



FIRENZE TECNOLOGIA

Azienda Speciale della Camera di Commercio

LA SICUREZZA DELLE INFORMAZIONI NELLE PMI

Metodologia Aperta
per la Gestione della Sicurezza
nelle Piccole e Medie Imprese

INTRODUZIONE	5
L'APPROCCIO METODOLOGICO	9
LO STANDARD DI RIFERIMENTO ISO/BS17799	21
LA SICUREZZA DEL SOFTWARE	27
LINK UTILI	36

INTRODUZIONE

Il contesto attuale del mondo della produzione e del lavoro introduce nuovi modelli di business che spingono le aziende a dotarsi di mezzi informatici sempre più sofisticati, per rimanere competitive. Adottare tali modelli significa spesso autorizzare l'accesso al Sistema Informativo Aziendale ai propri clienti, fornitori, partner e collaboratori. E-mail, internet, e-commerce, sistemi CRM sono strumenti oramai diventati indispensabili nelle attività aziendali quotidiane, ma possono altresì trasformarsi in fonti di vulnerabilità per le imprese. Il flusso di documenti e di informazioni digitali, scambiate all'interno di un'impresa e tra imprese diverse, è enorme: tali dati rappresentano un patrimonio strategico e di business fondamentale. Devono quindi essere protetti da tentativi di intrusione da parte di hacker e da terzi estranei all'azienda, ma soprattutto da possibili danneggiamenti causati da un utilizzo inadeguato da parte del personale interno.

Intendendo con l'espressione "sicurezza informatica" l'insieme delle misure organizzative e tecnologiche necessarie a salvaguardare i processi (e la loro evoluzione nel tempo) che gestiscono le informazioni digitali, diventa evidente che la sicurezza informatica rappresenta sempre più uno degli obiettivi prioritari per le imprese moderne.

La sicurezza delle informazioni è un insieme di misure più ampio che da una parte protegge le informazioni elettroniche per mezzo della sicurezza informatica e dall'altro protegge le informazioni cartacee attraverso misure organizzative.

Per raggiungere questi fini è indispensabile che il management aziendale imponga un'adeguata politica per la sicurezza del Sistema Informativo Aziendale, così da valutare i rischi legati all'infrastruttura ed all'organizzazione. La "politica di sicurezza" costituisce la specificazione ad alto livello degli obiettivi di sicurezza, espressi in termini di volontà di salva-

guardare la riservatezza, l'integrità e la disponibilità dell'informazione in presenza di minacce, che l'azienda si propone di conseguire.

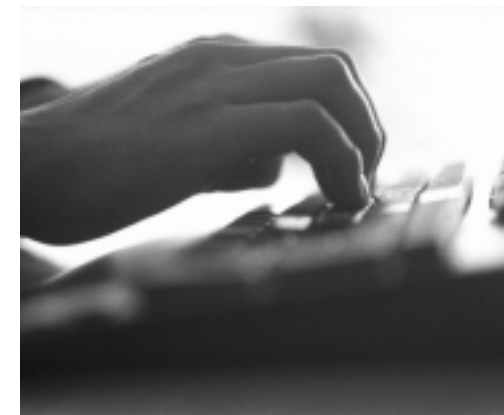
Ad oggi, tuttavia, le imprese non sempre percepiscono il reale valore della sicurezza in ambito informatico e i rischi connessi all'uso delle tecnologie. La mancanza di adeguata attenzione in questo ambito deriva principalmente da tre cause:

- la scarsa conoscenza sulle tematiche della sicurezza e sulle relative procedure;
- una percezione riduttiva delle problematiche legate alla sicurezza, che porta a gestire il problema in modo parziale, ad esempio riducendolo alla semplice installazione di un firewall;
- la valutazione superficiale delle vulnerabilità presenti nei sistemi informatici dell'azienda e della gravità degli attacchi informatici, considerando spesso tali aspetti un problema sporadico o attribuibile ad atti di vandalismo o alla pura casualità.

Sulla base di tali considerazioni, Firenze Tecnologia ha attivato un'iniziativa progettuale per promuovere e sviluppare nelle aziende l'attitudine alla corretta gestione della sicurezza informatica.

IL PROGETTO SICUREZZA INFORMATICA

Come precedentemente espresso, la diffusione dei sistemi informativi e delle nuove tecnologie rende sempre più importante la salvaguardia dei dati aziendali. Firenze Tecnologia sta intervenendo con un progetto, avviato agli inizi del 2003, finalizzato alla creazione di un servizio di informazione e consulenza permanente sulla sicurezza informatica a supporto delle piccole e medie imprese toscane. Il progetto ha lo scopo di introdurre una corretta metodologia per applicare la sicurezza informatica, non più attraverso operazioni saltuarie, bensì con un approccio strategico basato sulla gestione integrata con il business aziendale. Il progetto si è articolato su tre linee guida principali: l'organizzazione di seminari tematici, l'attivazione di un portale dedicato e il coinvolgimento di aziende del territorio.



1. Organizzazione di eventi

Nel 2003 Firenze Tecnologia, in collaborazione con CLUSIT (Associazione Italiana per la Sicurezza Informatica) e l'Associazione Industriali di Firenze, ha organizzato tre seminari di sensibilizzazione sui temi della sicurezza, analizzando i punti di vista organizzativo/procedurale, legale e tecnologico al fine di sviluppare la consapevolezza del rischio informatico. Nel corso dei seminari sono stati divulgati i risultati emersi nell'ambito del progetto, evidenziando le operazioni da svolgere per salvaguardare il patrimonio informativo, per essere in regola con la normativa vigente e per favorire la produzione di valore aggiunto nella creazione di business. Il calendario degli eventi proseguirà nel corso del 2004.

2. Sviluppo di un portale tematico www.SicurInfo.it

Si tratta di uno strumento di comunicazione per accompagnare gli imprenditori verso un percorso consapevole di adeguamento e investimento nella direzione della sicurezza. Sicurinfo.it pubblica informazioni guida (percorsi guidati, legati agli obblighi legali e all'analisi del rischio) utili alle PMI al fine di intraprendere il percorso verso la politica di sicurezza, secondo un modello di riferimento creato in collaborazione con i professionisti e le aziende aderenti al progetto. Le pubblicazioni, non a cadenza periodica, approfondiscono questa tematica nei diversi aspetti che la compongono, fornendo una documentazione approfondita, liberamente scaricabile dal sito.

