Un riuscito convegno sul Computer Crime

I recenti avvenimenti criminali di cui la stampa ha dato notizia, come ad esempio la scoperta del secondo colpo della «banda del Bancomat», hanno portato alla ribalta il fenomeno del «computer crime», ovvero il crimine mediante elaboratore che ha destato viva apprensione negli operatori finanziari e nel pubblico.

Con l'espressione "computer crime" ci si riferisce ad un complesso di attività o azioni illegali che vanno dall'illecito trasferimento di fondi all'utilizzo in proprio di banche dati o tattamento delle informazioni. Negli Stati Uniti per esempio si calcola che nell'83 le banche abbiano perduto circa 200 miliardi di lire a causa di frodi attuate a mezzo del computer. In Italia il fenomeno appare ormai di dimensioni preoccupanti anche se negli ambienti bancari c'è la tendenza a minimizzare o occultare il problema, considerando anche che i rischi posti dalle nuove tecnologie informatiche sono poco conosciuti malgrado i recenti avvenimenti.

Mentre la nuova criminalità si mostra pronta a servirsi del calcolatore per portare a termine i propri colpi, gli esperti di sicurezza, sia fisica che elettronica, stanno studiando da tempo idonee metodologie di difesa. Ma la struttura degli elaboratori elettronici e delle reti di comunicazione esistenti rende difficile l'adozione di strategie di protezioni che non facciano ricorso, per coprire una parte residua del rischio, ad idonee polizze di assicurazione.

Proprio delle strategie di protezione contro la nuova criminalità tecnologica si è parlato nel seminario – tavola rotonda che si è tenuto a Roma, il 30 aprile, all'Adrovandi Palace.

È stato un incontro che ha suscitato una vasta eco ben al di fuori del campo degli addetti ai lavori.

I maggiori quotidiani, le agenzie di stampa e la televisione (RAI 1 ha dedicato un insolito spazio all'avvenimento) se ne sono occupati diffusamente. Impeccabilmente organizzato dalla rivista «Insurance New Letters» e dalla società assicuratrice Ross Collins (Italia), il convegno ha presentato ed illustrato le strategie di difesa fisiche, elettroniche ed assicurative che possono essere adottate per raggiungere un soddisfacente grado di protezione contro la criminalità tecnologica.

L'analisi per la protezione da questi attacchi si è articolata in :

– Esame delle aree di rischio;

– Valutazione del volume e della frequenza probabile delle perdite;

– L'adozione di opportune tecniche di difesa;

– La protezione assicurativa.

A questo proposito i LLOYD'S di Londra hanno messo a punto, alcuni anni fa, una polizza di assicurazione contro il crimine elettronico, denominata LECCP (Lloyd's Electronic Crime and Computer Policy).

Il seminario è stato aperto da una relazione dell'Ingegner Biasiotti, noto specialista in campo internazionale, coordinatore tecnico delle riviste specializzate "Antifurto" e "Bancamatica", Direttore didattico del Centro di formazione e specializzazione in sicurezza; giornalista pubblicista e docente presso l'Istituto per la conservazione dei beni culturali.

Nel suo intervento ha approfondito il problema delle aree di rischio di un sistema di elaborazione dati in una situazione in cui l'uso degli elaboratori apre alla malavita nuove possibilità di frode: infatti a difesa delle nuove tecniche contabili elettroniche si mantengono tecniche di sicurezza di tipo mediocvale. In particolare Biasiotti si è soffermato sui rischi legati all'uso del software o sistema operativo che consente all'hardware di funzionare assegnando ad ogni parte il suo compito e sincronizzando ed ottimizzando la gestione.

Il sistema operativo può funzionare a due livelli di attività: quello di utenza e quello di supervisione, quest'ultimo decisamente più affascinante e pericoloso in quanto consente di accedere ai più intimi segreti del sistema di elaborazione, scavalcando ad esempio qualsiasi parola d'ordine, leggendo ogni file, anche il più segreto, togliendo ed immettendo autorizzazioni, alternando, creando o distruggendo qualsiasi informazione o istruzione conservata nel sistema. Da ciò è chiaro come il controllo sull'uso e l'accessibilità al livello di supervisione di un sistema operativo sia vitale.

Importanti inoltre i sottoprogrammi che consentono specifiche funzioni ad altissimo livello (restricted utilities) che altro non sono se non un perfetto assegno in bianco: copertura illimitata, firma al massimo livello di autorità, rintracciabilità inesistente.

Biasiotti si è soffermato su tutti i punti esposti a rischio di un sistema di elaborazione.

L'unica risposta immediata, mentre si studiano nuove procedure di sicurezza e si verificano le esistenti, può essere data da un'idonea copertura assicurativa. Questo è stato l'argomento affrontato dal Dott. Vittorio Levis, responsabile del Ramo Rischi Banche delle Assicurazioni Generali.

