

IL SISTEMA DI GESTIONE DELLA SICUREZZA

I gravi episodi dell'11 settembre, i sommovimenti politici, i collassi finanziari, la stagnazione dell'economia, le preoccupazioni per nuovi attacchi terroristici e per eventuali falle nei sistemi di sicurezza, hanno innalzato nel Top Management la consapevolezza dell'importanza della sicurezza delle informazioni e del rischio IT.

Questo ha significato, per molte aziende, una revisione e un rafforzamento delle misure di sicurezza sia di tipo fisico (anti-intrusione, anti-terrorismo), sia informatico (intrusioni, attacchi con virus).

Una maggiore attenzione verso la sicurezza informatica si percepisce anche in banca e, anche se non è provato che i cambiamenti sopra citati abbiamo avuto un diretto impatto sui sistemi di sicurezza informatica nel nostro paese, è sicuramente vero che hanno portato in primo piano nelle aziende questo tema che richiede oggi nuovi approcci e nuove modalità di soluzione.

Infatti, le continue innovazioni tecnologiche e le conseguenti nuove opportunità di business hanno portato a cambiamenti sostanziali nelle banche, con la diffusione di servizi telematici che rendono disponibili on line, e direttamente alla clientela, tutta l'operatività tipica dello sportello bancario.

Questo ha avuto impatti per quanto riguarda la natura e il profilo dei rischi che la banca deve affrontare: si passa, infatti, da una situazione in cui la sicurezza si doveva preoccupare soprattutto degli aspetti interni all'azienda ad una in cui è necessario proteggersi dall'esterno perché i clienti oggi possono interagire direttamente con i sistemi aziendali, senza essere "intermediati" dagli operatori della banca, e utilizzare tecnologie "aperte" come internet che sono nate per consentire la massima libertà e diffusione delle informazioni.

Ulteriori elementi di novità per la sicurezza informatica, riguardano i cambiamenti che sono avvenuti negli ultimi anni per quanto riguarda l'ordinamento giuridico; infatti, il legislatore italiano ha ormai preso atto delle nuove esigenze della moderna società informatica e ha più volte deliberato in materia:

- DL 518 (tutela giuridica dei programmi per elaboratori),
- Legge 547 (modifiche al codice di procedura penale in tema di criminalità informatica),
- Legge 675/96 (privacy),
- DPR 318/99 (misure minime di sicurezza).

Questi impongono alle aziende misure tecnico/organizzative coerenti con quanto richiesto dalla normativa che prevede, in alcuni casi, anche responsabilità penali per gli amministratori.

E' quindi evidente che la questione della sicurezza in azienda non è più solo un problema tecnologico ma anche organizzativo e culturale ed è opportuno che sia assunto dal management in prima persona.

Questo significa coinvolgere le direzioni nel disegno complessivo della gestione della Sicurezza d'Impresa perché, come abbiamo visto, è oggi molto più ampio che in passato e abbraccia non solo le discipline tecniche sia della sicurezza tradizionale IT sia dei nuovi canali telematici ma comprende anche aspetti organizzativi, legali, di gestione del personale, e di gestione del rischio.

Per raggiungere l'obiettivo la Sicurezza Logica del SanPaolo IMI ha adottato lo standard BS7799 come "framework" di riferimento per impostare e realizzare un Integrated Security Management

System (ISMS) coerente con le necessità di business, con i requisiti legali e organizzativi e tale da garantire un livello di protezione adeguato alle scelte strategiche dell'azienda.

Lo standard BS7799 si articola in 127 “regole” da seguire per costruire l'ISMS, ripartite in 10 sezioni: politiche di sicurezza, sicurezza organizzativa, classificazione e controllo dei beni, sicurezza del personale, sicurezza fisica ed ambientale, gestione delle operazioni e delle comunicazioni, controllo degli accessi, sviluppo e manutenzione dei sistemi, gestione della continuità operativa, conformità ai requisiti legali, tecnici e alle policy.

Una volta completata la realizzazione, è stato avviato un piano di verifiche, sulle diverse componenti del sistema di sicurezza, da parte di professionisti esterni ed indipendenti dall'Istituto, per garantire la sua adeguatezza e rispondenza agli standard; è stato quindi richiesta e ottenuta una certificazione.

Sulla base del “framework” è stata impostata una struttura organizzativa in grado di coprire le diverse fasi del “ciclo” della sicurezza: analisi dei rischi, identificazione delle vulnerabilità e delle criticità, individuazione delle contromisure, progettazione ed implementazione delle soluzioni, emanazione di policy, esecuzione di controlli, erogazione dei servizi di gestione e monitoraggio.

Per coinvolgere la direzione è stato poi attivato: il Comitato per la Sicurezza Informatica di Gruppo che si pone quale struttura e luogo deputato al monitoraggio degli aspetti di sicurezza dei Sistemi Informativi del Gruppo, al raccordo sul piano interaziendale e interfunzionale delle analisi, delle rappresentazioni architetture e delle valutazioni che hanno per tema impatti rilevanti sulla sicurezza informatica.

A livello tecnico il Sistema di Sicurezza si compone di moduli presenti nei diversi ambiti della Information Technology aziendale: sistemi legacy, sistemi dipartimentali, telecomunicazioni, nuovi canali e copre le esigenze di sicurezza sia all'interno sia all'esterno della banca. Sono presenti in particolare:

- Servizi e sistemi per l'identificazione ed autenticazione degli utenti mediante un sistema di controllo degli accessi che garantisce il Single Sign-on.
- Sistemi di controllo perimetrale
- Sistemi per la gestione centralizzata degli antivirus
- Sistemi PKI (firma digitale e cifratura)
- Sistemi per il monitor ed il controllo degli attacchi
- Soluzioni per la business continuity

Tutto ciò premesso, riteniamo comunque che il fattore umano sia il più importante e quello vincente

per predisporre “difese” adeguate nei confronti delle organizzazioni criminali, la cui “creatività” sta aumentando e diventa ogni giorno più aggressiva; abbiamo quindi posto al centro del Sistema Sicurezza le risorse umane e i loro comportamenti.

A tal proposito sono stati attivati opportuni interventi per Informare e per Formare i dipendenti della banca, predisponendo e diffondendo le policy di sicurezza che indirizzano i comportamenti dei colleghi nei vari ambiti lavorativi, e preparando, con la collaborazione della Formazione, un corso specifico sulla Sicurezza.

Sulla base delle regole comportamentali così definite, abbiamo poi avviato le attività del Nucleo Controlli di Sicurezza che ha il compito di:

- Impostare ed effettuare controlli atti a garantire una corretta applicazione delle Normative Aziendali
- Verificare la resistenza dei vari dispositivi adottati nel caso d’attacchi mirati a sfruttarne le vulnerabilità.