solucionar problemes financers. El segon és el dels *trastocats,* que tenen desequilibris psicològics més o menys greus. El tercer seria el del crim organitzat, com la màfia. Aquests encara són poc nombrosos.

L'espionatge seria la quarta motivació. Pot ser polític o bé comercial. Els delinqüents professionals que no pertanyen a xarxes de crim organitzat són el cinquè grup. El sisè estaria format pels *hackers,* caçadors de sistemes, que ho fan gairebé per addicció a la informàtica. Entren en bases de dades i les manipulen per pur plaer. Solen ser joves que dediquen moltes hores al seu ordinador. I el setè grup seria el d'organitzacions idealistes i terroristes. La llista es pot fer més extensa, però també es pot reduir a quatre motivacions principals, segons els objectius: benefici econòmic, adquisició de notorietat en els diaris i simple vandalisme, ideològics i psicòpates.

Una cosa sí que és comuna a tots: cal saber molta informàtica per a penetrar en xarxes d'ordinadors i manipular-les o bé organitzar fraus. El delinqüent informàtic ha de tenir una gran preparació en aquest camp.

Però el gran perill és que moltes xarxes estan interconnectades. Ja hi ha hagut molts casos de persones que han entrat en bases de dades teòricament inaccessibles, però que a més controlen milers d'ordinadors i que prenen decisions o reben informació delicadíssima. El jove americà que des de la universitat va introduir un virus a 6.000 ordinadors que depenien del Departament de Defensa, va provocar unes pèrdues d'uns mil milions de dòlars, però podia haver causat un desastre inimaginable. Pensem en els ordinadors que controlen xarxes elèctriques, serveis ciutadans o sistemes de defensa. Qualsevol persona que els infecti o els manipuli pot posar en perill tot un país.

Moltes empreses prenen mesures contra aquest perill. A les sales d'ordinadors hi ha guàrdies jurats que les vigilen. Les institucions financeres tenen departaments de seguretat informàtica. Al mateix temps, hi ha altres maneres de protegir-se de l'accés des de l'exterior, com les xarxes locals. Però en aquests casos es dóna un problema: la interconnexió dels ordinadors d'una mateixa empresa pot fer que un treballador qualsevol tingui accés a l'ordinador del di-

rector general. Això fa que s'instal·lin ordinadors fora de la xarxa local, vulnerables des de l'exterior. Però a més, es pensa que un 60% dels delinqüents informàtics provenen de la mateixa empresa.

A més, no s'ha de contemplar només la pèrdua econòmica directa. Les empreses tenen una cosa de gran valor: la informació. Els nous productes, els seus plans financers, els seus fitxers realitzats amb anys de treball. Tot això se'n pot anar en orris i provocar un perjudici incalculable.

BUIT LEGAL

Però la legislació, en aquest cas, va per darrere del delicte. Als països on la justícia es basa en el dret romà, el jutge no pot considerar delicte allò que no estigui contemplat en el Codi Penal. A l'estat espanyol només fa dos anys que està penada la còpia il·legal de *software* i no es parla de cap altre delicte. Encara no hi ha cap sentència en aquest sentit. A l'estat francès s'han fet lleis amb penes de dos mesos a cinc anys i indemnitzacions fins a 100.000 francs —uns dos milions de pessetes— per introducció fraudulenta en una base de dades, impedir el desenvolupament d'un sistema o fer ús il·legal de documents informatitzats. Als Estats Units existeix la «Equity», que permet al jutge considerar si hi ha o no delicte. Hi ha propostes de llei que contemplen més de quinze anys de presó.

Lluís-Ferran Martín explica que «la pirateria de programes és un delicte contra la propietat intel·lectual i es pot castigar amb penes d'1 a 3 anys. En canvi, robar diners és un delicte major i la propietat immobiliària és pràcticament inviolable».

Aquest buit legal no permet actuar contra el delicte informàtic, la qual cosa implica que moltes empreses i institucions es troben indefenses davant la justícia. La previsible extensió de la informàtica en els pròxims anys farà que les conseqüències del delicte informàtic siguin cada vegada més greus. Actualment les xarxes financeres americanes transfereixen cada dia un bilió de dòlars. I es preveu que a l'estat francès l'any que ve es realitzin 20 milions d'operacions interbancàries diàries. L'atac a aquesta xarxa pot provocar desastres financers. I atacar aquest sistema de telecomunicació pot aturar el funcionament de tot un país, mentre el delinqüent informàtic es troba qui sap a on, còmodament assegut davant la seva pantalla.

Xavier Duran