Un nuovo settore d'attività si è aperto per le assicurazioni

Quando il computer è «criminale»

La diffusione dell'informatica e della telematica nelle banche e nelle istituzioni finanziarie ha creato un nuovo rischio: quello dal «computer-crime» - I casi più clamorosi di truffe commesse grazie al calcolatore - I punti deboli dei centri di elaborazione dati - Da anni i Lloyds hanno messo a punto una polizza contro i rischi elettronici

L'assicurazione, in fondo, per certi aspetti è una scommessa. "Scommessa" calcolata con minuziosi calcoli attuariali, ma sempre scommessa. E come si può scommettere su tutto, o quasi, così non c'è rischio che non possa essere coperto da assicurazione. Recentemente l'inefficienza dello Stato da un lato ed il progresso tecnico dall'altro hanno aperto nuovi campi all'inventiva delle compagnie. Qualche esempio? Il collasso del sistema pensionistico e lo sfascio di quello sanitario stanno offrendo grosse opportunità a pensioni integrative e ad assistenza medica ed ospedaliera gestite su base privatistica da compagnie d'assicurazione. Ed il dilagare dell'informatica ha creato per le banche e le istituzioni finanziarie nuovi rischi, che le compagnie sono pronte ad assicurare.

La casistica del "computer crime", cioè di truffe e frodi commesse grazie al computer è già fittissima, e comprende episodi divenuti ormai quasi leggendari. A volte si tratta di errori banali, come quello dovuto al fatto che nel sistema inglese (e quindi nel computer) il punto che si mette dietro una cifra ha lo stesso valore che da noi ed in Europa in genere ha la virgola che segna i decimali. E così è accaduto che un greco si è visto accreditare invece di qualche migliaio di dollari, alcune centinaia di migliaia. Ha incassato senza batter ciglio, e da allora se ne son perse le tracce.

Altra volta invece la truffa è minuziosamente calcolata. Uno dei casi più clamorosi resta quello di un ignoto americano che, sotto falso nome, è riuscito a far partire da una banca americana un accredito di alcuni miliardi su una banca europea. Nel frattempo - ecco la trovata per certi aspetti geniale - aveva contattato i russi, chiedendo di acquistare una partita di diamanti. Ovviamente l'ente sovietico ha chiesto la copertura bancaria. La banca europea ha confermato l'esistenza dell'accredito, ed i russi hanno consegnato i diamanti. Poi hanno chiesto il pagamento alla banca europea, che ha trasmesso la richiesta alla banca americana, che è caduta dalle nuvole. E intanto il truffatore "elettronico" si godeva i suoi diamanti, che non hanno numeri di serie, non sono individuabili, e sono moneta contante e "pulita" in ogni parte del mondo.

In effetti l'uso del computer così come amplia le capacità operative di chi opera correttamente, amplia anche le possibilità del criminale. Per rendersene conto basta considerare questi dati: il "frutto" medio di una rapina bancaria, secondo dati della F.B.I. è, in America, equivalente a sette milioni di lire. Se invece è il dipendente di una banca ad organizzare una frode, il "colpo" frutta mediamente cinquanta milioni. Cifra quest'ultima che sale a ben 860 milioni di lire quando la truffa è organizzata per mezzo del computer. Più in generale, negli altri casi di "computer crime" la cifra truffata si aggira sul miliardo. Il rapinatore "in guanti elettronici" guadagna dunque, mediamente, da centoventi a centoquaranta volte più del rapinatore con la pistola.

Ancora oggi d'altronde, mentre l'informatica e la telematica si stanno espandendo sempre più rapidamente nel settore bancario, le difese contro questi "computer-crime" lasciano - secondo alcuni esperti - non poche maglie aperte. E' questa, ad esempio, l'opinione di Adalberto Biasiotti, uno dei maggiori esperti italiani in questo campo, che ha tenuto recentemente a Roma una relazione nell'ambito di un convegno organizzato dalla Ross Collins Italia.

Nell'ambito di quel Convegno sono state presentate alcune significative tabelle che evidenziavano appunto i "profili di rischio" di un Centro elaborazione dati. Nel caso di situazione "molto brutta", cioè di rischio molto alto, nella tabella erano raffigurati due teschi. Una situazione mediocre era simboleggiata con un teschio; una situazione media con un cerchietto. Una stella, due stelle e tre stelle raffiguravano poi rispettivamente le situazioni abbastanza buone, ed eccellenti. Secondo tale analisi, in un grande centro di elaborazione dati il margine di sicurezza è abbastanza buono. Una situazione di sicurezza mediocre si ri-

►

Dizionario del computer crime

DATA DIDDLING

E' il più semplice sistema di manipolazione. Consiste nella alterazione dei dati, prima o durante l'introduzione dei dati stessi nell'elaboratore.

