Anno 62° N. 94 Quotidiano
Sped. abb. post. gruppo 1/70 - Arretrati L. 2.000

l'Unità

ORGANO DEL PARTITO COMUNISTA ITALIANO

☆ DOMENICA 5 MAGGIO 1985

LIRE 1000

INCHIESTA / *Banche in allarme, si teme l'ondata dell'attacco elettronico*

Crimine al computer la rapina del futuro

ROMA — *È pulito, poco fatticoso, molto redditizio e non lascia tracce. È il crimine al computer, la rapina del futuro. Lance termiche, auto che sgommano per la fuga, assalti ai «caveaux», mitra e pistole non servono più: basta mettersi davanti alla tastiera di un terminale, avere un po' di cognizioni in materia, un po' d'ingegno e la necessaria propensione al furto e il gioco è fatto. Perché, almeno fino ad ora, le banche hanno dimostrato difese di burro contro l'attacco elettronico. Qui in Italia siamo ancora all'abc, o quasi, dell'informatica applicata al lavoro, siamo nella fase dell'euforia della scoperta, della introduzione e dell'entusiasmo conseguente. Ma poco si è pensato all'altra faccia della medaglia, alla prevenzione, ai controlli, agli sbarramenti. E la criminalità in pantofole veleggia.*

Quello che sta succedendo agli sportelli del Bancomat lo dimostra abbondantemente. Nel giro di pochi mesi è già la seconda volta che vengono presi d'assalto; l'ultimo episodio conosciuto risale al «week-end» di Pasqua. Un ignoto e abile truffatore si è portato via centinaia di milioni contraffacendo le tesserine magnetiche per il prelievo e svuotando indisturbato i distributori di banconote di mezz'Italia. Gli esperti dicono che è più facile di quel che si creda ricopiare le bande magnetiche e scoprire i codici personali e «segreti» dei singoli utenti.

Le banche sono prese in contropiede, imbarazzatissime perfino nel comunicare le notizie dei furti, incassano il colpo e sembrano incapaci di una reazione all'altezza. Il danno per loro è ben più grave di quelle migliaia di biglietti da diecimila portati via senza colpo ferire. È l'immagine che rimane scalfita e per un istituto di credito, come è noto, l'immagine è mezzo capitale. Si diffonde l'allarme e anche in Italia finalmente si comincia a pensare come neutralizzare il rapinatore in camice bianco. Forse per la prima volta nel nostro paese un seminario pubblico è stato dedicato allo spinoso argomento. Si è tenuto a Roma nei giorni scorsi ed è stato sponsorizzato da nomi illustri: i Lloyd's di Londra, la Ross Collins italiana, l'ambasciata e la Camera di Commercio inglese.

Sono le compagnie di assicurazione a buttarsi a pesce su quello che, per loro, è un affare carico di futuro. Gli episodi del Bancomat sono solo le prime avvisaglie, la vera valanga di criminalità elettronica deve ancora venire. Non sono solo le previsioni interessate delle compagnie di assicurazioni a dipingere di nero il futuro della computerizzazione bancaria e delle grandi imprese. Sottovoce, negli ambienti del credito e della finanza, si fa intendere che quello che appare all'esterno non è che la punta di un iceberg che si va ingrossando con il procedere dei sistemi di automazione e delle nuove tecnologie. Si dice che molte banche e perfino qualche grosso istituto pubblico abbiano preferito mettere tutto a tacere dopo la scoperta degli ammanchi, piuttosto che portare le cose in piazza.

Una rivista specializzata, «Management e impresa», sostiene addirittura che una società, per occultare un buco provocato da criminali elettronici, ha deliberatamente alterato alcune scritte contabili, con conseguente denuncia penale una volta scoperta la contraffazione. Cioè: meglio rischiare la galera che perdere la faccia. Il rapinatore elettronico conta molto su questa forzata omertà della vittima e va a rubare in carrozza. In Italia si sarebbero verificati già tre casi in cui furti al computer sono stati scoperti dalla Finanza e divulgati nonostante le resistenze dei dirigenti degli istituti di credito. Li riporta in un suo articolo la rivista di documentazione assicurativa «Insurance».

