Què faria un empresari si descobrís que un empleat filtra informació rellevant de l'empresa a la competència? Els experts recomanen discreció, assessorament permanent i, sobretot, respectar escrupolosament el procediment legal.

Espies a l'oficina

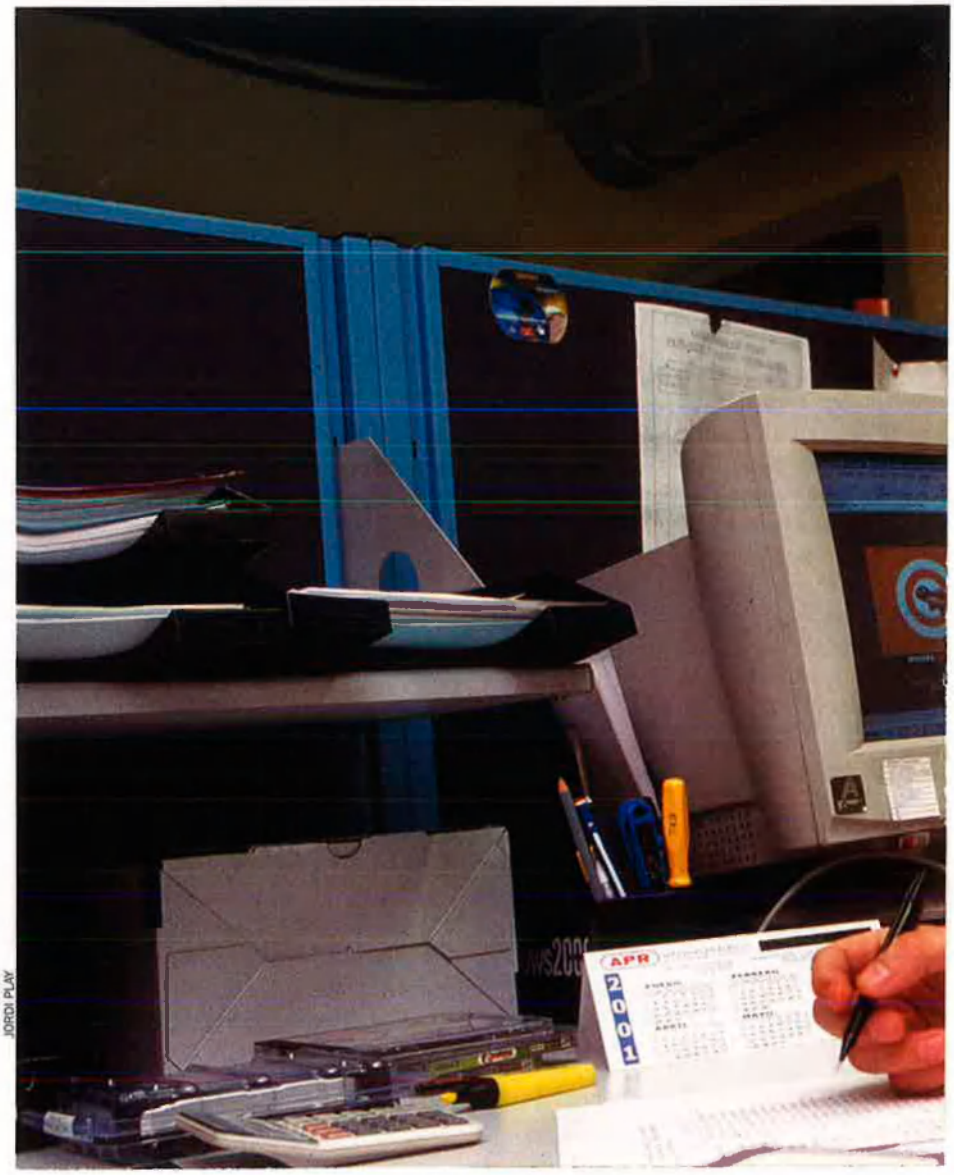
En Joan Martínez –nom fictici per a un cas real– acaba de penjar el telefon bocabadat i espantat alhora. El cap de l'empresa de la competència, amb qui manté una relació professional cordial, l'acaba de trucar per avisar-lo que una persona li ha ofert tota la base dades de la seva companyia. Martínez sap perfectament qui és el "traïdor": un antic empleat a qui va acomiadar per falta de professionalitat. Tot i així, no s'atreveix a denunciar-lo per por a una inspecció relacionada amb la normativa de protecció de dades.

Aquest cas és només un entre els milers que es produeixen al món de la petita i mitjana empresa. Tant és així que, segons dades de l'empresa d'investigació privada Winterman, un 65% de les consultes que reben tenen relació directa amb la competència deslleial i amb el robatori d'informació confidencial.