L'operazione può essere compiuta da chiunque abbia a che fare con i dati stessi, utilizzando dei metodi assai semplici, come ad esempio l'otturazione di fori nelle schede perforate, la creazione di nuovi fori, la sostituzione di nastri e dischi con altri già contraffatti e via dicendo. Esistono numerosi casi documentati di tale attività.

TROJAN HORSE

Consiste nell'introduzione fraudolenta di istruzioni di programmazione, che non influiscono sull'esecuzione normale della istruzioni del programma.

La modifica delle istruzioni, con conseguente attività fraudolenta, può avvenire al verificarsi di azioni specifiche (introduzione di determinati password) o di eventi concomitanti, ad esempio una data prefissata e l'elaborazione di un determinato file.

La rilevazione di queste istruzioni abusive è estremamente difficile, in quanto possono essere celate in programmi composti da centinaia di migliaia di istruzioni.

Un Cavallo di Troia si può individuare facendo confronti, con procedure automatiche, tra una copia sicuramente genuina del programma e la copia sospetta.

SALAMI TECHNIQUES

Consiste nel furto o nella distribuzione di piccoli importi da un gran numero di conti, senza alterare sostanzialemtne i singoli saldi.

Il successo della frode è basato sul fatto che ogni utente colpito perde talmente poco, da non rendere rilevabile od interessante la rettifica.

Esistono molti esempi di queste frodi, specie in ambiente bancario. L'origine della frode è stata sempre rintracciata in un dipendente dell'istituto od in un programmatore con contratto a termine.

SUPER ZAPPING

Il nome è preso da un celebre programma di Utility della IBM, che consente le più complesse manipolazioni dei dati, senza lasciare traccia alcuna. Rientra nel più generale problema dell'uso controllato delle "restricted utilities" e le difese più efficaci sono quelle di introdurre delle strette procedure di controllo.

TRAP DOORS

Tutti i programmatori prevedono degli accessi privilegiati nel corso dei loro programmi, per consentire l'introduzione di subroutines o per consentire l'uscita da loop funzionali. Tali porte secondarie esistono anche a livello di circuito elettronico, potendosi ad esempio scavalcare delle sequenze fisiche o logiche di difesa (ad esempio la neutralizzazione di contatti di allarmi sugli sportelli dei computers).

Queste porte consentono l'introduzione surrettizia nei cicli di elaborazione, scavalcando i blocchi funzionali e logici.

LOGIC BOMB

Una bomba logica consiste in un programma che viene seguito in tempi periodici o prefissati, ed in ciò assomiglia al Cavallo di Troia.

In genere esso è usato a titolo ricattatorio o distruttivo, più che per l'alterazione fraudolenta.

Un celebre esempio è quello di un dipendente di una società petrolifera, che programmò il computer in modo che, ove il suo numero di matricola fosse stato tolto dall'elenco dei dipendenti (quindi licenziato!) i nastri di tutti gli stipendi si sarebbero automaticamente cancellati.

scontra infatti solo per il cambio del "passwords", cioè della parole d'ordine. Ma per un piccolo centro il quadro è già meno rassicurante. Molto brutta (due teschi) è giudicata infatti la situazione di sicurezza nel cambio dei passwords, nel "back up" e nella qualità di controlli di verosimiglianza. Mediocre poi la sicurezza per documenti e procedure di gestione, per la gestione della biblioteca, per il controllo accessi. Passando poi agli aspetti della sicurezza materiale, in un grande Centro d'elaborazione dati in genere è molto brutta la situazione per quanto concerne la sicurezza fisica della rete, mentre per i piccoli Centri sotto questo aspetto il livello di sicurezza è molto basso o mediocre addirittura per sette voci su undici: lo studio specifico della sicurezza, il controllo fisico degli accessi, il danno da acqua, la qualità dei mezzi di soccorso, il condizionamento, l'alimentazione e l'impianto elettrico, la sicurezza della rete.

Vien da pensare, in effetti, che il computer crime non ha avuto sinora un grande sviluppo (ma solo un decimo dei casi di truffa elettronica finisce con l'essere reso noto) perchè la "cultura elettronica" era ancora in molti Paesi, Italia compresa, un fatto assai circoscritto ed elitario. L'85% dei casi di frode sono perpetrati infatti da professionisti dell'informatica. Ma con la diffusione dell'uso del computer, con l'allargarsi delle conoscenze a cerchie sempre più vaste, si allarga parallelamente anche l'area di rischio. Banche ed istituzioni finanziarie naturalmente si sforzano di rendere la vita sempre più difficile a questi truffatori elettronici con l'adozione di opportune tecniche di difesa. Ma il lavoro da fare in questo campo sembra essere ancora molto. Ed alla fine, c'è un'area di rischio che solo una opportuna polizza d'assicurazione riesce a coprire. Non a caso già da alcuni anni i Lloyds di Londra hanno messo a punto una polizza contro il crimine elettronico.

A.L.