

I truffatori elettronici

C'è chi ha compilato minuziosi elenchi delle più note rapine informatiche indicando anche tutti i possibili mezzi di difesa - I Lloyd's di Londra la prima assicurazione del mondo che offre una polizza contro i furti al software

Una delle principali caratteristiche dei «computer crime» (le rapine e le truffe elettroniche) è la difficoltà di sapere qualcosa su come sono stati perpetrati e sui loro autori. Questo per due ragioni principali. Un primo motivo è tecnico: è molto complicato rintracciare fra le milioni di istruzioni immagazzinate nelle memorie, l'ordine illecito. La seconda ragione riguarda invece la pubblicità negativa che colpirebbe una banca se ammettesse di essere stata derubata con simili metodi. Un libro, di recente uscito negli USA, «Fighting Computer Crime» di Donn Parker (Scribner's editore), apre uno spiraglio su questo nuovo genere di reati che suscitano molto interesse nell'opinione pubblica dei quali si sa ben poco.

L'autore, Donn Parker, lavora allo Stanford Research International, un istituto di Menlo Park, vicino a San Francisco, e nel suo libro traccia un minuzioso elenco delle più note rapine informatiche arrivando ad una specie di classificazione delle fantasiose tecniche con le quali è possibile trasformare un computer in un truffatore automatico. La varietà dei metodi con cui si può tentare una rapina elettronica è veramente sorprendente. Si va da tecniche alla portata di tutti quale l'alterazione dei dati a metodi che richiedono una profonda conoscenza dei sistemi informatici come l'attacco asincrono.

La segretaria che ha il compito di introdurre dati attraverso il terminale può permettersi la semplice alterazione dei dati. Un caso raccontato da Donn Parker riguarda infatti un'impiegata che capì il modo in cui il calcolatore conteggiava gli straordinari, identificando il dipendente non dal nome ma dalla matricola. La disinvolta signorina cominciò allora a contabilizzare gli straordinari dei dipendenti scrivendo nome e cognome esatti ma aggiungeva la propria matricola al posto di quella vera. A fine mese con soddisfazione notò come la sua busta paga fosse notevolmente migliorata. I controlli superficiali sugli stampati non rivelavano niente di irregolare poiché gli uomini, al contrario dei calcolatori, preferiscono leggere nomi e cognomi (e questi erano esatti) invece numeri. Le proteste dei lavoratori defraudati fecero però scoprire la truffa.

Anche il metodo del «cavalluccio» è relativamente semplice. Un caso classico di questa tecnica si verifica quando un impiegato viene allontanato dal suo terminale

con una scusa e il lestofante (spesso un collega) ne approfitta per inviare ordini illeciti. A Napoli recentemente è accaduto proprio un fatto del genere. Una telefonata anonima ha annunciato la presenza di una bomba nei locali della banca. Nella fuga precipitosa, un impiegato non ha disattivato i terminali per i trasferimenti di fondi con l'estero tramite la rete Swift. Quando dopo qualche ora, la calma è tornata l'adetto alla Swift si è accorto che un ignoto aveva trasferito mezzo miliardo su una banca di Francoforte, importo che era stato subito ritirato. Donn Parker include nel «cavalluccio» anche le azioni dei ragazzini terribili americani, gli «hackers», che si inseriscono nelle reti e nelle banche dati sfruttando la fragilità e a volte l'ingenuità delle misure di sicurezza.

Altri colpi richiedono conoscenza che solo un esperto programmatore può possedere. E' il caso dei «cavalli di Troia». Con questo nome si intende l'introduzione non autorizzata di istruzioni supplementari nel programma di un computer prima che questo venga usato. Quando il sistema entrerà in funzione, accanto alle operazioni di routine, ve ne saranno altre, illecite, che il lestofante sfrutterà al momento opportuno. Un esempio: il programmatore del centro elettronico di una banca americana inserì nelle istruzioni un cavallo di Troia che ordinava al computer di pagare certi assegni con una "E" stampigliata e di cancellare le tracce della transazione. I cavalli di Troia possono essere impiegati per automatizzare la truffa. In questo caso il metodo viene anche definito «tecnica del salame».

Le istruzioni illecite ordinano al calcolatore di rubare cifre insignificanti da un gran numero di conti. Il successo di questa particolare truffa si basa sulla certezza che nessun cliente si insospettirà per l'ammontare di poche lire. Nel corso del tempo le piccole cifre convogliate su un unico conto ammonteranno ad una somma notevole. Anche per costruire un «bomba logica»

occorrono solide conoscenze informatiche. Una bomba logica consiste in una serie di istruzioni abusive che ad un certo segnale entrano in azione. Una bomba logica può, ad esempio, essere programmata per scattare fra due anni, il 19 novembre alle ore 11,27, automatizzando un trasferimento di miliardi su una banca di Singapore dove il fuorilegge ideatore del colpo conta di trovarsi.