3. Sperimentazioni all'interno delle aziende

Usufruendo della collaborazione dell'Ente Cassa di Risparmio di Firenze, è stato possibile intervenire concretamente nella soluzione di problemi relativi alla sicurezza informatica in venti aziende pilota. Infatti, il progetto ha consentito di fornire a ciascuna di queste imprese otto giornate di consulenza, erogata da parte di esperti del settore, al fine di progettare all'interno delle aziende un adeguato processo di gestione della sicurezza informatica. Nell'erogazione di queste consulenze, Firenze Tecnologia si è avvalsa delle competenze di un gruppo di imprese con provata esperienza specifica nel settore di intervento.

Il processo sviluppato nelle singole aziende pilota è così sintetizzabile:

- analisi del grado di sicurezza informatica dell'impresa, a partire dalle procedure e infrastrutture adottate;
- identificazione di ambiti specifici su cui mettere a punto un piano d'azione;
- sviluppo di soluzioni concrete.

Il successo di questi interventi ha fatto sì che la Camera di Commercio di Firenze consentisse di proseguire l'attività per erogare ad ulteriori aziende pilota questo servizio, orientando verso una gestione strutturata della sicurezza informatica.

CHIAVE DI LETTURA E FINALITÀ DEL DOCUMENTO

Le azioni sopra indicate hanno consentito di sviluppare un modello di intervento nelle PMI. Tale approccio metodologico viene proposto in questo documento. Non si tratta propriamente di una "nuova metodologia" ma piuttosto dell'indicazione di un percorso strutturato e dinamico, basato sugli standard internazionali di riferimento (in particolare la norma ISO/BS17799), sul rispetto della normativa vigente, e sul buon senso.

Il metodo prende in considerazione l'intero processo di gestione delle informazioni e prevede il coinvolgimento e l'integrazione di tutti gli elementi della catena del valore dell'impresa, ovvero le persone, i processi, le tecnologie, al fine di consentire la corretta gestione del rischio informatico all'interno dell'azienda.

L'APPROCCIO METODOLOGICO

La Sicurezza Informatica è un processo di impostazione e di gestione delle misure atte a garantire la confidenzialità, l'integrità e la disponibilità dei "flussi di gestione delle informazioni digitali", in modo conforme alla normativa vigente.

Per "flusso di gestione delle informazioni" si intende il complesso delle persone, delle tecnologie e delle forme organizzative che intervengono nel processo di acquisizione, elaborazione, archiviazione ed utilizzo dei dati. La gestione della sicurezza informatica richiede un processo di analisi di tre aspetti complementari: il contesto organizzativo, normativo e tecnologico.

LE MISURE ORGANIZZATIVE

Per quanto concerne l'implementazione operativa dell'aspetto organizzativo, l'approccio fornisce un modello in linea con la ISO/BS17799. Vengono prese in esame le normative vigenti in Italia e suggerite le operazioni pratiche per la gestione tecnologica delle problematiche di base. Tale gestione può coinvolgere sia il personale interno, sia risorse esterne. Nel caso si faccia uso di consulenti esterni, sarà opportuno dedicare una particolare attenzione alla contrattualistica che ne regola il rapporto, definendo in modo quanto più chiaro possibile le rispettive responsabilità.

Gli obiettivi del management

La definizione di una politica di sicurezza attribuisce importanza strategica al trattamento delle informazioni e concretizza la volontà di difendere la confidenzialità, l'integrità e la disponibilità dei dati.



La politica della sicurezza si concretizza in un insieme di interventi per le seguenti finalità:

- proteggere le informazioni da accessi non autorizzati;
- tutelare la riservatezza delle informazioni;
- impedire la concessione di autorizzazioni al trattamento e alla modifica delle informazioni da parte di soggetti non autorizzati;
- garantire la disponibilità delle informazioni agli utenti autorizzati;
- redigere piani dell'attività aziendale costantemente aggiornati e controllati;
- formare il personale in materia di sicurezza delle informazioni;
- analizzare i punti deboli e le violazioni alla normativa vigente.

Il gruppo di lavoro

L'attuazione della politica della sicurezza richiede la costituzione di un gruppo di lavoro. I componenti del team si assumono in toto la responsabilità del sistema di gestione della sicurezza. Per quanto riguarda la composizione del gruppo, esiste una distinzione tra quello proprio delle piccole e medie imprese e quello che opera nelle grandi aziende.

CASO PICCOLA MEDIA IMPRESA

Il team è costituito da:

- un esperto nell'implementazione di modelli tipo ISO/BS17799;

- un titolare dell'impresa oppure da un responsabile con facoltà di gestione del budget;
- un responsabile dei sistemi informativi.

CASO GRANDE IMPRESA

È consigliabile aggiungere ai componenti della piccola e media impresa le seguenti figure:

- responsabile della qualità (se l'azienda ha un modello di certificazione per processi di tipo ISO9000);
- responsabile legale interno o esterno all'azienda.

Parallelamente alla definizione del gruppo di lavoro, vengono individuati i ruoli e le responsabilità diffusi su tutto il tessuto organizzativo dell'azienda descrivendoli visivamente attraverso un organigramma. Si è riscontrato che nelle aziende organizzate con un responsabile della sicurezza informatica, spesso coincidente con il responsabile della qualità, risulta molto semplificato il processo interno di adeguamento al modello proposto.

L'ambito di applicazione

Primo compito del gruppo di lavoro è l'individuazione degli ambiti di lavoro, intervenendo sui processi interessati e facendone una valutazione per verificare lo stato attuale e le esigenze di miglioramento. L'ambito di applicazione può essere definito sia in senso fisico (es. uno stabilimento aziendale), che secondo una logica di processo. Il documento cerca di individuare i processi fondamentali dell'impresa, considerando che ogni azienda li struttura sulla base di uno specifico modello di business e delle risorse possedute.