Tots els experts coincideixen a advertir que no és un problema que afecti només les grans multinacionals. No en va, el 90% de les empreses de l'estat són petites i mitjanes empreses. "En realitat, els atacs que provenen del món de la informàtica no amenacen les empreses pel fet de ser conegudes, sinó perquè, senzillament, poden fer-ho", afirma Daniel Arnanz, responsable de Solucions Corporatives de Symantec Espanya. Arnanz es refereix bàsicament als atacs que provenen de *hackers*, però ell mateix recorda que la seguretat informàtica i la vulnerabilitat global d'una empresa formen part, en realitat, del mateix concepte.

Lladres virtuals. La progressiva informatització de tots els processos a la gran majoria de les empreses –fins i tot les de reduïdes dimensions– ha creat un mercat natural per als investigadors de delictes digitals. Aquest és el cas d'INCIDE, constituïda per Winterman com a empresa especialitzada en l'actuació davant del delicte digital. "Fins fa uns anys, quan un empresari ens confiava una sospita de deslleialtat, seguíem els passos del treballador fora de la feina", explica Enric Vilamajó, director adjunt de Winterman. "Ara, en canvi –afegeix–, un treballador pot passar tota la informació que vulgui a l'empresa de la competència sense canviar el més mínim detall de la seva rutina de treball."

Per això la solució a aquest nou tipus de delicte exigeix fer una investigació més sofisticada, com explica Abraham Pasamar, expert en consultoria de Seguretat i director executiu de la filial INCIDE. Pasamar recorda que qualsevol moviment que faci un treballador utilitzant el sistema informàtic d'una empresa deixa un rastre, per molts coneixements que tingui l'empleat. I davant d'un cas com aquest –afegeix– la policia no és una opció realista: "Tant els Mossos d'Esquadra com la Guàrdia Civil tenen departaments especialitzats, i encara que molt sovint són gent preparada i entusiasta, el fet és que prou feina tenen perquè a sobre hagin d'investigar casos de sustracció d'informació procedents d'empreses privades."



JORDI PLAY

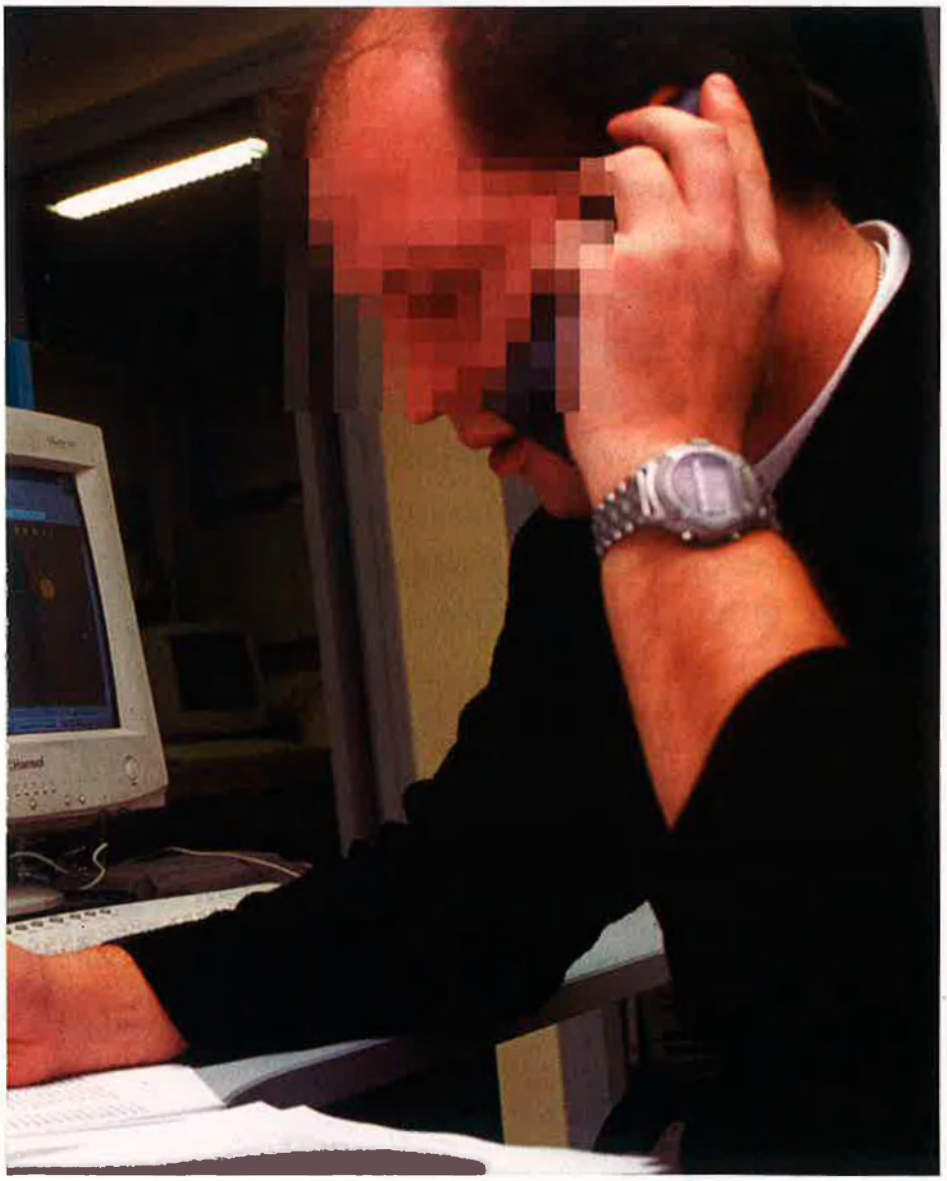
Com reaccionar? Davant d'una sospita fonamentada, el primer que ha de tenir en compte l'afectat –en aquest cas, l'empresari– és el que no ha de fer. Per exemple, no tafanejar en l'ordinador del sospitós ni llegir els seus correus electrònics. "Un error en el procediment podria desbaratar les possibilitats d'èxit de la investigació", assegura Pasamar. L'actuació correcta seria, doncs, cercar assessorament legal des del primer moment, i fins i tot demanar la intervenció d'un notari que certifiqui els moviments de l'empresa. L'objectiu final és garantir els drets d'intimitat del treballador, que d'aquesta manera no podrà argumentar una intrusió il·legítima.

