numero 15 - dicembre 1985 - lire 5.000

GENIUS

RAPINE ELETTRONICHE

MA LE BANCHE NON STANNO A GUARDARE

Si allarga a macchia d'olio la criminalità elettronica. Banche e imprese, quando scoprono il danno, spesso non lo denunciano nemmeno, per non allarmare i clienti. I loro specialisti, però, stanno escogitando misure di sicurezza sempre più sofisticate contro i truffatori. Chi vincerà?

DI LORENZO PINNA

Il caso "Bancomat", la truffa con il calcolatore dell'Inps, il trasferimento non autorizzato di mezzo miliardo di lire da una banca di Napoli in Germania: i "computer crimes", le rapine elettroniche, cominciano a fare paura anche in Italia. I Lloyd's, il famoso consorzio di compagnie inglesi, hanno già assicurato più di 20 banche italiane con la speciale polizza "Computer Crime Coverage". E proprio in questi giorni uno dei più importanti istituti di credito nazionale sta concludendo un contratto che prevede, in caso di danni provocati da "computer crime", un rimborso fino a 40 miliardi con un premio annuo di 800 milioni. Prima di stipulare la polizza assicurativa le banche o le imprese devono tuttavia dimostrare che i loro centri elettronici sono protetti in maniera adeguata.

Secondo il professor Robert Morris dei Laboratori Bell nel New Jersey, uno dei maggiori esperti nella sicurezza di sistemi computerizzati di telecomunicazioni, per proteggere un centro elettronico bisogna prima porsi queste due domande: qual è il valore delle informazioni immagazzinate? Chi ha interesse a rubarle? È necessario stabilire con precisione se l'avversario è un impiegato, un'azienda concorrente o un governo straniero. Una volta accertati l'identità e i mezzi a disposizione del potenziale nemico è sempre possibile trovare, secondo Morris, la contromisura adatta. Naturalmente bloccare un governo straniero costerà più caro che sventare le manovre dell'impiegato disonesto.

Ma queste contromisure spesso non vengono realizzate perché nessuno si rende conto del pericolo. In altre parole molte rapine elettroniche sono possibili grazie alla difficoltà culturale che impedisce a manager e dirigenti di valutare realisticamente i rischi della circolazione di dati e denaro in forma elettronica. "Se qualcuno ci regalasse un lingotto d'oro", dice Donn >

Ormai è la guerra tra le istituzioni e i criminali informatici: le compagnie di assicurazioni hanno creato speciali polizze a copertura del "computer crime", il furto commesso con il calcolatore.

B. Parker dello Stanford Research Institute di Palo Alto in California, "correremmo a depositarlo in una cassetta di sicurezza protetta da porte blindate, da guardie e da sistemi di allarme. Ma se lo stesso valore ci fosse trasmesso elettronicamente, con una serie di bit inviati attraverso i cavi o i satelliti, quanti di noi si chiederebbero quali difese proteggono il nostro gruzzolo di elettroni o di polarizzazioni magnetiche?".

Le reti computerizzate per la trasmissione di dati stanno diventando sempre più importanti, per svolgere qualsiasi attività. Una ricerca condotta dall'Università del Minnesota ha mostrato che oggi la maggior parte delle imprese americane medie e grandi potrebbe resistere, senza computer, meno di cinque giorni, poi andrebbe incontro al collasso. Più di 150 mila centri elettronici situati in Europa, Stati Uniti e Giappone si "parlano" in continuazione inviandosi informazioni o denaro. Questi centri sono collegati a più di 6 milioni di terminali.

I personal computer venduti in tutto il mondo sono quasi 2 milioni, e con questi apparecchi chiunque, da casa propria, può raggiungere le reti bancarie, universitarie, e alcune di quelle militari (negli Stati Uniti la Arfanet del Dipartimento della Difesa impiega linee telefoniche civili). Se poi si aggiungono i terminali tipo Bancomat e i "word processor" che possono collegarsi con le reti informatiche è facile intuire che i rischi di abuso sono veramente grandi.