ALCUNI DEI PROCESSI INDIVIDUABILI:

- gestione delle informazioni relative all'approvvigionamento;
- gestione delle informazioni relative al magazzino;
- gestione delle informazioni relative alla produzione;
- gestione di informazioni sensibili ai sensi della Legge sulla Privacy;
- gestione di informazioni per conto terzi;
- gestione di informazioni riservate dei clienti/fornitori;
- pubblicazione di informazioni su server web;
- accesso alle informazioni su sistemi aziendali dall'esterno della rete da parte di clienti/fornitori;
- accesso alle informazioni su sistemi aziendali da parte di sedi remote.

L'analisi e la gestione dei rischi

Individuati i processi strategici, questi vengono sottoposti ad analisi al fine di identificare le minacce più pressanti per la sicurezza. Spetta a questo punto al responsabile della sicurezza il compito di attivare le contromisure più idonee a tutelare l'impresa da ogni possibile rischio in ambito informatico.

Procedure di sicurezza

Le procedure di sicurezza sono le disposizioni operative che descrivono i processi e il funzionamento delle misure che sono adottate in azienda (ACL - Access Control List, backup, gestione di servizi, ecc.).

Di seguito sono elencate le procedure più rilevanti, considerando che alcune di queste non sono applicabili a tutti i casi aziendali.

LE PROCEDURE PER GLI UTENTI DEL SISTEMA INFORMATIVO:

- le procedure da far sottoscrivere ai dipendenti al momento dell'assunzione;
- le procedure per l'utilizzo del software: descrizione dei software utilizzabili in azienda;
- le procedure per il rispetto del copyright: descrizione delle modalità di utilizzo del software (licenze e copyright);
- le procedure per l'utilizzo del PC aziendale;
- le procedure per l'utilizzo di notebook nella rete interna;
- le procedure per l'utilizzo dell'e-mail;
- le procedure per l'utilizzo della connessione internet;
- le procedure per l'utilizzo del sistema antivirus;
- le procedure per la gestione del nome utente e della password;
- le procedure per l'accesso alle risorse aziendali (definizione ACL) - controllo accessi;
- le procedure per la classificazione delle informazioni;
- le procedure per la crittografia delle informazioni;
- le procedure per la formazione degli utenti;
- le procedure per il trattamento con strumenti elettronici di informazioni sensibili ai sensi della legge sulla privacy.

LE PROCEDURE PER L'AMMINISTRAZIONE DEI SISTEMI:

- le procedure per la gestione del backup;
- le procedure per la custodia fisica dei backup una volta verificata la loro integrità;
- le procedure per definire le modalità di recupero delle informazioni in caso di incidenti;
- le procedure per la gestione degli incidenti informatici;
- le procedure per la manutenzione dei sistemi server;
- le procedure per la manutenzione dei sistemi clienti;
- le procedure per la manutenzione dei sistemi di rete;
- le procedure per la protezione del perimetro logico aziendale;
- le procedure per la gestione dell'inventario hardware e software;
- le procedure per la gestione del giornale degli incidenti.

Il piano di formazione

Redatto il documento della politica della sicurezza, il management provvede a comunicarlo a tutto il personale dell'azienda.

Esistono molteplici metodologie e canali informativi utilizzabili, tra essi di fondamentale importanza è il piano di formazione, organizzato per il personale che interviene nel processo da salvaguardare.

Più precisamente, per quanto riguarda il personale impiegato nel trattamento dei dati sensibili/personali, le disposizioni sono disciplinate dal Testo Unico sulla Privacy.

In merito alle informazioni che costituiscono il core business dell'impresa, le risorse umane da coinvolgere nel processo formativo sono quelle che intervengono in attività e ambiti critici nel trattamento dei dati.

LE MISURE LEGALI

Il contesto normativo italiano si sta ampliando rapidamente.

Di seguito si riportano alcuni riferimenti del panorama normativo in generale e degli ultimi aggiornamenti:

- Decreto Legislativo n° 196 del 30/06/2003; in G.U. 29/07/03, Serie gen. n. 174, Suppl. ord. n. 123/L in vigore dal 1/01/2004, sostituisce la Legge n. 675/1996 e successive disposizioni modificative ed integrative e il DPR318/99. Conosciuto anche come "Testo Unico sulla Privacy", ad oggi (Gennaio 2004) è la legge di riferimento per una corretta gestione delle politiche di sicurezza.
- Decreto Legge n° 354 del 24/12/2003; in G.U. n. 300 del 29-12-2003 riscrive interamente l'art. 132 "Conservazione dei dati di traffico per altre finalità".
- Decreto Legislativo n° 68 del 09/04/2003 – Attuazione della Direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione.
- Direttiva del Presidente del Consiglio dei Ministri 16/01/2002, pubblicata sulla G.U. n. 69 del 22/03/2002 "Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali" dedicata alla Pubblica Amministrazione.
- Legge n° 248 del 18/08/2000 – Nuove norme in tutela del diritto d'autore.
- Decreto legislativo n° 169 del 06/05/1999 – Attuazione della Direttiva 96/9/CE relativa alla tutela giuridica delle banche dati.
- Legge n° 547 del 23/12/1993: "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica" (Legge sui crimini informatici).
- Decreto Legislativo n° 518 del 29/12/1992 – Attuazione della Direttiva 91/250/CE relativa alla tutela giuridica del software.

Le aziende che trattano dati personali, sensibili e giudiziari, in forma elettronica o cartacea, devono garantire una serie di "misure minime" di sicurezza.

