Questo articolo è apparso sul Corriere del Ticino di giovedì, 10 marzo 2005 nella sezione Primo piano

Gioie e dolori di Internet in ufficio

La sicurezza informatica è un aspetto sempre più importante nell'attività delle aziende. È essenziale non minimizzare i rischi - Sono fondamentali i comportamenti individuali

Silvano Marioni **www.marioni.org**

La sicurezza informatica in azienda è un argomento vasto e complesso che può essere esaminato in modo diverso a seconda che la si veda da una prospettiva tecnica, organizzativa o manageriale. Al di la dei punti di vista, l'obiettivo comune resta la protezione degli interessi di chi, per svolgere il proprio lavoro, dipende dalle informazioni in formato elettronico. Sicurezza informatica vuol dire infatti analisi di tutti i rischi che possono minacciare il corretto funzionamento delle attività aziendali e definizione delle contromisure per garantire la disponibilità, l'integrità e la riservatezza delle informazioni. Ma quella che in apparenza potrebbe sembrare un'attività di ordinaria amministrazione da delegare ai tecnici o agli specialisti, è in realtà un'attività più complessa che coinvolge l'intera organizzazione dell'azienda. Nella prima puntata di questa panoramica sulla sicurezza informatica ci eravamo occupati del problema dal punto di vista dell'utente privato, ricordando che una delle cose importanti è avere la consapevolezza dei rischi che corrono i nostri documenti, e noi con loro, quando colleghiamo a Internet il nostro computer. Non basta disporre di strumenti tecnici di protezione ma occorre anche adeguare i nostri comportamenti ai rischi che potenzialmente possiamo correre, anche sotto il profilo giudiziario (il nostro computer collegato in rete potrebbe ad esempio essere utilizzato a nostra insaputa da terzi per attività criminose). Ora, passando a parlare delle aziende e delle loro molteplici attività, le problematiche legate alla sicurezza appaiono ancora più complesse da affrontare.

Nuove tecnologie, nuovi rischi

L'evoluzione della tecnologia sta facendo emergere la sicurezza informatica come un aspetto sempre più importante nell'attività dell'azienda. Le nuove opportunità informatiche e di comunicazione che hanno portato all'eliminazione dei vincoli di spazio e di tempo, al decentramento della gestione e del controllo, ai processi automatizzati, stanno riducendo sempre più il ruolo decisionale delle persone, diminuendo la loro consapevolezza dei processi di lavoro e la visione diretta della realtà aziendale.

Per fare un esempio, nell'ufficio tradizionale il furto di informazioni era un'attività rischiosa perché comportava la sottrazione di documenti cartacei ingombranti e la possibilità di essere scoperti. Nell'ufficio elettronico il furto di informazioni può avvenire senza che nessuno se ne renda conto e il ladro può essere addirittura all'altro capo del mondo.

La mancanza di percezione dei pericoli porta spesso a minimizzare i rischi e a considerare i costi della sicurezza informatica come superflui ed eccessivi. Dal lato opposto un eccesso di fiducia nella tecnologia può indurci a pensare che la sicurezza informatica sia un risultato direttamente proporzionale alla quantità e alla sofisticazione delle apparecchiature di protezione di cui disponiamo. Il dilemma su quanto e come sia meglio investire per una corretta gestione della sicurezza informatica è un tema più che mai attuale.

Come investire in sicurezza informatica?

La rivista informatica ComputerWorld riporta un'interessante opinione su questo argomento. In un suo articolo intitolato «Come spendere un dollaro in sicurezza informatica» ha ipotizzato la seguente suddivisione:

- 10 centesimi: Valutazione dei rischi per capire quali beni devono essere protetti, quali sono la minacce e dove l'organizzazione è più vulnerabile
- 15 centesimi: Policy e documenti di alto livello sulle strategie di sicurezza per spiegare gli obiettivi della sicurezza informatica a tutto il personale.
- 15 centesimi : Processi aziendali mantenuti aggiornati nel tempo perché la sicurezza è un tema che va continuamente riesaminato.
- 20 centesimi: Utilizzo dei più aggiornati strumenti tecnici di sicurezza cercando di integrarli con quanto già presente in azienda.
- 40 centesimi: Formazione degli utenti sui comportamenti da tenere per contrastare i rischi informatici e degli specialisti informatici per sviluppare applicazioni e sistemi più sicuri.

