MEDIA PLANET | SICUREZZA AZIENDALE

LUGLIO 2007

UNA GUIDA PER UNA CORRETTA GESTIONE DEL RISCHIO AZIENDALE ED INFORMATICO

UNA PUBBLICAZIONE MEDIAPLANET

MEDIA PLANET

Risk Management: benefici di una strategia

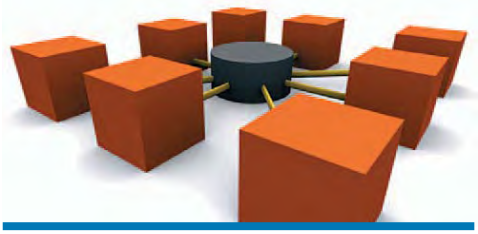
Una valida premessa è che non esiste la sicurezza informatica totale. Infatti sono tanti e tali i fattori in gioco, a partire dagli errori umani fino alle catastrofi naturali, che è impossibile controllarli e gestirli tutti. Il migliore approccio è quello che vede la ricerca di una soluzione ottimale, perseguendo il principio di un sufficiente livello di protezione, attraverso sistemi e misure progettate per affrontare situazioni ritenute critiche, o per limitare falle di sicurezza pericolose. La posizione che solitamente si osserva da parte di chi deve amministrare i beni aziendali è quella di operare per tutele differenziate, senza ragionare trasversalmente per ambiti operativi. Quindi ad esempio potranno essere assicurate le attrezzature informatiche, ma non sarà posta nessuna cura alle procedure generali che vedono protagoniste queste attrezzature, né si sarà posta attenzione ad una soluzione tampone in grado di arginare il problema sorto. E' pur vero che è sempre necessario considerare il budget a disposizione per l'intervento, cercando di non disperdere in mille percorsi quanto disponibile, ma operando al fine di massimizzare i benefici.
Il consiglio degli esperti è di dare corso ad una approfondita e seria analisi funzionale dell'organizzazione, quasi una fotografia della realtà aziendale, che comprenda caratteristiche strutturali, processi e flussi operativi, comportamenti e relazioni umane, obiettivi e priorità, benefici e costi. E' ciò che in altri settori viene definito come due diligence: il suggerimento è di prenderne a prestito tutte le specifiche funzioni e cognizioni per realizzare un documento di report ricco di contenuti informativi e di soluzioni adattative.
Il concetto di sicurezza informatica quindi è una filosofia generale di comportamento che non vuole correggere il problema eventualmente verificatosi, ma porre come cardine la prevenzione del rischio ed un atteggiamento interessato al problema da parte degli amministratori di una azienda, non solo dei responsabili del comparto IT. Riprendendo il discorso, quindi, un primo approccio al problema potrebbe essere rappresentato dall'analisi dei rischi, ovvero una valutazione obiettiva di tutte le possibili falle della sicurezza nel sistema informatico e ancora di più nella organizzazione del lavoro e dei collegamenti tra gli organi interni ed esterni dell'azienda.
Si possono valutare tutti gli asset hardware e software installati presso tutte le sedi e le filiali, tutti gli apparati di rete, e tutti i device interconnessi. Poi è possibile valutare lo stato generale dell'organizzazione che presiede all'utilizzo di tali dispositivi, ricomprendendo dirigenti, impiegati, lavoratori generici, agenti, addetti alla sicurezza informatica ecc.
Tutte queste valutazioni hanno lo scopo di comprendere il sistema nella sua interezza non limitandosi all'infrastruttura informatica che ne rappresenta solo lo strumento operativo. La normativa negli ultimi anni ha esplicitamente richiesto una migliore e più efficiente gestione dei procedimenti relativi all'informazione all'interno delle aziende. Non a caso la Risk Analisys è prevista come primo approccio per redigere il Documento Programmatico per la Sicurezza (DPS) come previsto dall'art. 6 del D.P.R. 318/99.
La definizione successiva di una politica per la sicurezza trae origine proprio dallo studio mirato a comprendere come proteggere al meglio i dati propri e di terzi soggetti, a maggior ragione quelli sensibili.
Sovente infatti accade "che una azienda si trovi per esigenze di business a collezionare una notevole quantità di informazioni che devono rimanere riservate. La diffusione di tali dati genererebbe una pesante ripercussione legale con conseguenze impredicibili e una perdita immediata d'immagine verso i clienti e i partner. In una fase successiva alla Risk Analisys possono essere progettate e implementate soluzioni tecnologiche che siano conformi a queste prime valutazioni. ◆

