

Speciale
AgricolturaSpeciale
Fisco

Lloyd's

I mercati
azionari
e valutari
in Italia
e nel mondo

Roma - Via Parigi 11 tel. 47430 - Milano - P.zza Borromeo 1 tel. 87 76 47

QUOTIDIANO DEL MATTINO * FINANZA * ECONOMIA * ATTUALITÀ

Una copia L. 900 - Arretrati L. 1.200

Il «computer crime» tra mito e realtà: occorre comunque una strategia di difesa

Negli ultimi giorni di aprile, organizzato dalla Rivista settoriale «Insurance news Letters», grazie alla collaborazione della Ross Collins (Italia) Spa., si terrà a Roma un incontro tra specialisti di crimine elettronico e rappresentanti dei Lloyd's di Londra su un tema di scottante attualità: «Computer crime: una concreta strategia di difesa».

I recenti avvenimenti criminosi, cui è stato dato ampio risalto, hanno destato negli operatori finanziari e nel pubblico una viva apprensione che induce a ricercare nuovi e più adeguati tipi e modalità di protezione. Gli esperti di sicurezza, sia essa fisica che elettronica, hanno da tempo studiato idonee metodologie di difesa, ma la particolare struttura degli elaboratori elettronici e delle reti di comunicazione nazionali ed internazionali rende assai difficile la messa in atto di strategie di protezione globale che non facciano ricorso, per coprire una parte residua del rischio, ad idonee polizze di assicurazione. Si deve in effetti ammettere che le nuove tecnologie informatiche pongono all'attenzione nuovi rischi che in Italia sono ancora poco conosciuti. Negli Stati Uniti ed in alcuni paesi europei sono già disponibili dati statistici ed indagini economiche che mostrano l'effetto potenzialmente dirompente di nuovi tipi di attacchi criminali. Brevemente si può dire che l'analisi e la conseguente protezione da questi attacchi si articola in: esame delle aree di rischio; valutazione della magnitudo 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 per primi 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/tavola rotonda in questione si pone appunto di presentare, in un quadro organico ed unitario, le strategie di difesa fisica, elettronica ed assicurativa che un'istituzione fi-

nanziaria può attuare per raggiungere un grado di sufficiente protezione coontro la nuova criminalità tecnologica.

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 imputere ad una incorretta introduzione di dati o errate istruzioni per il trattamento dei dati. Una azienda che utilizza degli elaboratori offre ai propri dipendenti sia le armi di difesa che di offesa e pertanto la 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.

Un calcolatore, specie per le aziende «data dependent», costituisce un elemento insostituibile della attività, aziendale. Le statistiche confermano che il 33% delle aziende il cui elaboratore è stato distrutto, a causa di un incendio, sabotaggio od altro, non riprendono più l'attività.

In Italia, per fortuna, il Computer Crime è ancora infrequente e, se capita, viene nascosto sotto il tappeto persiano della sala di presidenza. Si verificano però molti altri eventi dannosi, dei quali non ci si protegge se non con un adeguato studio delle difese fisiche (es. blindature), elettroniche (es. sistemi antintrusione). Sarà bene però non fermarsi qui: la storia recente insegna che i criminali imparano presto a trovare i punti deboli, vedi rapine ai vagoni postali ed il computer sarà certamente, presto, un attraente bersaglio.