NEL CASO DEL TRATTAMENTO DEI DATI DEI DIPENDENTI DA PARTE DELL'AZIENDA, I DATI SENSIBILI IN QUESTIONE SONO:

- la documentazione relativa alle visite mediche periodiche svolte in ambito aziendale (L. 626, sicurezza sul lavoro) o dati relativi alla salute prodotti in altri contesti (in questo caso, in presenza di patologie accertate, deve essere informato il titolare del trattamento);
- iscrizione alle liste sindacali



LE MISURE MINIME PREVISTE PER I DATI PERSONALI:

- i responsabili aziendali del trattamento dei dati personali devono attenersi ad una procedura sul trattamento tecnico/organizzativo di tali dati, formalizzata per iscritto;
- il decreto prevede l'implementazione di politiche di backup settimanali;
- redazione di una lista delle aree soggette a trattamento e dei singoli incaricati; aggiornamento periodico e verifiche (almeno annuali) della lista;
- installazione e aggiornamento software antivirus (almeno 6 mesi);
- installazione e aggiornamento software per prevenire vulnerabilità e correggere difetti (almeno annualmente, in presenza di dati sensibili ogni 6 mesi).

ULTERIORI MISURE PER DATI SENSIBILI E GIUDIZIARI:

oltre alle misure sopra indicate, in caso di dati sensibili e giudiziari occorre aggiungere le seguenti misure:

- istruzioni organizzative e tecniche per la custodia e l'uso di supporti rimovibili (floppy, cd-rom);
- istruzioni per la distruzione controllata dei supporti e per la cancellazione delle informazioni contenute (non tecnicamente ricostruibili);
- adozione di idonee misure per il ripristino dei dati in caso di danneggiamento dei dati e/o degli strumenti.

Alcuni di questi dati possono essere gestiti in outsourcing presso strutture terze (commercialista, esperto in gestione paghe, medico esterno, ecc.). In questo caso è fondamentale che le aziende redigano una regolare lettera di incarico al trattamento dati anche a tali soggetti. L'installatore deve rilasciare al responsabile del trattamento dati un documento che descriva l'intervento effettuato e che attesti la conformità alle disposizioni del disciplinare tecnico.

Infine, è necessario regolamentare le metodologie di scambio dei dati sensibili e di relativa gestione/archiviazione da parte di chi li prende in carico.

Il "Documento Programmatico sulla Sicurezza"

Le regole finora discusse, insieme alle altre previste dal codice (riportate nell'Appendice B del Testo Unico), devono essere raccolte nel Documento Programmatico sulla Sicurezza. La loro attuazione è responsabilità del titolare del trattamento che ha la facoltà di delegarla ad uno o più responsabili incaricati.

Il Documento Programmatico sulla Sicurezza, sulla base dell'analisi dei rischi, definisce la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati. Costituisce, quindi, un punto cruciale nella definizione delle misure di sicurezza adottabili poiché permette l'immediata verifica del livello attuale di sicurezza informatica, identifica le aree aziendali a maggior rischio e gli strumenti di garanzia adeguati.

IL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA SI COMPONE DELLE SEGUENTI PARTI:

- l'elenco dei trattamenti dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi;
- i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;
- i criteri e le procedure per assicurare l'integrità e la disponibilità dei dati;
- i criteri e le procedure per la sicurezza delle trasmissioni dei dati;
- l'elaborazione di un piano di formazione per gli incaricati;

- la descrizione dei criteri da adottare per garantire l'adozione delle misure di sicurezza in caso di trattamenti di dati affidati all'esterno della struttura titolare.

La normativa vigente rende obbligatoria la redazione del Documento Programmatico sulla Sicurezza per tutti i soggetti che trattano dati sensibili/giudiziari, ed inoltre richiede di evidenziare gli aggiornamenti nella relazione di accompagnamento al bilancio d'esercizio.

LE MISURE TECNOLOGICHE

La rete interna ed esterna

Per tutte le reti aziendali, che utilizzano internet per i servizi di navigazione o posta elettronica presso un provider, è necessario effettuare il servizio di gateway e separazione logica della rete privata da quella pubblica. A tal fine, può essere sufficiente utilizzare un buon router. Non sempre è necessaria l'installazione di un firewall.

FUNZIONALITÀ CHE IL ROUTER DEVE GARANTIRE:

- eliminare la possibilità di accedere in Telnet dall'esterno (se non necessario per l'amministrazione);
- usare una password (composta da caratteri e numeri) di amministratore per accedere al terminale, cambiandola periodicamente;
- abilitare solo le porte necessarie ai servizi attivi (21 per FTP, 22 per ssh, 80 per http, ecc);
- nel caso la connessione xDSL non sia più disponibile, predisporre una porta ISDN su cui è preconfigurata una linea di backup che fa una chiamata dial-up verso un altro provider.

La segmentazione della rete

Sul mercato sono disponibili molteplici soluzioni, sia hardware che software, in grado di risolvere la necessità di segmentazione della rete, attraverso l'uso di firewall, in aree funzionalmente omogenee e con livelli di vulnerabilità similari.

- Internet: solo il proxy server aziendale e i server SMTP e DNS devono potersi connettere direttamente con internet; non deve essere ammesso il processo inverso.



- DMZ: i sistemi compresi in questa rete sono raggiungibili direttamente da internet (questa è l'unica rete che, insieme alla VPN, può accettare le connessioni dalla Rete) solo per l'accesso a servizi specifici. Sono da evitare, invece, le connessioni verso internet.
- Rete utenti: questa rete comprende tutte le workstation. Non deve accettare connessioni da nessun segmento. Sono ammesse solo le connessioni verso la rete dei server e, solo in casi specifici, verso le altre reti. Le connessioni indirette verso internet devono essere filtrate il più possibile.
- Rete server: questa rete comprende tutti i server e può accettare connessioni provenienti dalle altre reti interne. I sistemi che la compongono, devono necessariamente effettuare connessioni verso internet e perciò devono essere controllati periodicamente.
- Rete VPN: questa rete comprende il server VPN che è accessibile da internet e consente di stabilire collegamenti verso la rete server (questa funzione può essere espletata dal firewall).

L'utilizzo delle ACL (Access Control List)

Le ACL possono essere create in modo specifico per monitorare gli accessi ad un servizio specifico, oppure possono essere utilizzate in modo centralizzato, attraverso l'introduzione di un dominio. L'utilizzo delle ACL, consentendo la gestione centralizzata degli utenti, determina vantaggi significativi nell'amministrazione del sistema e dei suoi utenti.