"I pirati elettronici", sostiene Cipher Deavors, un ex agente della National Security Agency americana, oggi consulente informatico, "sono di molti tipi: dal ragazzino che passa le ore con il suo home computer a provare numeri telefonici e parole chiave di qualche sistema informatico, allo stimato programmatore che decide di aggiungere qualche istruzione in più al software che sta scrivendo per una banca, perché il calcolatore ignori gli astronomici scoperti del suo conto. I nemici sono esterni e interni, è quasi impossibile trovare le tracce dei loro colpi. Anzi, la maggiore differenza fra una normale rapina e un furto elettronico è che di quest'ultimo qualche volta non si riesce a capire se sia avvenuto o meno".

Le vittime della nuova pirateria elettronica sono i centri di elaborazione dati, dove si trovano i grandi calcolatori, le moderne casseforti che contengono una ricchezza solo apparentemente invisibile e intoccabile. "Per verificare lo stato di salute e la resistenza di un centro elaborazione dati è necessario un check-up completo", dice Massimo Penco della Ross Collins Italia, una società di assicurazioni rappresentata ai Lloyd's di Londra. "Questo check-up comincia di solito dai locali: la loro collocazione, le vie d'accesso, i sistemi di allarme. Teoricamente solo le persone autorizzate possono entrare nei centri, ma per un ospite indesiderato quanto è facile superare i controlli? Una porta chiusa della quale solo gli addetti possiedono la chiave o la combinazione, non viene considerata, per esempio, una difesa sufficiente.

"Uno degli stratagemmi più semplici per forzare questo tipo di ingressi", continua Penco, "si chiama 'piggybacking' (cavalluccio). L'intruso aspetta, tenendo in braccio un'enorme pila di tabulati o di dischi magnetici, l'arrivo della persona autorizzata. Non appena questa persona apre la porta, l'intruso si accoda e forse l'altro, gentilmente, si offrirà di aiutarlo a portare il peso. Tesserini magnetici, sorveglianti, porte a tamburo che fanno passare una persona alla volta, telecamere sono misure sufficienti a scoraggiare chi voglia entrare a 'cavalluccio' di addetti autorizzati".

Senza dover attendere ore e ore con i tabulati in mano, si può raggiungere un centro elettronico attraverso la normale linea telefonica. Soltanto alcuni computer militari dispongono di linee isolate da quella civile; banche, aziende, università usano, per trasmettere dati, la rete telefonica. Stando comodamente seduti in poltrona a casa >

PICCOLO

DATA DIDDLING (Scambio o alterazione di dati)

È il metodo più semplice per commettere un computer crime. Si tratta di alterare i dati prima di immetterli in un computer o dopo che ne sono usciti. Chiunque abbia a che fare con terminali, nastri magnetici, dischi, schede, può tentarlo. Un esempio: un'impiegata del settore contabile di un'impresa cominciò a battere sulla tastiera del computer il nome del dipendente che aveva fatto lo straordinario e accanto il proprio numero di matricola. Il computer accreditava lo straordinario solo in base al numero e così l'impiegata percepì straordinari per i quali non aveva lavorato.

Conoscenze necessarie: molto scarse o nulle. Accesso ai terminali.

TROJAN HORSE (Cavallo di Troia)

Consiste nell'introduzione, non autorizzata, di istruzioni nel programma di un computer, prima che questo venga usato. Quando il sistema entrerà in funzione, accanto alle operazioni di routine, ce ne saranno altre, illecite, che il testofante attiverà al momento opportuno. Un esempio: il programmatore di un centro elettronico inserì nelle istruzioni un "cavallo di Troia" che ordinava al computer di pagare certi assegni contrassegnati da una "E" e di cancellare le tracce della transazione.

Conoscenze necessarie: padronanza dei linguaggi e delle tecniche di programmazione. Accesso ai centri di elaborazione.

SALAMI TECHNIQUE (Tecnica del salame).

Si tratta di una forma automatica di computer crime. Impiegando un "cavallo di Troia" si può ordinare al computer di rubare cifre insignificanti da un gran numero di conti. Il successo di questa particolare truffa si basa sul fatto che nessun cliente della banca si insospettirà per un ammanco di poche lire. Nel corso del tempo le piccole cifre convogliate su un unico conto diventeranno una cifra notevole.