Ma è soprattutto l'esperienza americana che non fa dormire sonni tranquilli ai dirigenti delle grandi banche e delle imprese computerizzate. Negli «States» l'applicazione dell'elettronica e dei sistemi informatici al lavoro è senza dubbio più diffusa che da noi e la sua introduzione meno recente. Là hanno raccolto una casistica di «computer crime» così voluminosa da far impallidire. L'anno passato sono stati più di duecento i miliardi fatti uscire silenziosamente dalle banche americane con qualche semplice operazione alla tastiera di un terminale. Eppure là si sono posti il problema della prevenzione e della difesa da diverso tempo. Là hanno già assistito al proliferare della creatività e della fantasia elettronico-criminale.

C'è addirittura un dizionario del «computer crime» che elenca le varie forme di attacco finora conosciute. C'è, per esempio, il «data diddling», il sistema di alterazione più artigianale: chi ha o riesce ad avere in qualche modo l'accesso al computer può otturare i fori delle schede perforate o praticarne di nuovi per impartire ordini a suo piacimento. C'è il «salami techniques» che consiste nel furto di piccoli importi da un gran numero di conti bancari. I singoli saldi non vengono sostanzialmente alterati, il cliente non si accorge di nulla, ma l'operatore che ha fatto la cresta così tante volte, alla fine si mette in tasca un bel gruzzolo. C'è il «data leakage», una sottrazione di dati ad un terminale. A «Securicom 85», a Cannes, una ditta olandese ha dimostrato la possibilità di ricevere a distanza le radiazioni di un terminale: si può leggere da un posto lontano chilometri ciò che sta scritto sopra il video. Rientra in questa casistica il furto di notizie, qualche tempo fa, dall'Ambasciata americana a Mosca: il rumore delle macchine scriventi veniva recepito e decodificato a distanza.

C'è poi il «code 999», il più temuto. Le ditte che forniscono computer puntano sulla flessibilità dei programmi per coprire un mercato il più vasto possibile. Poi, al momento della vendita, straciano dai manuali di istruzione quelle parti non acquistate. Ma nella macchina comprata rimangono i programmi: chi se ne intende può rintracciarli e attivarli senza bisogno di istruzioni. L'uso che ne può fare, generalmente non è di carattere benefico.

Nella copiosa casistica di truffe tecnologiche ci sono già episodi che passeranno alla storia. Come quello della Equity Funding Corporation of America (Efca): manomettendo gli «input» dell'elaboratore i dirigenti della società fecero credere agli operatori di Wall Street di aver creato molte e lucrose assicurazioni sulla vita. Con questo credito fasullo giostrarono a piacimento nel mercato finanziario. Quando furono scoperti, il loro crac risultò di dimensioni gigantesche: un miliardo di dollari (duemila miliardi di lire).

Famoso è anche il caso Schneider, dal nome di un giovanotto che riuscì a copiare i sistemi elettronici di ordinazione della Pacific Telephone & Telegraph di Los Angeles. Per conto suo e a più riprese, Schneider ordinò materiale elettrico per un milione di dollari che poi piazzò privatamente.

Il crimine computerizzato è penetrato perfino nei paesi dell'Est. A Vilnius, in Lituania, ad esempio, alcuni addetti al computer di un'azienda hanno inserito i nomi di impiegati-fantasma nell'elaboratore e pagato loro gli stipendi. E in Italia ci sono già i sintomi di un salto di qualità da un livello artigianale ad uno più sofisticato. I giornali hanno parlato del tentativo di un impiegato di banca di trasferire illegalmente attraverso il computer una grossa somma di denaro presso un istituto di credito estero. È finita bene, nel senso che il rapinatore elettronico è stato individuato e arrestato.

Ma l'antichissima partita tra guardie e ladri è aperta. Fino all'ultimo «chip».

Daniele Martini

ROMA — L'interno di un istituto di credito e, sotto, un cliente che ritira denaro ad un Bancomat

I furti agli sportelli del Bancomat hanno dato il via La contraffazione delle tesserine magnetiche L'imbarazzo degli istituti di credito, che preferiscono tacere - I «colpi» da manuale che già fanno storia nel mondo