COMPUTER CRIME – PAURA DI UN MISTERO

«Computer Crime»

Queste due parole inglesi sono diventate ormai familiari a molti dirigenti italiani, anche se non tutti conoscono bene la lingua inglese.

Taluni traducono, erroneamente, questa espressione con l'italiano «crimine con il calcolatore».

La traduzione non è corretta perché potrebbe lasciare l'impressione che il calcolatore abbia una qualche parte attiva nell'azione criminosa. Più felice è la traduzione «crimine mediante elaboratore». Esso infatti è mezzo per il perpetramento dell'atto criminoso, ma non è certamente soggetto attivo.

Con l'espressione «computer crime» ci si suole riferire a tutto un complesso di attività o azioni illegali, che vanno dall'illecito trasferimento di fondi all'utilizzo in proprio di banche dati o trattamento delle informazioni.

È assai difficile fare un completo panorama di tutti i modi in cui un computer può essere utilizzato in modo illegale, proprio per la versatilità, flessibilità e potenza operativa, che sono le caratteristiche salienti di un buon elaboratore. Cercheremo però, pur nello spazio ristretto di un'articolo, di analizzare alcuni esempi più clamorosi e, soprattutto, dare alcuni consigli sulle misure di difesa, già attuabili oggi.

In considerazione del fatto che gli Stati Uniti hanno la più elevata densità di elaboratori esistenti, e da maggior tempo, è quasi naturale che ci si rivolga alle esperienze americane per avere un quadro abbastanza aggiornato delle molteplici occasioni disponibili, per un criminale scaltro e competente o, purtroppo, anche sciocco, ma con gli occhi aperti.

Buoni secondi in questa poco edificante, ma altamente istruttiva, analisi sono gli inglesi, che, dal canto loro, hanno evidenziato alcuni «originali» aspetti delle attività criminali dipendenti dagli elaboratori.

Gli errori

Anche se gli errori non sono, a rigore, da classificare come atti criminosi, è molto importante tenerli in debita osservazione, perché non sempre è possibile definire, a-posteriori, se una perdita o un uso improprio è stato causato da errore accidentale o deliberata azione. La dimensione del rischio, legata agli errori, è documentata da casi plateali, fra i quali vale la pena di menzionare quello del Fondo Assistenza della Città di New York, che assegna sussidi ai bisognosi. La conversione da un sistema centralizzato di elaborazione dati ad uno distribuito provocò una omissione di dati, che causò l'emissione di migliaia di assegni non giustificati, con un danno complessivo pari a 8 milioni di dollari.

È bene ricordare che un elaboratore non sbaglia quasi mai, almeno secondo gli standards della ben più fallace natura umana. Quasi tutti gli errori sono da imputare ad una incorretta introduzione di dati o errate istruzioni per il trattamento dei dati. È quanto meno sorprendente che le stesse persone che si irriterebbero assai per l'errore di un impiegato allo sportello, accettino poi abbastanza serenamente la scusa che la causa della loro irritazione è da imputare, ad esempio, ad una fattura errata emessa dal computer. Personalmente, mi irriterei assai di più con il «softwarista» od il programmatore che ha fornito gli inputs errati al calcolatore, che proprio non c'entra nulla con l'errata fattura da esso emessa. È come accussare una macchina calcolatrice di aver sbagliato una somma, della quale abbiamo noi fornito gli addendi errati.

L'opportunità di un crimine

Troppo spesso succede che i sistemi di gestione e controllo dell'elaboratore siano talmente ingenui, da far venire tentazioni degne di un santo al più onesto dei dipendenti. Ricordo il caso di un totalizzatore per corse dei cavalli in Florida. Il sistema di scommesse della triplice accoppiata prevede la corretta giocata di tre accoppiate su tre corse non successive. Il montepremi è formato dal totale delle giocate, detratta una certa percentuale, e suddiviso tra i vincitori. È un tipo di scommessa ove si può vincere da 20 lire contro 1 a 1000 lire contro 1.