Di fronte ai rischi ingenti connessi alle nuove tecnologie che si stanno imponendo in tutto il mondo, è naturale che l'industria assicurativa adegui le proprie risposte in base a criteri uniformi.

Si realizza così un livellamento tendenziale nei rischi che possono trovare copertura, negli standards tecnici che devono essere rispettati, nella dimensione dei premi.

Accanto a questi fattori di uniformità internazionale – afferma il Dr. Levis – esistono però naturalmente anche elementi specifici per ciascun paese, settore economico, singolo rischio: per questo anche in Italia devono venire adottati strumenti assicurativi che tengano conto della nostra realtà giuridica (importante soprattutto nella fase di liquidazione dei danni), nonché delle caratteristiche economico-organizzative di aziende complesse, che chiedono all'assicuratore un'assistenza globale per l'insieme dei rischi ipotizzabili.

Oliver C. Prior, Amministratore Delegato della Sedgwick Financial Institution Service, ha parlato dell'Assistenza ed il ruolo del broker di assicurazioni in relazione all'evoluzione dei rischi elettronici, affermando che ogni innovazione che non rientri propriamente in una delle classificazioni tipiche dei vari settori assicurativi crea grosse difficoltà a chi si occupa di assicurazioni e valutazione dei rischi.

"La posizione di un sottoscrittore dei Lloyd's nei confronti di rischi ad alta specializzazione tecnologica" e "La perizia preventiva: scopi ed implicazioni" sono gli argomenti degli ultimi due interventi rispettivamente di D. J. Newman, Membro Sottoscrittore dei Lloyd's di Londra, e Jeremy G. Grant, consulente di elaborazione dati della WBK International.

Oggi il numero di persone con conoscenze informatiche è aumentato considerevolmente. Esiste un largo contingente di persone esperte in questo settore, con conoscenze sufficienti per portare a termine un atto criminoso. Inoltre l'uso del computer è divenuto negli anni sempre più semplice. Purtroppo i sistemi di controllo in questo "Universo computerizzato" non hanno mantenuto lo stesso livello di evoluzione ed aggiornamento. Forse nei prossimi dieci anni l'automazione sarà messa sotto un reale controllo, tanto più efficace quanto più le associazioni di revisori saranno coscienti di questo problema.

CRIMINI INFORMATICI

Anche in Italia questo tipo di attività criminosa frutterà ottanta miliardi entro la fine del corrente anno. Il rimedio? Assicurarsi contro questo genere di furti. Ma i costi sono vertiginosi.

La situazione è stata analizzata nel corso di un convegno patrocinato da una società internazionale di assicurazione. Parliamo di un nuovo tipo di reati quelli che per essere commessi non hanno bisogno di una pistola o di una lancia termica né di uno scassinatore particolarmente esperto, ma, della complicità di un addetto ai lavori non necessariamente di alto livello e di una buona conoscenza dei meccanismi che sovraintendono al funzionamento di un mega o micro computer. Parliamo dei furti elettronici. Una nuova categoria di reati che in Italia ancora si contano in poche decine ma in paesi più avanzati del nostro come gli Stati Uniti o il Giappone hanno già superato le centinaia e, cosa da non sottovalutare, le svariate centinaia o migliaia di milioni.

I giuristi hanno già coniato un nome ad hoc e parlano di «crimini informatici» appunto perché possono essere commessi grazie alla conoscenza delle procedure informatiche cioè «smanettando», come usa dire oggi in Italia, un computer.

Togliere mille lire da ogni conto di una banca e depositarle sul proprio senza farsi vedere una sola volta dal cassiere della banca, disporre un accredito di miliardi a favore di un complice senza parlare mai con un funzionario di qualsiasi livello di un istituto di credito, ordinare a un'industria attraverso una banca prodotti di altissimo valore senza pagarli; ecco alcuni esempi di crimini informatici cioè di reati compiuti attraverso un elaboratore, crimini che nel mondo hanno provocato danni valutati in migliaia di miliardi.

In Italia il caso più famoso è quello del Bancomat, il sistema di prelevamento elettronico di valuta che garantisce ai correntisti di diversi istituti bancari consorziati fra loro di prelevare nei giorni e nelle ore di chiusura degli sportelli un certo quantitativo di biglietti di banca, prelievi che vengono addebitati elettronicamente sui singoli conti correnti attraverso una cassaforte alla quale si può accedere con una tessera magnetica e digitando un numero segreto conosciuto da ogni singolo correntista.

Tutti sanno per aver letto le cronache dei giornali delle ultime settimane come qualcuno sia riuscito a sostituire con tessere contraffatte e numeri segreti a fantasmici quanto legittimi correntisti e prelevare piccole cifre. Tutto qui? Direte. Il fatto è che questa operazione, ogni volta un prelievo massimo di duecento mila lire, è stata ripetuta illecitamente per un numero indefinito di volte e così, un prelievo dopo l'altro, le varie operazioni illecite hanno raggiunto cifre di tutto rispetto: varie centinaia di milioni di lire se non decine di miliardi.