Effettività dei modelli organizzativi ai sensi del D.Lgs. 231/01

AVV. GIANCARLO BESIA
Partner Responsabile Area Compliance PIT Consulting

GIAMPIERO LAMPASONA
Amministratore Delegato PIT Consulting

I modelli organizzativi introdotti dal D.Lgs.231/01 predicano, tra l'altro, condotte etiche e lecite per i destinatari. L'efficacia dei modelli e la loro capacità esimente dipendono dall'effettività degli stessi, ovvero dal livello di conoscenza delle condotte attese da parte dei destinatari e dal livello di conformità delle prassi operative rispetto alle stesse condotte attese. Compito dei vertici (esecutivi e di controllo) è quello di vigilare sul livello di effettività del modello. Tale attività può essere svolta grazie a strumenti che permettono di valutare il livello di effettività e suggerire azioni correttive o migliorative, fornendo altresì informazioni a supporto dei soggetti responsabili per l'adeguatezza organizzativa. ◆



GFI Security Lab: un centro europeo Technology Independent per la Security Governance

Etica, competenze consolidate e un'organizzazione "team work based" per affiancare le aziende nella creazione del valore

La consulenza di professionisti che operano nel settore da diversi anni unita a un'esperienza tecnica unica, acquisita grazie al gran numero di progetti realizzati, consente a GFI Italia di perseguire un approccio integrato alla sicurezza, che tiene nella giusta considerazione gli aspetti tecnici, ma anche quelli strategici, organizzativi, economici e legali.

Con i suoi 450 dipendenti, GFI Italia, presenza nazionale del Gruppo GFI Informatique – oltre 8000 dipendenti a livello mondiale - opera in materia di sicurezza delle informazioni e delle reti a livello nazionale ed europeo attraverso il suo Security Competence Center, una struttura nata per progettare, realizzare e gestire servizi e architetture ICT e di Security Governance per i settori Telco, Utility, Finance, Pubblica Amministrazione, Industria e Servizi.
"Da sempre aiutiamo le aziende a crescere creando per loro strutture IT affidabili e sicure" ha affermato Eugenio Pontremolesi, General Manager di GFI Italia, "e con loro è cresciuta anche la nostra esperienza che ci permette di individuare ogni volta i margini di miglioramento su cui operare combinando le esigenze di sviluppo e di competitività dettate dal mercato con l'offerta tecnologica sempre più dinamica e in continua evoluzione".
Attraverso il Security Competence Center, struttura che vanta oltre 40 professionisti qualificati e certificati (Lead Auditor ISO 27001, CISA, ISO 9001, CISM, ITIL, ecc.) esperti in servizi e soluzioni di sicurezza logica, fisica e organizzativa, GFI Italia è in grado di collaborare con le aziende in un campo caratterizzato da una continua evoluzione e da un'esigenza di aggiornamento costante, rimanendo sempre vicina ai propri Clienti, presidiando il territorio nazionale, ascoltando e indirizzando i loro bisogni, e offrendo loro un servizio di consulenza in grado di identificare la "migliore" soluzione possibile.

In un contesto in cui competitività, qualità ed efficienza sono i requisiti minimi per la sopravvivenza di qualsiasi organizzazione, le aziende si dimostrano sempre più attente al tema delle certificazioni, entrate a far parte anche delle decisioni strategiche.Le certificazioni sono il risultato finale di un percorso che, attraverso l'ottimizzazione di tutti i processi aziendali, permette alle aziende di concentrare l'attenzione sulla capacità di comprendere e soddisfare le esigenze del Cliente, garantendo un'elevata affidabilità attraverso l'utilizzo di metodologie compliant.

Per questo, il Security Competence Center di GFI Italia è un Security Lab specializzato nel seguire e supportare la clientela in tutte le fasi di assessment, di compliance (Basilea II, SOX, ISO 20000, Dlgs196/03) e di accreditamento per la certificazione della sicurezza organizzativa e infrastrutturale. Le certificazioni di software e di sistemi sono sempre affiancate a quelle di processo tramite team specializzati per la certificazione ISO 27001 e ITIL (ISO 20000).
Il Security Lab grazie alla presenza di valutatori abilitati dagli Organi Istituzionali è un Laboratorio di Valutazione della sicurezza di architetture, sistemi, applicazioni, software e prodotti ICT a norma ISO 15408 e ITSEC ed opera ai massimi livelli di garanzia, sia in ambito civile che classificato. Inoltre, un Technical Auditing Team, composto da specialisti accreditati, si occupa delle attività di Vulnerability Assessment, Ethical Hacking, Hardening, Information Security Monitoring e Computer Forensics Analysis.

