MEDIA DUEMILA

Caccia in banca al ladro informatico

ROMA. *Un bottino di 80 miliardi di lire nel 1985: è l'ammontare dei furti che subiranno le banche italiane a causa del* computer crime, *il furto elettronico attraverso gli elaboratori. Non che gli altri paesi stiano meglio di noi: in Francia si dovrebbero raggiungere, sempre in quest'anno, i 130 miliardi e negli Stati Uniti superare i mille.*

Queste cifre sono state previste da Adalberto Biasiotti, coordinatore tecnico della Compagnia di Assicurazione «Ross Collins Italia», alla presentazione a Roma della prima polizza di assicurazione in Italia contro tutti i rischi di frode e di sabotaggio con il computer. Biasiotti ha stimato che fino ad oggi le banche italiane hanno subito crimini informatici per un valore di almeno 30-40 miliardi, una cifra paragonabile negli ultimi tempi a quella dei bottini delle comuni rapine, ma destinata, nel giro di pochi anni, a divenire superiore di 10 volte, come già accade negli Stati Uniti. Difatti, secondo una statistica dell'Fbi, negli Usa il numero dei crimini informatici ha raggiunto quello delle rapine, ma mentre il valore medio di ogni atto criminoso tradizionale è di circa 7 milioni di lire, quello compiuto con un computer va da 860 milioni a 1 miliardo di lire.

«In realtà – ha sottolineato Biasiotti – il tetto del valore di un computer crime *non ha limite, poiché non prevede l'immediata "riscossione" del denaro sotto forma cartacea: può quindi raggiungere anche il doppio o il triplo del capitale sociale di una banca».*

Vediamo ora qual è la tipologia dei computer crime *più diffusi, secondo una statistica elaborata dallo* Stanford research institute, *sulla base di 633 casi. Il furto elettronico si compie nel 26% dei casi con la possibilità di accedere fisicamente al calcolatore, modificandone il programma o inserendo istruzioni truffaldine. Il 23% è dovuto a manipolazioni dell'*input, *mentre il 15% avviene attraverso il cosiddetto «accesso logico ai dati» cioè senza entrare in diretto contatto con l'elaboratore, ma comandandolo a distanza attraverso un terminale. Percentuali minori si riferiscono a furti compiuti con l'accesso al sistema operativo, ai programmi applicativi, alle procedure d'emergenza o alla trasmissione dei dati.*

Ma il ventaglio dei crimini informatici non si limita solo a quelli compiuti a scopo di lucro immediato: sempre secondo la ricerca di Stanford, sono in crescente aumento altri tipi di reati che provocano danni talvolta anche più gravi a un centro di elaborazione. Ad esempio il sabotaggio (aumentato del 25% negli ultimi 5 anni), il furto di tempo macchina (+ 15%) cioè l'uso di un sistema di elaborazione da parte di un dipendente a scopi privati; il furto di informazioni (+ 23%) o la distribuzione di informazioni (+ 19%).

Ma come si fa a penetrare nell'universo elettromagnetico di un computer? Di quali chiavi e di quali invisibili lasciapassare occorre essere in possesso per inserirsi illecitamente nella privacy *dei* bit *che rappresentano il suo prezioso tesoro? Uno dei punti dove i ladri informatici aprono più facilmente una breccia è quello delle parole d'ordine o* password, *definite da Biasiotti «il più grande inganno della sicurezza dei computer». Spesso sono di una banalità disarmante (un'indagine compiuta negli Stati Uniti ha messo in risalto che il 30% degli operatori dei centri di elaborazione dati avevano adottato la stessa parola d'ordine,* Mickey Mouse, *cioè Topolino) e quindi intuibili abbastanza facilmente.*

Altre volte invece la password *che ogni operatore dovrebbe custodire gelosamente con sé viene scritta sotto i portapenne o i posacenere se non addirittura sull'esterno del terminale. Altre volte ancora non viene cambiata rispetto a quella impostata dal fabbricante del computer, con il risultato che tutti gli utenti di uno stesso modello di elaboratore possono servirsi indisturbati del terminale degli altri.*

«Altro problema – aggiunge Biasiotti – è rappresentato dalle famose "code", memorie a disco su cui il sistema operativo riversa i dati da stampare in attesa che la stampante sia libera. In queste fasi di attesa è possibile accedere piuttosto facilmente al disco e quindi alterarvi i dati. Oppure si può provocare a bella posta un "fermo macchina" che azzera automaticamente la parola d'ordine di massimo livello; basta poi riavviare la macchina introducendo la parola d'ordine prescelta e neppure il responsabile della sicurezza potrà più modificarla. La stessa correzione di eventuali errori compiuti, l'intervento riparatore, o la correzione di dati sono spesso un rischio e quindi una manifesta occasione di frode».

