ASSICURAZIONI

RIVISTA DI DIRITTO, ECONOMIA E FINANZA DELLE ASSICURAZIONI PRIVATI

Computer crime: un nuovo tipo di rischio

L'utilizzo sempre più diffuso degli elaboratori elettronici nelle banche e negli istituti finanziari di tutto il mondo ha creato una nuova tipologia di rischio, connessa all'uso fraudolento di tali mezzi e le cui conseguenze in termini patrimoniali sono spesso ingentissime e di difficile previsione.

Per far fronte a tale rischio — insito potenzialmente in ogni elaboratore per la facilità con cui si può accedere alle informazioni, a patto, ovviamente, di avere una certa... fantasia criminosa — gli assicuratori hanno studiato particolari tipi di copertura che, uniti ad opportune misure di sicurezza, consentono alle aziende assicurate di tutelarsi contro gli eventuali danni derivanti da un uso troppo disinvolto degli elaboratori elettronici.

Alla luce di questa complessa problematica la Ross Collins (Italia) S.p.A. ha organizzato a Roma il 30 aprile 1985 un Convegno sul tema «*Computer crime*: una concreta strategia di difesa».

In apertura dei lavori, dopo il saluto del dott. M. F. Penco, Vice Presidente della Ross Collins, l'ing. A. Biasiotti, Coordinatore tecnico della stessa società, ha svolto la sua relazione su *Le aree di rischio di un sistema di elaborazione dati*, in cui ha analizzato il funzionamento di un sistema di elaborazione, mettendone in evidenza le aree più delicate.

Il sistema operativo o *software* — ha osservato il relatore — funziona a due livelli di attività: di utenza e di supervisione. Il primo corrisponde alla condizione normale in cui tutti gli utenti possono accedere, tramite terminali autorizzati, alle funzioni autorizzate. Il secondo livello (supervisione) è ben più interessante e pericoloso perché consente di accedere ai più intimi segreti del sistema di elaborazione, scavalcando qualsiasi parola d'ordine, leggendo ogni *file*, anche il più segreto, alterando, 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 di vitale importanza.

Infiniti — ha proseguito l'oratore — sono i punti «caldi» di esposizione al rischio: ad esempio i terminali e le reti, numerosi e distribuiti in ambienti con lacunosa possibilità di controllo; i *passwords* (parole d'ordine) che sono spesso banali, vengono cambiati assai di rado e sovente vengono trascritti su manualetti o addirittura sul terminale e, frequentemente, sono gli stessi imposti dalla casa costruttrice. Talvolta la stessa correzione degli errori, l'intervento riparatore o la correzione di programmi o dati rappresentano un rischio, e spesso una patente occasione di frode. Anche nella pratica, sana e raccomandabile, di fare duplicati degli archivi dati e programmi bisognerebbe usare

degli accorgimenti: ad esempio dividere in modo netto la responsabilità tra chi custodisce gli originali e chi custodisce le copie.

Concludendo, ha detto l'ing. Biasiotti, la varietà delle aree di rischio di un sistema di elaborazione è tale che ben difficilmente si potrebbero coprire tutte ed in breve tempo. Nel frattempo c'è una sola cosa da fare, mentre si attuano nuove procedure di sicurezza e si verificano quelle esistenti: affidare il completamento della protezione ad un'idonea copertura assicurativa.

È stata quindi la volta del dott. V. Levis, Responsabile del Ramo Rischi Banche delle «Generali», che ha trattato il tema *Assicurazioni, riassicurazioni e nuove tipologie di rischio.*

Partendo dalla premessa che le coperture assicurative costituiscono un supporto insostituibile allorquando l'attività economica è sottoposta al rischio di fatti che si possono verificare raramente, ma che sono in grado di provocare perdite molto rilevanti, il dott. Levis ha analizzato le nuove tipologie di rischio derivanti dalla cosiddetta «rivoluzione» informatica. In proposito ha rilevato che esiste una sostanziale omogeneità di base tra realtà lontane dal punto di vista fisico ed organizzativo; i rischi ai quali sono sottoposti gli utenti hanno una dimensione comparabile; esiste una spiccata internazionalità per quanto riguarda sia i fatti che possono verificarsi, sia le contromisure che, su diversi livelli, si può cercare di adottare. L'insieme dei fattori suddetti rappresenta il terreno ideale nel quale si può esercitare l'attività del riassicuratore.

La funzione del riassicuratore in presenza di rischi «di punta» ed altamente innovativi quali sono i rischi informatici è determinante, allorquando — agendo in modo efficace da stanza di compensazione fra rischi, Paesi, andamenti tecnici diversi — mette a disposizione degli assicuratori mondiali un prodotto che abbia requisiti di qualità ed affidabilità patrimoniale, derivi da esperienze ricavate da un'ampia casistica, rappresenti un livello tendenziale di quotazione, valido in campo mondiale.