Oltre a soluzioni nei settori della business continuity e del risk management, il Security Competence Center progetta e realizza architetture di networking e perimeter security (IAM & SSO) facendo leva su solide esperienze e partnership tecnologiche qualificanti quale quella con l'azienda israeliana Check Point.
GFI Italia è infatti Platinum Partner di Check Point, l'azienda leader nella sicurezza su Internet, con una vasta gamma di soluzioni per la sicurezza delle reti, dei dati e la loro gestione.
L'esigenza delle aziende di avere un'architettura di sicurezza affidabile ed unificata che renda sicure sia le comunicazioni - con dipendenti, fornitori, partner e clienti - che le risorse di business, trova risposta nella piattaforma NGX di Check Point che comprende un ampio range di soluzioni dedicate alla sicurezza perimetrale, delle reti interne, delle connessioni web e della posta elettronica. Tra le più recenti novità dell'azienda israeliana, c'è un dispositivo per la gestione unificata delle minacce (UTM) adattato alle esigenze di PMI e imprese multi-sede, l'UTM-1, che assicura una protezione completa e multi-livello contro minacce Internet quali spyware, virus o attacchi alla rete.

La partnership con Check Point si inserisce in una strategia di miglioramento continuo che consente a GFI Italia di progettare per le aziende e per la Pubblica Amministrazione soluzioni per ottimizzare e rendere sicura l'infrastruttura IT, in linea con le più moderne metodologie e standard nazionali ed internazionali.
Potendo contare su personale qualificato ed aggiornato distribuito sul territorio e su partnership di valore, GFI Italia opera da 40 anni con la missione di rappresentare un punto di riferimento nel mercato IT nazionale ed internazionale, restando sempre fedele alla propria identità di azienda affidabile e dinamica e sostenendo costantemente lo sviluppo dei nostri clienti.

GFI Italia SpA
Via Mosca, 52 – 00142 Roma
Tel 06/514651 - Fax 06/51465000
www.gfitalia.it

EXPERT PANEL EXPERT PANEL EXPERT PANEL EXPERT PANEL EXPERT

La parola agli esperti

Mauro Zaccari
Gestione e Sviluppo offerta
GFI Italia

Michele Bianco
Security Competence Center Director
GFI Italia

L'imprenditore che guarda la sua azienda e comincia porsi il problema della sicurezza perché dovrebbe porsi il problema? Da dove dovrebbe iniziare?
Più il business evolve verso modelli aperti all'interscambio tra clienti, dipendenti, fornitori e partner, più diventa necessario guardare alla sicurezza informatica come ad una delle leve strategiche che consente all'azienda di "aprirsi al mondo" mantenendo l'integrità e l'affidabilità dei propri dati. In un campo in continua evoluzione come quello della sicurezza delle reti, un iniziale punto di approccio può essere affidarsi a consulenti esperti che, partendo dall'analisi della rete aziendale, trovino la soluzione ottimale in termini-di tecnologie e di policy, guidando l'imprenditore attraverso le scelte più adatte alla dimensione e alla complessità della propria azienda.

(Mauro Zaccari)

Quali sono tempi, modalità e costi dell'implementazione?
Tempi e costi possono essere ridotti o diluiti nel tempo a patto che per individuare soluzioni appropriate al contesto ci si avvalga realmente di competenze etiche indipendenti dalle tecnologie. La sicurezza è spesso percepita come un costo associato a prodotti ma non é così. La sicurezza non é un prodotto, ma parte del processo organizzativo aziendale che se ben fatto determina un modo di lavorare, di trattare e proteggere dati e informazioni importanti per il business e per la tutela della privacy. *(Michele Bianco)*

Il futuro: in che direzione si andrà? Cosa succederà domani?
La cultura sta cambiando. La sicurezza passa da "costo" ad "opportunità" di creare valore per l'azienda. Una infrastruttura di sicurezza "certificata" e affidabile, coerente espressione del processo aziendale che attua le contromisure individuate dagli assessment potrà evolvere, essere "gestita" e monitorata sia dall'Impresa che dal partner attraverso indicatori (Security Key Performances Indicators) e cruscotti che serviranno a migliorare continuamente i processi interni, risparmiando sugli sprechi e consentendo di differenziare il proprio business da quello dei competitors.

(Michele Bianco)