Il sistema, per sicurezza, utilizzava due elaboratori. Bastò ai criminali escludere un elaboratore dal circuito, appena noto il risultato finale, inserire un elenco fasullo di biglietti vincenti, e rimetterlo in servizio con il nuovo pacchetto di dati. Nessuno si poteva accorgere della manipolazione perché l'altro elaboratore continuava regolarmente a funzionare. Il giochetto, con il quale venne sottratto almeno 1 milione di dollari, fu scoperto quando un vincitore, questa volta vero, ebbe una vincita eccezionalmente elevata. Qualcuno si insospettì e la truffa fu scoperta per puro accidente.

Una delle maggiori truffe realizzate con l'ausilio dell'elaboratore è stata attuata dagli stessi gestori, che sfruttarono il fatto che ormai quasi tutti gli auditors utilizzano gli elaborati del computer per le loro analisi economiche. La Equity Funding Corporation of America (EFCA) creò dal nulla molte polizze di assicurazione sulla vita poliennali. Con questo credito presunto potè giostrare tranquillamente nel mercato finanziario, sino al giorno della resa dei conti, con una bancarotta del valore di 1 miliardo (avete letto bene!) di dollari. I venti massimi dirigenti dell'azienda avevano deliberatamente manomesso gli inputs dell'elaboratore, creando dati fasulli, che furono presi per buoni anche dai più smaliziati analisti di Wall Street.

Il caso Schneider è forse il più famoso e riguarda un brillante giovanotto che, avuta l'abilità di copiare i sistemi di ordinazione computerizzati della Pacific Telephone & Telegraph di Los Angeles, ordinò in più riprese un milione di dollari di materiale telefonico, che rivendette per suo conto.

Per cambiare un pò l'aria proviamo ad andare nella Corea, durante la guerra che vide il confronto diretto fra Cinesi ed Americani.

Il movimento dei materiali logistici veniva controllato tramite un sistema di elaboratori. Con la connivenza di personale americano e coreano, enormi quantità di materiali sono state fatte apparire come esistenti nella memoria dell'elaboratore, ma non nei magazzini, con un sistema di una efficacia ed ingenuità incredibile. Il danno è stato valutato a più di 100 milioni di dollari.

Poiché non è giusto svelare solo i misfatti al di qua della cortina di ferro, è bene forse ricordare che a Vilnius, in Lituania, alcuni dipendenti crearono degli impiegati fantasma nel computer aziendale, con il conseguente pagamento di stipendi fittizzi per un totale di 78.548 rubli.

Non credo davvero valga la pena di procedere in questa analisi.