L'articolo dimostra che la gestione del rischio informatico è da affrontare con un approccio multidisciplinare e, analogamente a quanto si fa nella gestione del rischio finanziario con la diversificazione degli investimenti, è importante

utilizzare differenti misure di protezione. Generalmente la difesa dei beni informatici è focalizzata soprattutto sugli strumenti tecnici che sono sicuramente indispensabili per la protezione dei nostri computer, ma che non possono essere i soli elementi di difesa per garantirci da tutti i possibili rischi informatici.

L'importanza del fattore umano
È fondamentale la componente umana perché sempre più spesso gli attacchi non vengono portati solo a livello tecnico ma sono combinati con la truffa e con l'inganno delle persone. Per questo oltre a rendere sicuri i sistemi, oggi è importante migliorare la consapevolezza dei dipendenti, informandoli sui rischi e insegnando loro i giusti comportamenti per identificare e combattere le eventuali minacce.
La sicurezza informatica deve essere fondamentalmente una responsabilità di tutto il personale, a partire dagli utenti che devono utilizzare quotidianamente le apparecchiature e le informazioni fino alla direzione che deve definire le indicazioni strategiche per garantire la continuità delle attività.
Solo così, utilizzando in modo integrato gli strumenti tecnici e i comportamenti individuali, si può tenere alto il livello di sicurezza intorno ai beni informatici aziendali e assicurare il buon funzionamento dell'azienda.

Chek-list per una protezione informatica di base

Il sito Internet della Fondazione Infosurance (*www.infosurance.ch*) contiene informazioni e istruzioni sul tema della sicurezza informatica per le aziende. Tra queste è disponibile una check-list che presenta i punti essenziali per minimizzare i danni alle informazioni aziendali vitali e per ridurre al minimo le perdite finanziarie:

Stabilire i compiti della direzione e assegnare le responsabilità.
Definire un responsabile informatico e stabilire il suo elenco dei compiti.

Backup - Salvare i dati regolarmente e archiviarli correttamente.
Conservare le copie di salvataggio fuori dall'azienda. Fare delle copie dei documenti importanti.

Installare un programma antivirus e aggiornarlo regolarmente.
Eventualmente installare un programma combinato di antivirus e personal firewall. Non dimenticare i computer portatili e i collaboratori esterni.

Installare un personal firewall e aggiornarlo regolarmente.
Eventualmente installare un programma combinato di antivirus e personal firewall. Non dimenticare i computer portatili e i collaboratori esterni e i computer collegati alla rete locale via radio (wireless).

Effettuare l'aggiornamento del software periodicamente.
Il programma informa automaticamente dei nuovi aggiornamenti («patches») oppure è necessario informarsi periodicamente sul sito del fornitore di software?

Portare i computer portatili dall'insicurezza a una maggiore sicurezza mobile.
Utilizzare i collegamenti di rete senza fili esclusivamente via VPN (Virtual Private Network, reti virtuali realizzate su Internet o Intranet e dotate di protezioni e sistemi di sicurezza), modificare la password del fabbricante e attivare il WEP (protocollo di cifratura su rete wireless).

Proteggere le password e le autenticazioni da possibili abusi.
Utilizzare password sicure e cambiarle regolarmente.

Le direttive sull'uso dell'informatica e le campagne sulla sicurezza permettono di ottenere maggior chiarezza presso i collaboratori.
Definire l'uso della posta elettronica, degli accessi a Internet, delle informazioni riservate. Prevedere ogni due anni una revisione delle procedure di sicurezza informatica.
Svolgere regolarmente attività di informazione sul tema della sicurezza informatica.

