Avvenire

ANNO XVII N. 92 — Ss. Filippo e Giacomo — ** Venerdì 3 maggio 1985 L. 600

RAPINE

Banche sempre più allarmate per le azioni dei "virtuosi" del computer contro i forzieri

Il furto diventa scienza

di Gianni Flamini
inviato

ROMA. Una volta il cuore di una banca era la sua imponente cassaforte, bersaglio di sogni alla fiamma ossidrica.

Adesso, invece, il cuore di una banca è il suo computer.

Ma i sogni non sono cambiati, è cambiato piuttosto il modo di conquistare quel cuore. Sono modi da società post-industriale, che alla fiamma ossidrica hanno sostituito l'informatica, scienza contemporanea.

Gli scassinatori si sono messi la cravatta e sanno tutto sul "software", sui "bit", sui "linguaggi", sui "passwords".

E riescono a intascare miliardi altrui senza doversi presentare di persona allo sportello, per pronunciare la fatidica frase: "Questa è una rapina".

Dipende anche dal fatto che l'analfabetismo informatico, fino a ieri garanzia di inaccessibilità ai nuovi santuari della rivoluzione tecnologica, si è venuto sempre più riducendo; che l'uso del computer è diventato sempre più semplice e che, contemporaneamente, i sistemi di controllo e di protezione dell'universo computerizzato sono rimasti indietro.

Adesso gli scassinatori, quelli che portano l'attacco al cuore della banca, usano tecniche che le società di assicurazione vanno affannosamente classificando. Si chiamano per esempio: "trojan horse" (cavallo di Troia), che consiste nell'introduzione fraudolenta nel computer di istruzioni di programmazione ad uso criminale; oppure "salami trick" (trucco del salame), col quale si istruisce il computer a sottrarre qualche centinaio di lire da ogni conto corrente, depositandole in un altro conto aperto clandestinamente; o addirittura "logic bomb" (bomba logica), una specie di bomba a orologeria messa a punto dal dipendente di una società che programmò il computer della sua azienda in modo che, se fosse stato licenziato, i nastri degli stipendi di tutti gli altri dipendenti si sarebbero automaticamente cancellati.

Ma c'è di peggio. Qualcuno è già riuscito a ricevere e decodificare a distanza il rumore delle macchine scriventi di un elaboratore elettronico, mentre proprio quest'anno alcuni scienziati olandesi hanno dimostrato la possibilità di intercettare addirittura le radiazioni di un terminale, riuscendo a leggere a chilometri di distanza i testi e le informazioni visualizzate su quello stesso terminale.

La fantasia e la creatività della criminalità informatica sono ormai talmente sbrigliate che soprattutto gli istituti bancari si sentono come tanti Fort Apache, sul punto di essere espugnati. I miliardi perduti in pochi anni sono un drammatico ammonimento. Per esempio, una delle più recenti e diffuse innovazioni come la carta di credito ha prodotto perdite che nessuno avrebbe immaginato. Negli Stati Uniti i possessori di carta di credito sono 75 milioni e, due anni fa, gli istituti emittenti sono stati frodati per più di cento milioni di dollari.

E allora come garantire la sicurezza di Fort Apache? Purtroppo la sicurezza assoluta è impossibile; si può fare molto, ma non tutto. A dirlo, è un esperto del settore come l'ingegner Adalberto Biasiotti, della società assicuratrice Ross Collins Italiana, che ha appunto organizzato un convegno sulla strategia di difesa dal "computer crime". Ha detto: "La varietà delle aree di rischio per un sistema di elaborazione è tale che ben difficilmente potranno essere tutte coperte. Il completamento della protezione può solo essere affidato ad una buona assicurazione".

Non staremo a dire quale società assicuratrice è la più idonea, visto che il convegno è stato promosso da una di esse.

E tuttavia qualche dubbio resta. Dubbio raccontato in lingua inglese da David Newman, che ha dato conto di alcune peripezie vissute dai "Lloyd's" di Londra.

E la storia di 21 milioni di dollari che, partiti dal Sudamerica, sono approdati nelle banche di mezzo mondo, Europa compresa. Nessuno riesce più a recuperarli, ormai sommersi in un groviglio di telex, di ordini computerizzati, di trasferimenti e di frazionamenti. Dove andare a cercare le singole responsabilità in una simile giungla? A chi dare la colpa?

E poi c'è il resto. Ossia c'è il silenzio e la non collaborazione delle vittime.

Circostanza ben nota a Carlo Sarzana, magistrato che al ministero della Giustizia studia da anni l'evolversi dei "computer crimes". Presente al convegno, ha detto: "Le vittime, quasi sempre istituti bancari, ritengono che le ripercussioni negative derivanti dalla notorietà di una perdita subita potrebbero provocare effetti dannosi nella fiducia del pubblico e quindi causare danni ancora maggiori. Perciò le vittime quasi sempre preferiscono non denunciare i fatti, in qualche caso arrivando addirittura a comprare il silenzio del criminale".

Ma la legge guarda da lontano e interviene molto raramente.

Ricorda l'ingegner Biasiotti: "Sappiamo di alcuni casi in cui frodi a mezzo computer furono scoperte e divulgate da ispettori della Finanza, mentre i dirigenti delle banche interessate avevano preferito nascondere i fatti. Ma solo in un caso è seguita una denuncia penale, in quanto erano stati alterati alcuni dati contabili proprio per celare l'accaduto".

Anche l'Italia è dunque patria del "computer crime", e questa non è una novità. Ma se ne parla poco, anzi meglio non parlarne.

Incalza Biasiotti, esperto di sicurezza: "In Italia il 'computer crime' c'è, ma nessuno lo dice". E conclude, da esperto di assicurazioni: "A chiedere protezione vengono molte banche, soprattutto casse di risparmio. Vuol dire che probbilmente hanno già subito danni". Però non risulta.

I ladri informatici usano la scienza e la tecnica della società post-industriale, ma hanno dalla loro parte anche una vecchia risorsa da società preindustriale: l'omertà.