Un cop fet això, és recomanable que els tècnics que investiguen els moviments compleixin certs requisits, bàsicament que tinguin experiència en processos similars i que puguin recollir tota la informació de les màquines amb categoria de pèrits. "Això esdevé fonamental en el moment en què el jutge demana dades pericials", explica Pasamar. "Lògicament, si qui ens contracta és l'empresa mateixa, probablement el jutge o els advocats del treballador demanaran un 'contra-informe' d'un pèrit independent. Però si aquest segon pèrit confirma que li donem totes les facilitats, s'acabarà comprovant que la nostra intervenció ha estat fiable", conclou.

Una empresa pot arribar a desaparèixer

Les conseqüències d'un robatori d'informació o una actuació informàtica inadequada poden ser dràstiques per a una empresa, però en el cas d'una microempresa poden posar en perill la seva existència, com explica l'expert Abraham Pasamar. Aquest és el cas d'una petita societat dedicada al negoci de la gestoria i assessoria d'empreses que un dia va comprovar que la totalitat de les seves dades havien desaparegut. La primera reacció de l'empresari va ser la de cridar l'informàtic, que de seguida es va adonar que la situació excedia el seu control.

Després de recórrer a experts en investigació digital, van arribar a la conclusió que havien estat víctimes d'un atac extern, i que no solament s'havien esborrat aquelles dades, sinó que tampoc s'havien arxivat correctament les dades de *back-up* o còpia de seguretat. Entre altres documents, hi havia centenars de nòmines de treballadors de diverses empreses. Finalment, després de moltes hores de feina, es va poder fer una reconstrucció del material perdut. L'empresa havia salvat la vida... pels pèls.



Difícil prevenció. La principal diferència entre els atacs informàtics comuns –els d'un *hacker* que boicotegi una web, per exemple– i el robatori de dades digitals, és que en aquest segon cas la prevenció és més difícil. Òbviament, existeixen les recomanacions bàsiques, com ara limitar els "privilegis", ser discret amb les contrassenyes i, en definitiva, aplicar una mínima política de discreció.

Malgrat tot, el perfil d'un "lladre informàtic" respon a una persona en qui teòricament es pot confiar, com per exemple un directiu o un administrador de sistemes. És per això que l'activitat a priori resulta, si més no, complicada. Pel que fa als preus, generalment es treballa amb preus per hora de feina, de manera que resulta difícil concretar una quantitat. A títol orientatiu, INCIDE treballa amb preus d'entre 80 i 120 euros per hora.

Reprenent el cas amb què començàvem aquest article, Joan Martínez va tenir molta sort: el comprador potencial va resultar ser una persona honrada. Però, si no hagués estat així, quants diners li podria haver costat el robatori? I el que és pitjor: sense assabentar-se'n.

Aureli Vàzquez