Una volta riusciti a «entrare» in un computer, esistono mille modi diversi per rubare denaro senza che nessuno o quasi se ne accorga, o

almeno in un tempo ragionevolmente breve per consentire ad eventuali complici di sparire. Una delle tecniche più usate è quella del «salame» ed è in genere compiuta da chi ha la possibilità di accedere per lungo tempo ai terminali di un centro elettronico di una banca. Consiste nel modificare il programma di gestione dei conti correnti togliendo da ognuno di questi una cifra irrisoria, ad esempio 1000 lire. Cifra che però, moltiplicata per il numero dei conti correnti, può divenire estremamente sostanziosa. La si può poi accreditare su un conto aperto da un prestanome, con la certezza che i clienti della banca difficilmente protesteranno con il direttore per le 1000 lire in meno.

C'è infine il sistema della «bomba a tempo» che non procura un bottino immediato ma consente di ricattare una banca o un'industria anche per cifre astronomiche. È solitamente compiuta da programmatori molto esperti prossimi al licenziamento o alle dimissioni volontarie. Questi nascondono in uno dei programmi una particolare istruzione che dopo un certo periodo di tempo comincia a distruggere i dati essenziali contenuti in un centro elettronico. Una bomba che può essere disinnescata solo da chi l'ha inserita, ma con quali pretese...

Come fare quindi per prevenire il dilagare della criminalità informatica? Secondo Jeremy G. Grant, consulente della Wbk International, società di revisione di sistemi Edp, è indispensabile compiere una perizia preventiva su un sistema informatico, in particolar modo revisionando tutte le procedure di controllo. Si prosegue con difese fisiche o elettroniche (blindature e sistemi di allarme) per passare poi alle difese procedurali (parole d'ordine e ripartizione di responsabilità). «Ma molto spesso, a fronte di tecniche di elaborazione altamente sofisticate – ammonisce Biasiotti – si mantengono tecniche di sicurezza di tipo medioevale. Anche il sistema antintrusione più perfezionato di un centro Edp non serve a niente se, per pigrizia, gli impiegati lasciano la porta sempre aperta, o gli operatori lasciano i terminali accesi e in funzione quando scendono al bar a prendersi un caffè». In ùltima analisi – sottolineano i responsabili delle società assicuratrici – occorre una buona polizza. Quella della «Ross Collins Italia», la prima a coprire in Italia tutti i rischi di frode informatica, è stata istituita dai «Lloyd's» di Londra e, per una copertura di dieci miliardi di lire, richiede un premio annuo di circa 200 milioni. È stata sottoscritta già da un gruppo di sette banche italiane.

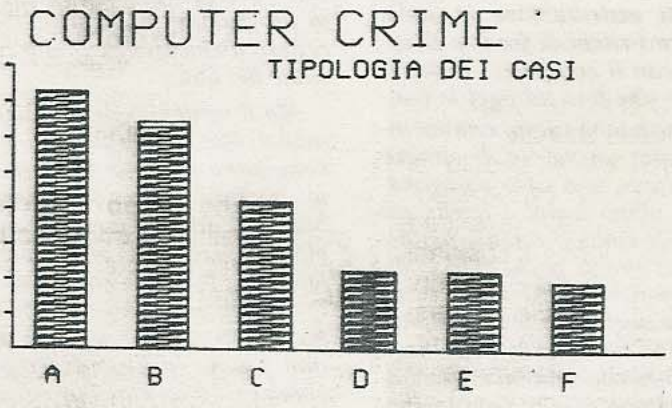
Giorgio Rivieccio

DATA POINTS...(PER CENTO)

A	35.5
B	21.5
C	21
D	11.5
E	9.5
F	1

A=PRINCIPI INFORMATICI GENERALI
B=SICUREZZA DELLA GESTIONE EDP
C=SICUREZZA DEGLI STUDI INFORMATICI
D=SICUREZZA DELL'H/W E DEL S/W DI BASE
E=SICUREZZA DELL'IMPRESA IN GENERALE
F=FATTORI SOCIOECONOMICI
FONTE: APSAIRD (FRANCIA)

Come la sicurezza di un centro Edp viene suddivisa nelle varie aree. Più alta è la percentuale e più l'area relativa è responsabile della sicurezza dell'insieme.



DATA POINTS....

A	26
B	23
C	15
D	8
E	8
F	7

A=ACCESSO FISICO AL COMPUTER
B=MANIPOLAZIONI DELL'INPUT
C=ACCESSO LOGICO AI DATI
D=MALVERSAZIONE PROFESSIONALE
E=MANIPOLAZIONE DELL'OUTPUT
F=ACCESSO AI PROGRAMMI APPLICATIVI