Esaminando poi il ruolo dell'assicuratore, il dott. Levis ha affermato che questi, di fronte a nuovi tipi di rischio, deve porsi professionalmente vari obiettivi: garantire che siano soddisfatti gli *standards* tecnici minimali, che sono indispensabili per la stessa assicurabilità del rischio; far sì che le pattuizioni normative contratte con il proprio cliente siano compatibili con la disciplina giuridica locale; essere in grado di mediare tra le diverse e talvolta contraddittorie esigenze espresse dal mercato mondiale come livello tendenziale.

A conclusione del suo intervento, il relatore ha osservato che per far fronte efficacemente ai *computer crimes* occorrerebbe un tipo di contratto unico che elimini alla radice la possibilità di controversie, intento questo che sembra ormai perseguito dalla maggior parte degli assicuratori italiani, che hanno predisposto un nuovo strumento assicurativo, reso necessario dalle «nuove tipologie di rischio» nel campo dei *computer crimes*, con specifico riferimento al settore bancario e finanziario.

È seguita quindi la relazione di Mr. D. J. Newman, Sottoscrittore del Lloyd's di Londra, che ha riferito sulla sua specifica esperienza nel campo del *computer crime*, illustrando i risultati di un'analisi compiuta allo scopo di studiare ed introdurre sul mercato un nuovo tipo di polizza, la *Lloyd's Electronic and Computer Policy*, in grado di fornire la prima reale copertura contro le più moderne tecniche di frode elettronica.

È intervenuto poi Mr. Oliver C. Prior, Amministratore delegato della «Sedwick Financial Institution Services», che, parlando su *L'assistenza e il ruolo del broker di assicurazione nei rischi elettronici*, ha osservato che il settore assicurativo è per sua natura sensibile e reattivo alle esigenze e richieste della clientela. Le polizze più innovative sono la risposta a nuove leggi od a nuove aree di rischio proposte all'attenzione dell'assicuratore dal potenziale cliente. La comunicazione tra assicurati ed assicuratori, spesso attuata attraverso i mediatori di assicurazioni, è in questo senso di grande importanza.

Se l'industria assicurativa vuole soddisfare le esigenze della clientela nel campo dell'alta tecnologia deve necessariamente creare uno spazio in cui siano possibili proficui scambi di idee, evitando situazio-

ni ove tutto ciò che concerne nuove tecnologie ed innovazioni in generale venga guardato con diffidenza o trattato con linguaggio da iniziati, con la conseguenza che i rischi che ne possono derivare siano avvertiti con difficoltà ed in modo inadeguato.

L'ultimo relatore in programma, Mr. J. G. Grant, Consulente di elaborazione dati della «WKB International», ha trattato il tema *Perizia integrativa: scopi ed implicazioni.*

Partendo dal presupposto che per una corretta analisi del rischio occorre distinguere il crimine commesso «per mezzo del *computer*» da quello perpetrato «sfruttando l'uso del *computer*», ha rilevato che mentre l'uso dell'elaboratore è divenuto man mano sempre più semplice, i relativi sistemi di controllo non hanno mantenuto lo stesso livello di evoluzione e di aggiornamento.

La funzione del revisore, che nell'accezione più tradizionale del termine era quella di esaminare la contabilità societaria onde accertarne l'accuratezza di tenuta, recentemente si è andata dilatando, includendo la revisione delle procedure di controllo anche allo scopo di suggerire eventuali miglioramenti da apportare alle procedure stesse.

La tendenza attuale, pertanto, è quella di includere il controllo delle sofisticate procedure informatiche nelle funzioni di *routine* delle revisioni contabili, ed in proposito l'oratore ha pronosticato l'introduzione di una apposita prassi codificata per il controllo delle gestioni automatizzate.

È seguito, quindi, un dibattito — coordinato da un esperto di criminalità informatica, il dott. C. Sarzana, magistrato, Direttore dell'Ufficio Ricerche, Documentazione e Monitoraggio del Ministero di Grazia e giustizia — nel corso del quale sono intervenuti gli esperti di sicurezza dei maggiori istituti bancari italiani e di altri enti sia pubblici che privati, perché — come ha tenuto a precisare il dott. Penco — il problema della criminalità elettronica non riguarda solo le banche, ma interessa, con portata «catastrofale», anche tutti gli altri enti *computer dependent* (anagrafi, aziende elettriche, telefoniche, banche-dati, ecc.).

E. Bico