Bisogna ammettere che gli «attacchi asincroni» non risultano per il momento mai tentati. E' questa una delle tecniche più complesse e richiede conoscenza da esperto dei sistemi. L'attacco asincrono sfrutta il fatto che i grandi computer non svolgono dall'inizio alla fine un dato lavoro. Se in una certa fase dell'elaborazione manca spazio per immagazzinare i dati, il computer sospende il lavoro e si occupa di altri compiti, finché non si libera qualche memoria per continuare il primo. In questo modo i grandi computer riescono ad utilizzare al massimo il tempo a disposizione. Le pause nei tempi di elaborazione possono essere sfruttate per leggere e alterare dati altrimenti inaccessibili.

Le tecniche del «computer crime» non si fermano qui. Esiste anche uno «sciaccalaggio» elettronico, cioè un metodo per procurarsi informazioni da un computer dopo che ha terminato un lavoro. Un esempio banale è la ricerca di stampati gettati nel cestino dei rifiuti. Proprio rovistando nell'immondizia uno studente di Los Angeles riuscì a scoprire i numeri di codice usati da una ditta di materiale elettronico per le consegne. L'imprudenza di gettare stampati nei rifiuti costò a quella ditta più di due miliardi di lire.

I grandi computer hanno memorie temporanee (memorie buffer) per immagazzinare dati che servono solo in una certa fase. Uno sciaccallo può leggere quei dati dopo che il legittimo utente ha finito di lavorare. Nonostante che la descrizione delle astuzie dei nuovi fuorilegge possa far pensare che la difesa è molto difficile se non impossibile, le contromisure per bloccare le varie truffe sono già state inventate. Il pericolo più grande non si trova dunque nella mancanza di difese ma nel fatto che non vengono applicate. Tutti sono convinti che per proteggere un lingotto d'oro siano necessari «caveau», porte blindate, guardie, sistemi di allarme. Ma se lo stesso valore fosse in forma di elettroni o polarizzazioni magnetiche quanti sentireb-

bero la necessità di usare misure analoghe?

Un modo per difendersi dal pericolo dei nuovi rapinatori elettronici è quello di assicurarsi. I Lloyd's di Londra, il famoso consorzio di assicuratori, ha presentato recentemente una nuova polizza, la «Computer Crime Coverage», che copre i rischi derivanti dalle nuove tecnologie informatiche. Oltre al «computer crime» vero e proprio la polizza assicura anche contro la distribuzione accidentale di dati e contro gli abusi compiuti con le carte di credito. In Italia questa polizza è offerta dalla società «Ross Collins Spa» e fino ad oggi almeno 20 banche si sono già assicurate.

Per poter sottoscrivere il contratto assicurativo, le banche devono tuttavia dimostrare che i loro centri elettronici adottano efficaci misure di sicurezza. Il «check-up» completo prevede il controllo dell'ubicazione, dei sistemi di allarme, delle vie di accesso, del personale impiegato. Ma l'analisi non si ferma qui. Lo stesso «software» cioè i programmi che fanno funzionare i grandi computer viene studiato attentamente. Dove è stato prodotto il software? Internamente all'impresa o alla banca oppure da una ditta esterna? E queste istruzioni contengono allarmi capaci di segnalare operazioni fuori della norma?

Una delle misure richieste dai Lloyd's è, per esempio, il giornale di bordo, uno stampato dove il computer riporta tutte le transazioni superiori a un importo prefissato. Ma il giornale di bordo non è sufficiente a garantire una sicurezza assoluta. Altre istruzioni, aggiunte al software, sono necessarie perché il computer possa individuare operazioni sospette. Questo «controllo di verosimiglianza» mette il computer in grado di conoscere le oscillazioni massime che possono avvenire ad esempio, sul conto corrente di un pensionato. Se quel conto viene scelto come punto di appoggio da un lestofante elettronico, il computer si accorgerà immediatamente che i miliardi che vanno e vengono sono molto strani. Una volta realizzate tutte queste misure di sicurezza quanto costa assicurarsi?

Proprio in questi giorni un'importante istituto di credito nazionale sta negoziando un contratto assicurativo «Computer Crime Coverage». Secondo alcune indiscrezioni la polizza coprirà danni fino a 40 miliardi ed il premio annuo per questa copertura sarà di 800 milioni.