Conoscenze necessarie: padronanza dei linguaggi e delle tecniche di programmazione. Accesso ai centri.

LOGIC BOMB (Bomba logica)

Una bomba logica consiste in una serie di istruzioni abusive che entrano

DIZIONARIO DEL COMPUTER CRIME

in funzione a un segnale prestabilito. Una bomba logica può, per esempio, essere programmata per scattare fra due anni il 19 novembre alle ore 11.27, autorizzando un trasferimento fondi su una banca di Singapore, dove il testofante conta di trovarsi. Bombe logiche lecite vengono inserite da alcune imprese produttrici di calcolatori e di software quando questi sistemi vengono dati in prova a un cliente. Dopo un certo tempo o in seguito a certe operazioni (per esempio un tentativo di copiare il software) i sistemi di prova si bloccano.

Conoscenze necessarie: padronanza dei linguaggi e delle tecniche di programmazione. Accesso ai centri.

TRAP-DOOR (Trabocchetti)

Tutti i programmatori prevedono, durante la scrittura del software, degli accessi privilegiati ai loro programmi per consentire l'introduzione di istruzioni supplementari. Di solito queste temporanee impalcature per la costruzione del programma vengono eliminate con il collaudo finale. Ma alcune possono restare e da queste porte logiche secondarie si possono facilmente e illecitamente inserire nuove istruzioni.

Conoscenze necessarie: padronanza delle tecniche e dei linguaggi di programmazione. Accesso ai centri.

SUPERZAPPING

È una specie di programma "passepartout" usato nella manutenzione dei grandi centri computerizzati. Quando le normali procedure non riescono a far ripartire il calcolatore in "panne", un progamma Superzap, superando parole chiave e altri blocchi, permette di riparare il guasto. È uno strumento che deve rimanere sotto il controllo delle persone autorizzate alla manutenzione. Superzap è il nome di un celebre programma di manutenzione dell'Ibm.

Conoscenze necessarie: a livello di esperto dei sistemi. Accesso ai centri.

ASYNCHRONOUS ATTACK (Attacco asincrono)

L'attacco asincrono è una delle forme più raffinate e complicate di computer crime e richiede un'altissima competenza. Esso sfrutta il fatto che un grande computer non svolge dall'inizio alla fine un dato lavoro. Se per esempio in una certa fase dell'elaborazione manca lo spazio per immagazzinare i dati, il computer sospende quel lavoro e si occupa di un altro, finché non si libera qualche memoria per continuare il primo. Il regista di questa complessa attività è il sistema operativo che fa procedere i vari lavori a seconda dei circuiti disponibili. Le pause nei tempi di elaborazione possono essere sfruttate per leggere o alterare dati altrimenti inaccessibili.

Conoscenze necessarie: a livello di esperto dei sistemi. Accesso ai centri.

SCAVENGING (Sciacallaggio)

Si chiama così la tecnica per ottenere le informazioni rimaste in un computer dopo la fine di un lavoro. Un esempio banale è la ricerca di stampati non utilizzati o gettati nel cestino dei rifiuti. Esistono tuttavia metodi più sofisticati. I grandi computer hanno memorie temporanee (memorie buffer) per immagazzinare dati che servono in una certa fase dell'elaborazione. Uno "sciacallo" può leggere quei dati dopo che il legittimo utente ha terminato di lavorare. In molti centri elettronici i dati immagazzinati su nastri o dischi per un certo lavoro non vengono di solito cancellati, anche quando non servono più, perché questa operazione fa perdere tempo. L'abitudine è quella di inciderci sopra nuove informazioni. Anche in questo caso uno sciacallo può leggere le vecchie informazioni prima di incidere le nuove. Un caso di spionaggio industriale venne effettuato negli Stati Uniti proprio con questo metodo. Il cliente di un grande computer che veniva affittato a più utenti (time-sharing) si faceva caricare i nastri dai quali ricavava informazioni sulle ricerche di una compagnia petrolifera.

Conoscenze necessarie: da scarse a livello di programmatore. Accesso ai terminali.