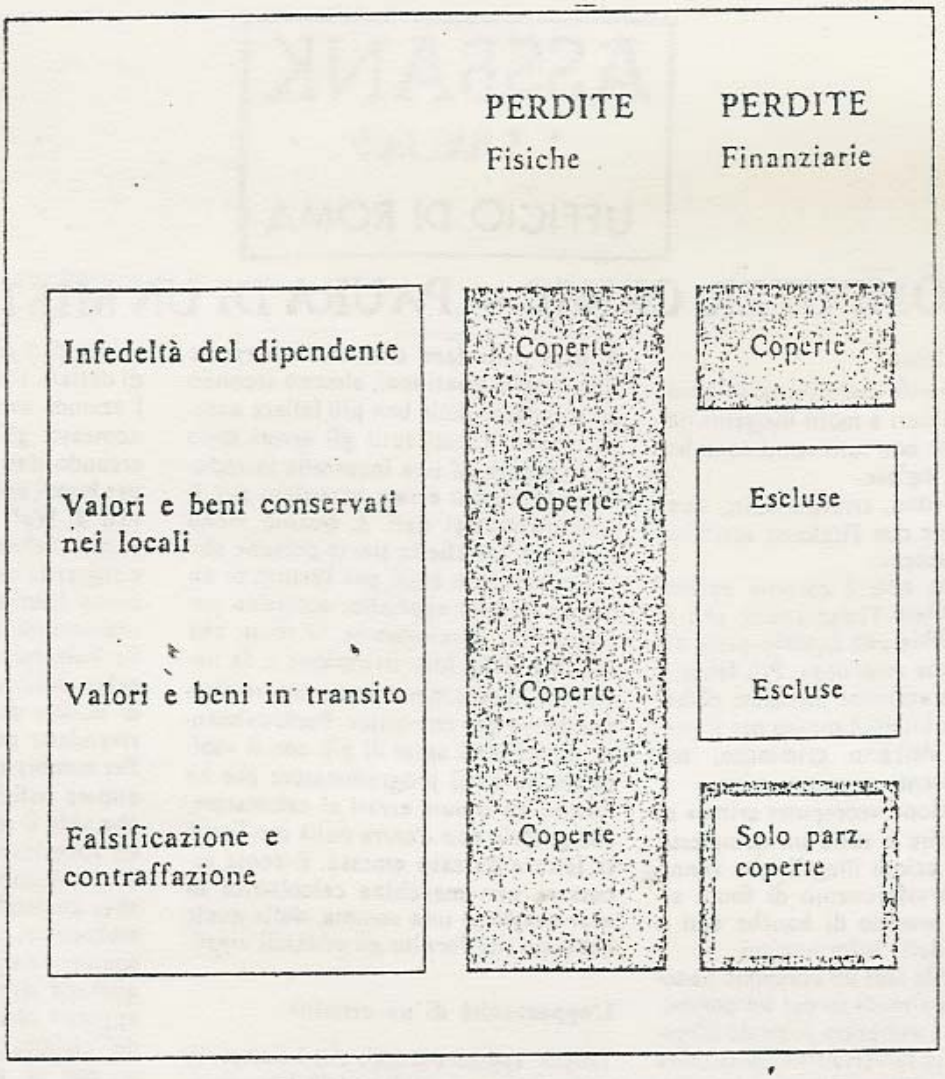
Errori e crimini sono legati, in quanto spesso i secondi colgono al volo l'occasione offerta dai primi.

Il controllo del rischio

È indubbio che gli attuali metodi di controllo siano del tutto insufficienti, non solo a livello di procedure di gestione, ma anche a livello di sistemi controllo.

Non dimentichiamo che una azienda che utilizza degli elaboratori offre ai propri dipendenti sia le armi di difesa che di offesa e pertanto l'opportunità di destinare l'elaboratore a fini impropri è estremamente attraente.

Il rischio di essere scoperti è decisamente basso, in quanto molte istituzioni, specie quelle finanziarie, preferiscono nascondere questo tipo di perdita, piuttosto che denunciarlo apertamente. Esistono ben tre casi in cui frodi a mezzo computer furono scoperte e divulgate da ispettori della Finanza, mentre i dirigenti degli istituti avevano preferito nascondere il tutto. In un caso ciò ha portato ad una denuncia penale, in quanto erano state alterate alcune evidenze contabili, proprio per celare



