Anno XV

ASSISTAMPA

agenzia giornalistica d'informazione

Registrazione Tribunale di Roma N. 14261 del 9-12-1971 - Sped. in abbon. Postale gruppo 1° bis (70%) - Trisettimanale

Computer's crime: quando il rischio viene dal "futuro"

BIASIOTTI: "INTANTO E' IMPORTANTE ASSICURARSI"

roma, 9 mag.(Assistampa) - Di sicuro nessuna banca renderebbe noto con disinvoltura di aver subito una truffa attraverso il proprio sistema computerizzato: sarebbe come dire "le nostre casseforti sono aperte a chiunque abbia la capacità di raggiungerle". Forse é proprio questa la ragione per la quale, nel nostro Paese, non si parla molto di computer's crime, pur in presenza di una indiscutibile realtà di fatto.

Negli Stati Uniti, ad esempio, da quando é stata introdotta la obbligatorietà di denunciare le frodi con il computer subite (perché in sostanza si tratta di perdite che gravano sugli azionisti dell'istituto), le statistiche riferite a questo tipo di reato hanno registrato una impennata eccezionale. In questo senso, non é credibile che nel giro di poco tempo ci sia stata un'inflazione di Arsenio Lupin tecnologici, quanto piuttosto che ci si trovi di fronte ad un fenomeno fino ad oggi mimetizzato da un'evitabile "omertà".

Il seminario organizzato a Roma, nei giorni scorsi, dalla Ross Collins ha presentato un'ampia panoramica su quanto si sta facendo, soprattutto in Europa, per prevenire e limitare i danni dovuti al computer's crime. In occasione di questo convegno, Assistampa ha incontrato e intervistato Adalberto Biasiotti, coordinatore tecnico della Ross Collins, nonché consulente in problemi di sicurezza di molte banche nazionali.

Assistampa - Solo da poco tempo si é iniziato a parlare, anche a livello di opinione pubblica, del computer's crime: si tratta effettivamente di un fenomeno preoccupante e tale da richiedere un grosso impegno verso la sicurezza?

Biasiotti - In effetti ci troviamo in una situazione in cui l'uso degli elaboratori apre alla malavita nuove possibilità di frode, agevolate dalla particolare struttura di un sistema di elaborazione dati, ed ancora in una situazione in cui contro l'utilizzo di tecniche contabili elettroniche si mantengono tecniche di sicurezza di tipo "medioevale".

Assistampa - Più in dettaglio, quali sono le principali aree "delicate" di un sistema di elaborazione?

Biasiotti - Il "software" o "sistema operativo", che consente allo "hardware" di funzionare assegnando ad ogni parte il suo compito, é il primo e più importante passo da analizzare se si vuole ottenere una sicurezza intrinseca nel sistema di elaborazione. Il sistema operativo, di regola, può funzionare a due livelli di attività: il livello di utenza e quello di supervisione. Questo ultimo é quello ben più affascinante e pericoloso. Esso 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, alterando, creando o distruggendo qualsiasi informazione o istruzione conservata nel sistema stesso di elaborazione.

Assistampa - Quindi, sono molteplici i punti deboli di un sistema operante, ad esempio, in una banca.

Biasiotti - Sì, questo é vero anche se esistono numerosi sistemi di controllo dell'accesso ai dati: a base di parole d'ordine, di livelli di autorizzazione a livello di aree di accesso e così via. Tuttavia la maggioranza di questi sistemi controlla l'accesso più che il contenuto. Infiniti altri sono i punti di esposizione a rischio di un sistema elettronico di elaborazione: i termi

AUMENTO DELLA INCIDENZA DI COMPUTER CRIMES (1978-1983)

Sabotaggio	+25 %
Furto di tempo macchina	+15 %
Furto di informazioni	+23 %
Distruzione informazioni	+19 %
Trasmissione dati	+43 %

Il totale dei casi del Computer crimes noti é ritenuto pari al 10 per cento dei casi effettivi. L'85 per cento dei casi noti di frode sono perpetrati da professionisti dell'informatica.

nali e le reti, numerosi e distribuiti in molti ambienti con relativa lacunosa possibilità di controllo. I "passwords", o parole d'ordine il più grande inganno della sicurezza dei computer. Sono spesso banali, sono cambiate assai di rado, vengono spesso trascritte su manualetti o addirittura sul terminale, sovente non vengono cambiate rispetto a quelle impostate dal fabbricante.

Assistampa - In questo senso, anche la componente umana risulta quale punto "debole" dell'intero sistema di elaborazione.

Biasiotti - Effettivamente la stessa correzione di errori fatti da parte dell'impiegato, l'intervento riparatore o la correzione a livello di programmi o dati, sono spesso un rischio e spesso una patente occasione di frode. Anche nella pratica, sana e raccomandabile, di fare duplicati degli archivi dati e programmi bisognerà usare delle accortezze: dividendo, ad esempio, in maniera assoluta la responsabilità di chi custodisce l'originale e chi custodisce le copie.

Assistampa - Alla luce di quanto lei ha affermato, quali sono le prospettive per una efficace lotta al computer's crime e, contestualmente, é prevedibile un "aggiornamento" anche da parte dei truffatori?

Biasiotti - Io credo che anche il più raffinato lestofante preferisca una buona vecchia truffa all'americana, piuttosto che manipolare dati e programmi di un sistema di elaborazione. Ciò però é vero solo se l'interazione tra controlli formali e fisici crea le condizioni per un'efficace azione deterrente. Nel frattempo credo che la varietà delle aree di rischio di un sistema di elaborazione é tale che ben difficilmente potremo coprirle tutte ed in breve tempo. E nel frattempo che si fa? La risposta a mio avviso é una sola: mentre si attuano procedure di sicurezza e si verificano le esistenti, il completamento della protezione può solo, e subito, essere affidato ad un'idonea copertura assicurativa.