DATA LEAKAGE (Fuga di dati)

È un computer crime che comporta la sottrazione di dati. Le sue forme possono essere semplici come il furto di nastri o stampati. Ma esistono versioni più raffinate. A Mosca il rumore delle telescriventi dell'ambasciata americana veniva registrato a distanza e decodificato. È recentissimo lo studio di un laboratorio olandese che dimostra la possibilità di ricevere, a vari chilometri di distanza, le radiazioni dello schermo di un teminale per leggere testi e informazioni.

Conoscenze necessarie: disponibilità di sofisticate apparecchiature elettroniche.

WIRETAPPING (Intercettazioni)

In modo simile alle intercettazioni telefoniche si possono intercettare le linee che trasmettono i dati. Una valida protezione sono i codici crittografici.

Conoscenze necessarie: disponibilità di sofisticate apparecchiature elettroniche.

PIGGYBACKING (Cavalluccio)

È un attacco che si può realizzare in vari modi. Un esempio classico è entrare illegalmente in un centro elettronico insieme al personale autorizzato portando pile di tabulati. Il "cavalluccio" elettronico si verifica quando un dipendente viene allontanato dal suo terminale con una scusa. L'infiltrato può allora lavorare sul terminale lasciato acceso con la stessa autorità della persona che lo aveva attivato. Anche le incursioni elettroniche degli hackers possono considerarsi una forma di "piggybacking", poiché sfruttano numeri e parole chiave veri, sebbene trovati casualmente.

Conoscenze necessarie: da scarse fino a livello di programmatore. Accesso ai terminali.

CODICE 999

Molti programmi vengono realizzati da una sola ditta di software e venduti a molti utenti. Ciò impone alla ditta fornitrice di offrire programmi flessibili per allargare al massimo il proprio mercato. Ma non tutti gli utenti sono interessati all'intera gamma di prestazioni; allora il fornitore ricorre al semplice espediente di togliere dal manuale di istruzione le pagine dei servizi non richiesti. Naturalmente tali servizi rimangono nel programma. Un esempio è il codice 999. In molti programmi questo è un codice generico cui addebitare spese non imputabili ad altri settori. Poiché un software di contabilità autorizza l'emissione di assegni solo se vengono addebitati a qualche "centro di spesa", il 999 permette di aggirare questo controllo di sicurezza.

Conoscenze necessarie: mediocri. Accesso ai terminali.

propria, con un personal collegato al telefono con un "modem" (un apparecchio che trasforma e invia, o riceve, i segnali di un calcolatore lungo i cavi telefonici) si può tentare di indovinare la parola chiave che apre le porte per curiosare nelle informazioni custodite negli archivi computerizzati.

Secondo Cipher Deavors della Nsa, "spesso le parole chiave di riconoscimento rappresentano un punto debole nelle reti informatiche, poiché sono concepite in modo da essere ricordate facilmente. Una parola facile da ricordare è anche facile da indovinare. In genere è una protezione insufficiente".

Aggiunge Massimo Penco: "Una delle parole chiave più comuni in Italia era, almeno fino a qualche tempo fa, Topolino, o la marca del calcolatore o il nome dell'impresa. Le parole chiave sicure sono quelle costituite da sequenze di lettere o di numeri casuali, abbastanza lunghe da rendere difficile azzeccarle per tentativi". Gli "hackers", i ragazzini terribili americani, per irrompere in un sistema computerizzato usano proprio il metodo delle prove a casaccio, facendosi aiutare da programmi che svolgono automaticamente la ricerca (uno di questi programmi, scritto in linguaggio Basic, è apparso anche su una rivista di computer italiana).

Per bloccare questa specie di roulette elettronica, oltre alle parole chiave complesse, il calcolatore può disporre di istruzioni che facciano cadere la linea dopo tre o cinque tentativi, oppure può registrare ogni prova e dopo un certo numero dare l'allarme. Esiste tuttavia un limite alla complessità delle misure di sicurezza per proteggere un computer dagli attacchi via cavo telefonico. Una parola chiave formata da mille caratteri (lettere, numeri, segni di interpunzione) è assai difficile da indovinare e ben pochi "hackers" riuscirebbero ad azzeccarla. In questo caso tuttavia gli utenti autorizzati sprecherebbero troppo tempo per farsi riconoscere. E anche i secondi perduti dal computer nei controlli di sicurezza

WALTER BATTISTESSA

possono diventare alla fine della giornata, dopo migliaia di transazioni, decine di minuti e forse ore.