l'accaduto.
Anche le pene emesse dai tribunali, nei rari casi in cui si è andati in giudizio, sono la prova di una scarsa sensibilità al rischio potenziale offerto dagli elaboratori.
Abbiamo citato solo i casi di più elevato valore, ma, per un esperto, è assai più temibile il caso del programmatore che riuscì a trasferire sul conto della moglie 41 volte 100 dollari, prelevandoli da conti correnti a scarso movimento, con la neutralizzazione dell'emissione dell'addebito. Sono questi infatti i crimini che sono potenzialmente più pericolosi, perché ripetibili un elevato numero di volte.
Un altro interessante aspetto del crimine computerizzato è la mancanza di documenti reali che provino il crimine stesso, trattandosi, per la maggior parte dei casi, di transazioni di natura elettronica, ove ciò che rimane è un flusso di bits e non carte.
Il sistema SWIFT, utilizzato per il trasferimento di fondi (EFT) tra varie banche del mondo, ha dei punti deboli potenziali, noti agli addetti ai lavori, che riguardano sia l'introduzione dei dati, che la trasmissione e la ricezione. La stampa italiana ha recentemente dato grande risalto ad un tentativo di frode da 6 milioni di dollari presso una banca emiliana, attuato mediante alterazione dei dati del sistema SWIFT.
Ben più gravi sono i problemi di natura legale ed assicurativa legati all'EFT. Nel caso infatti un'istruzione di trasferimento attraversi più sistemi di elaborazione dati di banche diverse, può divenire difficile risalire alla banca nel cui sistema si è verificata l'alterazione. Dei complessi sistemi di cifratura a chiave, in possesso dei vari enti interessati, sono una soluzione, che però ha problemi gestionali non indifferenti.
Tralasciamo, perché anche troppo pubblicizzato, il caso della fiaba con il Bancomat realizzata nel nord Italia nel 1984. Le notizie date dalla stampa sono state spesso assai distorte ed alterate, ma la sostanza della truffa rimane. Non so chi rimborserà questa perdita, ma non lo invidio certamente.

La protezione assicurativa

In attesa di ben più accurate analisi e valutazione dei rischi e della prevenzione dei crimini con l'elaboratore, è costume di molti istituti, specie quelli finanziari, proteggersi con polizze assicurative.
È interessante rilevare la difficoltà della definizione di una corretta polizza protettiva, sia per l'indisponibilità di validi strumenti di valutazione del profilo del rischio, sia per l'estrema difficoltà di definire il valore massimo assicurabile, che in certi casi è decisamente ingente.
Proviamo ad analizzare insieme una delle più complete polizze esistenti per istituti finanziari: la famosa BBB dei Lloyds (Bankers Blanket Bond) rispetto alle categorie di rischio riguardanti il settore bancario.
Classificando le perdite in fisiche, dovute cioè a sottrazioni di denaro o documenti per furto o rapina, e finanziarie, dovute alla creazione o eliminazione di uno stato di indebbitamento, si può costruire la tabella qui di seguito riportata.
Appare ben chiaro come rimangano scoperte delle aree di estremo rischio. Si provi ad esempio ad analizzare il caso dei valori e beni conservati nei locali, se con un artificio si cancellano dalla memoria dell'elaboratore i dati relativi al credito vantato verso un terzo, la polizza non offre copertura. Parimenti non vi sarà copertura per la cancellazione di una transazione EFT attraverso il sistema computerizzato della banca.
A maggior ragione non varrà la copertura di polizza per accrediti emessi fraudolentemente, senza l'attiva partecipazione di dipendenti infedeli. Questo tipo di truffa è facilmente realizzabile usando i terminali remoti gestiti dall'utente (ATM - Automated Teller Machines). La clamorosa dimostrazione, fatta poco tempo fa a Los Angeles, della facilità di ricopiatura delle tessere magnetiche e la possibilità, molto meno remota di quanto si creda, di conoscere i codici personali (PIN - Personal Identification Number) degli utenti sono la prova della pericolosità, insita nella decentralizzazione di terminali attivi.
Non per nulla gli stessi Lloyd's hanno messo a punto una polizza CCC (Computer Crime Coverage) che riempie appunto le lacune della tabella precedente.
Il complesso problema dell'interconnessione tra profilo e prevenzione del rischio è attualmente oggetto di un'indagine, che dovrebbe consentire alle istituzioni finanziarie di avere un quadro più completo della effettiva validità della loro copertura e dei modi di migliorarla.
Resta sempre vero il fatto che solo da un'efficace prevenzione possono scaturire condizioni e premi accettabili per l'assicuratore e l'assicurato.
Per concludere una parola di attenzione a tutti i possessori di carte di prelievo tipo Bancomat e similari: leggete molto attentamente le clausole di rilascio delle tessere. Scoprirete qualche cosa che vi darà da pensare.

Adalberto Biasiotti