LE POLITICHE TIPICHE DELLE ACL SONO:

- suddivisione fra tipologie di utenti diversi (interni/ esterni/ wireless, ecc.);
- suddivisione delle tipologie di servizi accessibili per gli utenti;
- abbinamento fra utenti e servizi in modo da raggiungere il livello di controllo desiderato.

L'introduzione del controller di dominio

Si tratta di un sistema software che permette l'autenticazione degli utenti al dominio di appartenenza, così da semplificare e centralizzare la gestione degli stessi. L'amministrazione del dominio richiede tempo e skill avanzati, fornendo però il vantaggio di distribuire le nuove politiche di dominio in modo facile e veloce.

Le postazioni client

Il sistema operativo delle postazioni client deve permettere l'accesso alla rete solo dopo che l'utente ne faccia richiesta. Tale accesso è regolato da un processo di riconoscimento anche attraverso un sistema di autenticazione debole come nome utente e password. In ogni caso non deve essere possibile accedere alla rete facendo ESC sul login.

LE POLITICHE MINIME DI GARANZIA ALL'ACCESSO SONO:

- l'introduzione dell'uso di una password "riservata" dell'utente per accedere alla rete aziendale;
- l'aggiornamento del sistema operativo (installazione dei service pack, aggiornamento delle protezioni del Sistema Operativo), che può essere svolto direttamente dagli utenti oppure distribuiti attraverso un sistema centralizzato e governato dall'amministratore di sistema;
- la presenza di un antivirus, su ciascuna postazione client Microsoft, aggiornabile manualmente da parte dell'utente o, preferibilmente, attraverso una distribuzione programmata.

Le patch dei sistemi

Per mantenere in sicurezza i sistemi aziendali è necessaria la manutenzione e l'aggiornamento degli applicativi e dei sistemi operativi con le patch adeguate. A questo scopo, Firenze Tecnologia ha aderito al pro-

getto europeo EISPP (European Information Security Promotion Programme), in collaborazione con CLUSIT. In tale ambito, alle imprese, viene distribuito in modo tempestivo il materiale di prevenzione sviluppato da qualificati gruppi di lavoro CERT (Computer Emergency Response Team) europei, che consente all'utente di venire a conoscenza di vulnerabilità dei propri sistemi, delle possibili conseguenze e delle azioni per ridurre il rischio.

GLI STEP DI EROGAZIONE DEL SERVIZIO SONO:

- la mappatura dei sistemi presenti in azienda;
- l'iscrizione al servizio;
- l'invio giornaliero delle patch relativamente ai sistemi presenti in azienda;
- l'applicazione, da parte dell'amministratore, delle patch ai sistemi.

Un'attività complementare è quella di "hardening" dei sistemi, intervenendo sulle configurazioni dei sistemi operativi e degli applicativi per renderli il meno possibile vulnerabili. Ne sono esempi l'installazione dei soli servizi necessari, la rimozione dei privilegi e password di default, ecc.

Le politiche e la custodia di backup per postazioni client

Per centralizzare l'amministrazione del backup su postazioni client può essere utile introdurre un file server, su cui gli utenti salvano le informazioni fondamentali per l'azienda. La procedura di backup per recuperare le eventuali informazioni perdute (anche attraverso backup passati) deve essere condivisa dal personale preposto.

È fondamentale associare alla pratica del backup una procedura di restore e verificare periodicamente il funzionamento dei meccanismi di ripristino dei dati.

Il metodo da impiegare per la custodia fisica dei backup dipende dal grado di riservatezza/sensibilità delle informazioni trattate. Generalmente i backup si custodiscono in azienda, ma collocati in altri luoghi rispetto ai server, secondo una policy specifica. Può essere necessario, in alcuni casi, mantenere copia dei backup in locazioni remote che non sono soggette alle stesse minacce della sede principale. Per prevenire situazioni di grave rischio può essere implementato un piano di disaster recovery, tale da consentire il recupero delle informazioni e dei sistemi attraverso procedure comprovate.

LO STANDARD DI RIFERIMENTO ISO/BS17799

Per l'impostazione del "Sistema di Gestione della Sicurezza delle Informazioni" (SGSI) all'interno di un'azienda, il riferimento è la norma inglese BS7799 (2002) che è stata ripresa dalla direttiva europea ISO/IEC 17799 (2000).

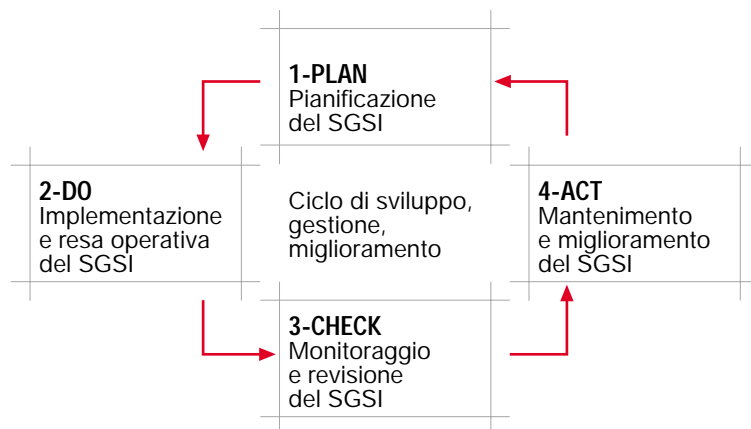
Lo standard BS7799 è diviso in due parti:

- una prima parte già riconosciuta dall'International Standard Organization (ISO/BS17799);
- una seconda parte in fase di riconoscimento (BS7799-2).

A SEGUITO DEL RICONOSCIMENTO DELLA NORMA A LIVELLO NAZIONALE, IN ITALIA SI SONO VERIFICATI DUE IMPORTANTI CAMBIAMENTI IN MATERIA DI SICUREZZA

- SINCERT (www.sincert.it), Sistema Nazionale per l'Accreditamento degli Organismi di Certificazione, alla data del 31 Dicembre 2003, ha accreditato RINA (www.rina.org), DNV Italia (www.dnv.it), e IMQ (<http://www.imq.it>) a rilasciare certificazioni sui sistemi di gestione per la sicurezza delle informazioni secondo lo standard BS7799-2.
- Il 16 Gennaio 2003, il Ministero per l'Innovazione Tecnologica, d'intesa con il Ministero delle Comunicazioni, ha rilasciato la cosiddetta "Direttiva Stanca per la PA" in cui sono descritte le Best Practice per la gestione di un sistema di sicurezza delle informazioni nelle pubbliche amministrazioni.