Un'informazione chiara sulla sicurezza è fonte di fiducia
Stabilire un elenco delle chiavi, proteggere i locali dei server, conservare i dati sensibili, i documenti del personale, i dati dei clienti e i contratti sotto chiave

Maggiore sicurezza grazie a una migliore organizzazione
Introdurre un sistema di classificazione che permetta una corretta archiviazione dei documenti non più utilizzati

Sicurezza e informazioni: un esempio svizzero

Intervista con Hanspeter Lingg, presidente della «Fondazione Infosurance»

Nel 1996 solo il 3% delle piccole e medie imprese svizzere disponeva di un collegamento Internet ma già si iniziava a parlare di strategie di sicurezza delle infrastrutture informatiche svizzere.
Nel 1997 si costituiva il gruppo *Sicurezza delle infrastrutture svizzere dell'informazione* che iniziava le prime analisi sulle minacce informatiche. Nel 1998 il Consiglio federale incaricava un gruppo di lavoro di elaborare un concetto di «Information Assurance» per garantire la disponibilità e la qualità delle informazioni e che conteneva tra le varie proposte anche la creazione di una fondazione per sensibilizzare l'economia e l'amministrazione sulla sicurezza informatica.
Per questo nel 1999 veniva creata la Fondazione Infosurance che recepiva molti dei temi presenti nel concetto di sicurezza delle informazioni in fase di elaborazione in quegli anni.
Per capire il ruolo che oggi ha la Fondazione Infosurance ne parliamo con il presidente Hanspeter Lingg

Che cosa è la Fondazione Infosurance, da chi è costituita e quali sono i suoi scopi?
«Infosurance è una fondazione per la collaborazione fra economia, ente pubblico e mondo scientifico nel settore della sicurezza delle informazioni in Svizzera.
Essa è stata fondata nel novembre del 1999 con i seguenti obiettivi:
sensibilizzazione, prevenzione, coordinazione e comunicazione sul tema della sicurezza informatica sia all'interno dei diversi settori economici così come tra i diversi settori economici, in particolare per le infrastrutture di base quali l'approvvigionamento energetico (in special modo nel settore elettrico) e le telecomunicazioni.
In seguito sono stati interessati anche i restanti settori economici: finanze e assicurazioni, trasporti, industria, sanità e servizi di soccorso.
In una prima fase la Fondazione è stata istituita e finanziata dall'economia, in particolar modo dal settore delle telecomunicazioni e dal settore finanziario. In seguito è intervenuta la Confederazione, sotto l'egida dall'*Organo strategia informatica della Confederazione* (OSIC)».

Perché considerate la sicurezza dell'information tecnology così importante e che cosa può fare una Fondazione che non possa essere fatto da una singola azienda?
«La dipendenza dell'economia nel suo insieme dalle tecnologie dell'informazione è in continua crescita nelle attività di integrazione e gestione dell'intero processo aziendale.
Ci sono due motivi che giustificano l'attività della Fondazione:
Una Fondazione finanziata da tutte le cerchie interessate e fondata su un rapporta di fiducia, può svolgere al meglio la sua funzione quale piattaforma neutrale e autonoma di partenariato tra gli enti pubblici e l'economia privata.
Non si tratta di sensibilizzare singole ditte sul tema della sicurezza informatica, ma l'intera piazza economica svizzera, specialmente le piccole e medie imprese che sono circa 295'000.
Per questo motivo questa piattaforma di interesse comune è la forma adatta per la prevenzione e per le attività congiunte».

Con quali organizzazioni, organismi commerciali o autorità pubbliche collaborate e su quali soggetti?
«Infosurance lavora con tutte le organizzazioni attive in questo settore, nell'ambito della Confederazione quali ad esempio l'*Organo strategia informatica della Confederazione (OSIC)*, il *Centro di analisi e segnalazione per l'Information Assurance (MELANI)*, la *Task Force speciale sull'Information Assurance (SONIA)* o altre organizzazioni pubbliche o di diritto privato in Svizzera e all'estero».

Che attività svolgete per promuovere la sicurezza dell'information technology in Svizzera?
«Fino al 2004 sono stata effettuate analisi dei rischi soprattutto nei settori delle telecomunicazioni, dell'energia e nella finanza, tradotte in seguito in piani operativi di business-continuity, che saranno realizzati nel 2005.
Negli altri settori le analisi dei rischi sono state appena avviate. Questo compito in futuro sarà svolto dall'*Ufficio federale per l'approvvigionamento economico del paese*.
Infosurance sarà punto di riferimento soprattutto per le piccole e medie aziende, perché è qui dove il fabbisogno è più grande.
Saranno coinvolte in queste attività varie associazioni, istituti di formazione (scuole professionali e università) ecc.»

Per saperne di più:
www.isb.admin.ch
www.infosociety.ch