Questo nuovo tipo di attività criminosa è tanto in ascesa che si prevede aumenteranno fino a un totale di ottanta miliardi per la sola Italia entro la fine del 1985. L'analisi delle stime riguardanti gli altri paesi coincide con il livello di progresso che la rivoluzione informatica ha toccato in ogni singola nazione: le statistiche riguardanti il solo anno in corso parlano di crimini informatici per 130 miliardi di lire in Francia e circa mille miliardi negli Stati Uniti d'America.

Quali sono le caratteristiche dei nuovi reati?

C'è anzitutto da fare una osservazione che non tranquillizzerà i vari istituti bancari o comunque i detentori di computer ai quali sono affidati compiti di trasferimento di valuta o di certificati di credito. Secondo una statistica dello FBI nei soli Stati Uniti il numero dei crimini informatici ha raggiunto rapidamente quello delle rapine, ma con un valore medio dieci volte maggiore. Come dire che, anche se questo nuovo tipo di criminali non usano più i tradizionali passamontagna, il classico piede di porco, la pistola o altre armi, hanno spesso risultati di gran lunga maggiori.

Il primo caso di crimine informatico, ormai entrato nei manuali, avvenne qualche anno fa in Inghilterra e, a rigor di logica o meglio di diritto, non potrebbe neanche definirsi reato.

Vediamo di riassumere le caratteristiche. Bisogna fare una premessa: secondo una vecchia legge del Regno Unito di Gran Bretagna, probabilmente perché la sterlina una volta valeva tanto, le banche non calcolavano nei rispettivi conti le cifre comprese dalla terza o quarta cifra dopo la virgola. Come dire che se un signore versava 300,0003 sterline nel proprio conto sullo stesso figuravano accreditate soltanto 300 sterline: 003 centesimi rimanenti finivano nelle casse della stessa banca a coprire una serie di rischi che la stessa sopportava durante tutto l'esercizio finanziario.

Ora un bel giorno, e parliamo di un crimine che non fu possibile catalogare come tale, accadde che un signore, modesto impiegato di quella banca ne conosciuto sopraffino del computer che era stato installato per accelerare ed economizzare tutto il lavoro di accredito ed addebito, aguzzò l'ingegno per incrementare il proprio misero stipendio. L'*operazione* fu molto semplice: Mister Smith aprì un regolarissimo conto corrente e poi dette l'ordine all'elaboratore automatizzato della banca di accreditare sullo stesso tutte le cifre comprese dopo la quarta a partire dalla virgola di tutti i versamenti effettuati nella banca stessa. Erano pochi decimi o centesimi di centesimo per volta, ma, siccome le transizioni ammontarono in un anno a parecchie decine di migliaia, nel suo conto vennero rapidamente ad assommarsi varie centinaia se non migliaia di sterline. Il macchineggio funzionò per qualche tempo. Poi accadde che qualcuno lo scoprì.

Cosa fare? La legge non vietava un'operazione del genere. Al dirigente dell'istituto di credito che metteva rono facilmente l'intestatario del conto corrente incriminato, non rimase che invitare lo stesso a dimettersi dall'istituto anche a costo di licenziarlo per il diritto ad esser liquidato. Quello di mister Smith fu il primo ma anche il più ingenuo dei «furti» informatici e venne scoperto con una certa facilità dato che il nostro fu scaltro ma non troppo nel mettere in pratica il suo progetto criminoso. Gli sarebbe bastato dare al computer della banca l'ordine di cancellare totalmente il conto, se la domanda di leggere i dati dello stesso fosse pervenuta da una persona diversa, per distruggere ogni notizia dei vari trasferimenti di valuta e quindi del suo reato pulito.

Dalla prima rovata del signor Smith le cose sono cambiate, le banche hanno aumentato i loro sistemi di prevenzione dei crimini informatici, ma ancora non sono riuscite che a contenere i rischi di tipo di crimine in vertiginosa ascesa.

Per ora comunque nessun marchingegno né sul hardware né sul software è riuscito a contenere il numero di queste illecite operazioni, anche perché pare che l'unico sistema realmente efficiente sia un «pacchetto» software inventato da un inglese ma ancora proibito per motivi di sicurezza militare. Un duro è certo: i crimini informatici sono molto di più di quanto si pensi e comunque di gran lunga superiori di quelli che vengono denunciati spontaneamente. La cosa è stata constatata negli Stati Uniti, dove da quando una legge impone la denuncia degli stessi, i reati sono quintuplicati da un giorno all'altro. Come dire che se tanto mi da tanto, la cifra che verrà realmente raggiunta in Italia in questo 1985 sarebbe di 400 e non 80 miliardi. Unico rimedio per ora resterebbe, dunque, l'assicurazione. Le tariffe? La Ross Collins fa pagare, per una copertura di dieci miliardi, duecento milioni di lire all'anno.

C.P.