IL MODELLO PROCESSUALE PROPOSTO DALLA NORMA BS/ISO SI COMPONE DELLE SEGUENTI FASI



1 - LA FASE PLAN

La fase di pianificazione si pone l'obiettivo di impostare tutti gli elementi necessari per predisporre una concreta programmazione delle attività di sicurezza, di definire gli obiettivi di sicurezza che l'azienda intende perseguire, di calcolare il livello di rischio cui le risorse risultano esposte e di gestire, infine, le opzioni applicabili al rischio residuo.

LE ATTIVITÀ DA SVOLGERE IN FASE PLAN E SU CUI SI IMPLEMENTA IL SGSI:

- Definizione del documento strategico per la politica di sicurezza
- Ambito di applicazione
- Risk assessment
- Risk management
- Scelta delle contromisure
- Dichiarazione di applicabilità

1.1 - Definizione del documento strategico di politica di sicurezza

Il documento strategico di politica della sicurezza non è un documento di tipo operativo, bensì un testo in cui l'azienda comunica ai propri dipen-

denti quali sono o saranno le proprie iniziative in materia, concentrando l'attenzione sui seguenti aspetti:

- linee guida sugli investimenti in sicurezza dell'azienda;
- le responsabilità ad alto livello;
- i riferimenti di legge cui attenersi.

1.2 - Ambito di applicazione

È importante focalizzare bene l'ambito in cui l'azienda intende applicare le regole per ottimizzare gli investimenti e averne un ritorno diretto e verificabile.

Ambiti diversi con priorità diverse necessitano politiche specifiche. È possibile, tuttavia, individuare due aree di intervento principali:

ORGANIZZAZIONE, NEL SUO COMPLESSO

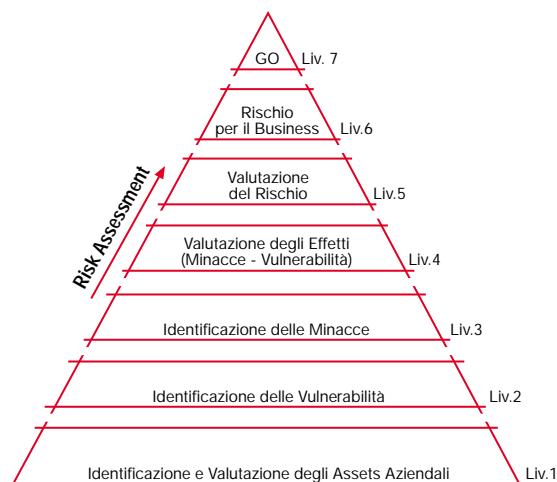
Include tutti i processi e i servizi che l'impresa è in grado di erogare. Fra questi possono essere citati:

- il processo di gestione delle informazioni relative a clienti/fornitori;
- il processo di gestione dell'integrità, disponibilità, autenticità, dell'informazione accessibile per Rete Telematica (es. anagrafe dei comuni, deposito bilancio presso la CCIAA, ecc.);
- l'analisi, progettazione, sviluppo, mantenimento e fornitura di servizi di internet banking;
- altri processi o servizi strategici per l'impresa;
- le informazioni che afferiscono al processo di produzione;
- le informazioni inerenti la progettazione e produzione di prodotti ed oggetti, affidata a terzi ma sviluppata sulla base del know-how aziendale.

1.3 - Risk assessment

La valutazione dei rischi e la selezione delle contromisure da adottare sulla base dei livelli di rischio è un'attività da ripetere nel tempo. Infatti, le priorità del business aziendale, le minacce, la variazione nell'organizzazione, sono variabili e come tali gli interventi di sicurezza devono essere periodicamente aggiornati.

L'obiettivo dell'analisi del rischio è di ridimensionare le minacce in relazione alla tipologia e al contesto dell'attività aziendale. L'introduzione di contromisure specifiche, infatti, riduce drasticamente le probabilità che i rischi si possano trasformare in danni economici.



LA FASE DI RISK ASSESSMENT COMPRENDE:

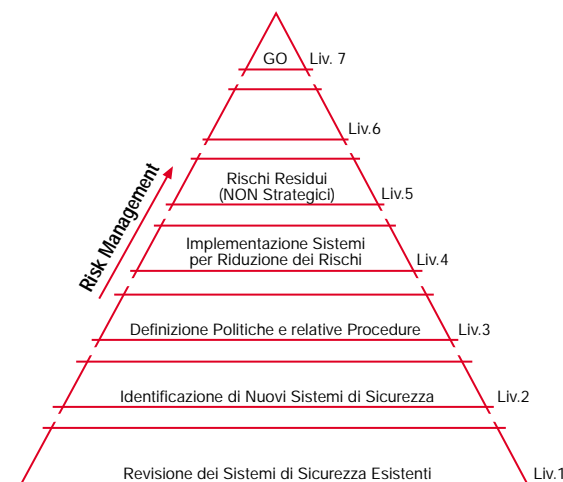
- la catalogazione degli asset da proteggere (informazioni, software, hardware, ecc.);
- l'assegnazione di un valore graduato agli asset (es. da 1 a 10);
- la valutazione delle minacce rispetto agli asset definiti (individuazione dei punti deboli);
- la determinazione delle contromisure da adottare in relazione alle minacce previste.

1.4 - Risk management

La gestione del rischio viene fatta partendo dai dati raccolti nella precedente analisi. Si inizia con l'individuazione dei sistemi di controllo esistenti e quelli da implementare, che, ad un'analisi strategica, risultano fondamentali per ridurre il rischio.

GLI OBIETTIVI DELL'IMPRESA:

- ridurre il rischio ad un livello accettabile per il business aziendale, attraverso le apposite contromisure;
- decidere di accettare il rischio se non è possibile eliminare attività che lo generano;
- trasferire il rischio ad altre parti come fornitori o assicuratori.