Secondo Donn B. Parker, autore dello studio *Fighting Computer Crime* (Scribner's, New York 1983), i pericoli più gravi non provengono dall'esterno ma dal personale interno e dagli esperti di software consultati per risolvere qualche problema. L'impiegato disonesto che approfitta dell'occasione propizia per truffare l'azienda è sempre esistito, ma con i mezzi elettronici i danni possono moltiplicarsi centinaia di volte. A Napoli, alcuni mesi fa, il centralinista di una banca rimase di sasso quando la voce all'altro capo del filo gli comunicò che una bomba a orologeria era stata nascosta nei locali dell'agenzia. La polizia giunta sul posto fece sgombrare l'edificio, ma una meticolosa ricerca non rivelò la presenza di alcun ordigno. Poche ore dopo, quando un po' d'ordine tornò nell'attività della banca, l'addetto al trasferimento fondi con l'estero tramite il sistema elettronico "Swift", si accorse che dal suo terminale qualcuno aveva trasmesso un accredito di mezzo miliardo su una banca di Francoforte, importo che, ovviamente, era stato subito incassato. Nella fuga, dopo l'annuncio della bomba, l'addetto si era dimenticato di spegnere il terminale e un altro impiegato, lo stesso che aveva ideato la telefonata del terrorista, ne aveva approfittato. In questo caso l'impiegato disonesto non conosceva la parola chiave per mettere in funzione il sistema Swift e fu così costretto ad architettare il macchinoso piano della finta bomba a orologeria.

In altre situazioni, assai diffuse, quell'impiegato avrebbe dovuto faticare molto meno. Le parole chiave per attivare i computer di numerosi centri elettronici rimangono uguali per mesi e vengono abitualmente usate su tutti i terminali. Le regole di sicurezza per stipulare la polizza assicurativa dei Lloyd's prevedono che le parole chiave interne vengano cambiate una volta la settimana e che ogni terminale abbia la propria.

A volte i pericoli cominciano addirittura prima che un centro elettronico entri in funzione. Dove sono stati acquistati i programmi che guideranno l'attività dei computer? Chi è l'autore? Dentro un programma, nelle lunghe serie di istruzioni potrebbe già trovarsi un "cavallo di Troia", cioè una sequenza di pochi ordini abusivi che permetterà all'esperto di portare a termine il colpo non appena il centro elettronico comincerà a lavorare. Al posto del "cavallo di Troia" potrebbe trovarsi una "bomba logica", un altro tipo di programma che a un preciso segnale, una parola, un numero, una data, bloccherà tutto il sistema.

"Una delle più famose bombe logiche", racconta Donn B. Parker, "venne inserita da un programmatore nel computer dell'azienda per la quale lavorava: se il suo nome e il suo numero di matricola fossero finiti nell'elenco dei licenziati, il calcolatore sarebbe impazzito. Fra l'altro queste truffe sofisticate sfuggono ai normali controlli. È difficile rintracciare fra milioni di ordini il cavallo di Troia o la bomba logica. Solo un altro calcolatore, disponendo di una copia non contraffatta del programma sospettato, può eseguire il confronto automaticamente e scovare la serie parassita di istruzioni".

Un altro punto debole dei grandi centri informatici sono i nastri magnetici e i dischi che contengono programmi e dati. Chi li custodisce? Se chiunque può circolare nelle nastroteche, non si può escludere che un malintenzionato possa alterare un pro- >

Un terminale "al punto di vendita" abilitato a trasferire fondi dal conto corrente bancario del cliente a quello del supermercato. Particolari sistemi di difesa contro le truffe elettroniche sono in corso di allestimento in vista dell'introduzione in Italia di questo sistema di pagamento.