1.5 - Scelta delle contromisure

Per ridurre le probabilità che i rischi si possano trasformare in danni economici per l'azienda devono essere identificate opportune contromisure, la cui implementazione deve tener conto dei seguenti fattori:

- il costo dell'attivazione in rapporto al rischio;
- i potenziali danni economici diretti (es. impossibilità di erogazione di servizi);
- i potenziali danni economici indiretti (es. perdita di immagine per scarsa affidabilità).

Le contromisure che non risultano convenienti sulla base dei tre precedenti fattori, non vengono prese in considerazione. Tutto ciò che non viene gestito si trasforma in un potenziale rischio per l'impresa.

1.6 - Dichiarazione di applicabilità

Alla fine di mappare il sistema SGSI con la norma BS7799-2, viene richiesto all'organizzazione di indicare, in un documento scritto, quali dei 127 controlli della norma sono applicabili nel proprio sistema e quali non lo sono. Per quelli non applicabili, l'organizzazione deve darne giustificazione.

Mentre i primi 5 passi della fase Plan sono preparatori alla norma, anche se non relazionati direttamente, al passo 6 la norma diviene centrale: la Dichiarazione di Applicabilità costituisce la mappa documentale a corredo del processo, e consente di fornire una visione organica di tutta la documentazione che fa parte del "Piano di Sicurezza" aziendale.

2 - LA FASE DO

Al fine di rendere operativo il SGSI, la fase di implementazione prevede:

- l'attuazione delle decisioni e delle soluzioni individuate nella fase Plan;
- l'implementazione delle contromisure fisiche, logiche e organizzative;
- la predisposizione degli strumenti tecnici e procedurali atti a rilevare ed analizzare gli eventi che impattano sulla sicurezza, oggetto delle successive fasi di verifica e monitoraggio.

3 - LA FASE CHECK

La fase prevede la valutazione e la misurazione delle prestazioni del SGSI, attraverso:

- la pianificazione di audit periodici;
- il monitoraggio continuo dell'efficacia delle misure di sicurezza;
- l'investigazione a fronte di incidenti;
- l'analisi dei cambiamenti del contesto di riferimento.

Sulla base dei risultati di tali valutazioni, in caso di inefficienze, vengono predisposte le opportune azioni preventive o correttive. In caso di risultati soddisfacenti, occorre prevedere una standardizzazione del processo.

4 - LA FASE ACT

Affinché l'efficacia e l'efficienza dell'SGSI e delle misure di sicurezza implementate siano mantenute nel tempo, in questa fase vengono eseguite:

- le azioni preventive e correttive individuate a seguito delle attività di verifica;
- le attività volte alla standardizzazione del processo.

Gli interventi sono mirati soltanto a quelle specifiche aree che necessitano di essere migliorate, reiterando il processo a partire dalle attività risultate fonti di errori e/o inefficienze.

LA SICUREZZA DEL SOFTWARE

Premesso che ogni elemento del sistema informativo aziendale è potenzialmente vulnerabile e la conoscenza e la gestione di queste criticità costituiscono per l'azienda una problematica prioritaria, si vogliono fornire in questa sezione del documento una serie di elementi per evidenziare i punti di vicinanza fra la norma ISO/BS17799 e l'utilizzo del Software Libero.

Prima di entrare nello specifico argomento è utile fare alcune premesse.

Una parte considerevole delle problematiche aziendali relative al software su postazioni client sono tipicamente causate da applicazioni note comunemente con il nome di "software malevolo", una tipologia di software, che include virus, worm, cavalli di troia e bombe logiche, ha raggiunto un'ampia diffusione poiché capace di "infettare" il software su sistema operativo Windows*.

UNO DEI PROBLEMI DELLE AZIENDE È UTILIZZARE UN "SOFTWARE LEGALE", OVVERO UN SOFTWARE DI CUI SI RISPETTANO I TERMINI DI LICENZA FORNITI DAL PRODUTTORE.

Un fattore importante, anche ai fini della sicurezza, è la possibilità, da parte dell'amministratore di sistema, di poter realizzare le installazioni all'interno dell'azienda partendo da un codice sorgente. Questo non risulta sempre applicabile sia per la non disponibilità dei sorgenti, sia per la necessità di competenze specifiche per poter installare correttamente il codice in questo modo. Il codice sorgente, comunque, garan-

* per approfondimenti si veda ad esempio "Cyber-insecurity: the cost of monopoly - How the dominance of Microsoft's products poses a risk to security" (2003) di Geer Pflieger, Schneier, Quarterman, Metzger, Bace, Gutmann, reperibile all'indirizzo <http://www.cclanet.org/papers/cyberinsecurity.pdf>

tisce la possibilità di conoscere e utilizzare le linee di codice originarie, così come sono state scritte inizialmente dal programmatore. Sono utilizzabili anche software compilati (binari), per i quali, tuttavia, è consigliabile che la “catena di fiducia”, ovvero il percorso del codice sorgente da un user all’altro fino alla installazione in azienda, sia nota e verificabile. Premesso questo, emerge la differenza fondamentale tra software proprietario e Software Libero. Nel primo caso, la garanzia sulla sicurezza dipende unicamente dal produttore e da ciò che quest’ultimo dichiara in proposito. Nel caso del Software Libero, invece, l’azienda può esaminare (e far esaminare a terzi) il codice che verrà installato, innalzando quindi il livello di sicurezza.

Spetta all’azienda titolare dei diritti di sfruttamento decidere la tipologia di licenza da utilizzare. Può fornire una licenza proprietaria oppure optare per licenze di Software Libero, come la GNU/GPL.

Il Software Libero è caratterizzato dal fatto che il codice è disponibile senza limitazioni e garantisce all’utente “le quattro libertà”, ovvero:

LIBERTÀ 0:

- libertà di eseguire il programma per qualunque scopo senza vincoli sul suo utilizzo;

LIBERTÀ 1:

- libertà di studiare il funzionamento del programma e di adattarlo a specifiche esigenze;

LIBERTÀ 2:

- libertà di redistribuire le copie del programma;

LIBERTÀ 3:

- libertà di migliorare il programma e di distribuirne liberamente i miglioramenti.

In particolare, il Software Libero distribuito tramite licenza GNU/GPL (fornita dalla Free Software Foundation e scaricabile dall’indirizzo <http://www.gnu.org/licenses/gpl.txt>), a cui questa appendice fa riferimento, rispetta queste quattro libertà.

La Norma ISO in materia di sicurezza del software

Come già descritto, il modello processuale proposto dalla norma BS7799-2 prevede alla conclusione della fase di pianificazione una Dichiarazione di Applicabilità, con la quale si indicano quali dei 127 controlli previsti dalla norma sono di interesse dell’azienda e nelle fasi successive si vanno a definire le contromisure e le modalità di gestione operativa di tali aspetti. Di seguito si analizzano i principali controlli identificandoli con la numerazione riportata nella norma dedicati alla sicurezza del software, esplicitando i motivi per i quali le contromisure da adottare in tema di sicurezza informatica sono già contenute, in buona parte, nel Software Libero. I controlli considerati sono identificati con la numerazione riportata nella norma.

Controllo n° 8.3: la protezione contro il software malevolo

IL SOFTWARE LIBERO, COME DESCRITTO DA RENZO DAVOLI (2002), GARANTISCE UNA MINORE PROBABILITÀ DI INFEZIONI.

- Tutto il codice malevolo non autoreplicante (cavalli di troia, bombe logiche, ecc.), in linea teorica, non può venire nascosto in programmi a codice sorgente aperto per il motivo che quest’ultimo è leggibile a tutti. Va tuttavia considerato il fatto che questa garanzia ha una validità più teorica che pratica. Esistono, infatti, contingenze concrete in cui vengono implementate tecniche di occultamento di canali nascosti sottoforma di operazioni apparentemente innocue, ma che nascondono funzionalità non dichiarate e potenzialmente rischiose per la sicurezza del software.
- I programmi liberi utilizzati sono stati scritti, controllati e corretti da moltissimi sviluppatori, poiché sono veicolati e impiegati nell’ambito di una comunità di utilizzatori aperta e in continua espansione. In questo senso, i programmi che arrivano ad essere utilizzati hanno superato una sorta di “selezione naturale” fra i prodotti con caratteristiche simili, presentando perciò solitamente una maggiore resistenza alle “infezioni” rispetto agli altri. In sintesi, questo processo garantisce che la qualità del codice di un Software Libero sia molto spesso superiore a quella di programmi proprietari.
- Nel caso del Software Libero, il continuo processo di scambio e di divulgazione di informazioni, risultati e correzioni tra i membri della comunità



on line, assicura che ogni possibile rischio o danno alla sicurezza venga tempestivamente individuato e corretto con maggiore precisione, rispetto al software proprietario. In quest'ultimo caso, spesso, i fornitori tendono a mantenere riservate le notizie relative ai problemi di sicurezza fino a che non sia disponibile la patch adatta. Così facendo però gli amministratori di sistema si trovano a combattere ad armi impari con i cracker attaccanti, con il solo aiuto delle informazioni provenienti da altri utenti di tali prodotti. In ogni caso, anche se potessero usufruire prontamente delle notizie sui bug, sarebbero posti di fronte ad un'unica scelta: sospendere i servizi o mantenere inalterata la situazione, lasciando che i sistemi siano attaccabili da tutti coloro che conoscono il bug.

Controllo n° 8.3.1– Controlli contro il software malevolo

AI FINI DI PREVENIRE O RESISTERE AGLI ATTACCHI DEL SOFTWARE MALEVOLO, POSSONO ESSERE IMPLEMENTATE APPOSITE AZIONI:

- L'introduzione di una procedura formalizzata, ovvero di un documento scritto che permetta all'azienda di essere conforme alle licenze software e che proibisca l'uso di software senza autorizzazione. L'uso di Software Libero semplifica enormemente l'adozione di questa regola in quanto la licenza GNU/GPL è unica a livello internazionale e fornisce le quattro libertà citate sopra.

- L'adozione di una procedura che applichi le disposizioni previste al controllo 10.5.
- L'adozione di un antivirus e delle relative procedure non è applicabile nell'ambito del Software Libero essendo quest'ultimo sostanzialmente non affetto da virus.
- Il responsabile del sistema deve condurre delle revisioni periodiche rispetto al software utilizzato per supportare i processi critici. L'uso di Software Libero garantisce una visione di lungo periodo per la crescita delle infrastrutture informatiche aziendali.
- La necessità di controllare i file provenienti da reti non fidate per cercare eventuali virus: se i file vengono salvati in formati proprietari (esempio .doc) o formati binari, non provenienti da reti fidate, le possibilità di infezione sono elevate. Nel caso si utilizzino formati aperti composti principalmente da testo (esempio XML, TXT, RTF), la presenza di codice malevolo è più difficile, anche se non impossibile.
- Un maggiore livello di affidabilità delle applicazioni scaricate dalla rete è fornito dal Software Libero, poiché le applicazioni e il codice inserito sono controllati nel tempo dalla comunità on line. Per aumentare il livello di sicurezza si potrebbe, ad esempio, ipotizzare un sistema di trusting rivolto all'affidabilità di siti di distribuzione del Software Libero noti e controllati dalla comunità on line.
- L'introduzione di un sistema di procedure e di responsabilità per tenere sotto controllo, nel tempo, le attività legate ai malfunzionamenti e alle infezioni (questa contromisura non è legata all'utilizzo del Software Libero).
- Introduzione di un piano che permetta la continuità del business e il recupero delle informazioni. Il salvataggio in formati aperti permette il recupero dei file che potranno essere difficilmente danneggiati o infettati.

Controllo n° 10.5– Sicurezza nello sviluppo e nelle attività di supporto

Il manager deve assicurare che le proposte di adeguamento dei sistemi informativi siano conformi alla politica della sicurezza informatica, in modo da non compromettere il sistema e l'operatività aziendale. L'uso di Software Libero fornisce ai responsabili la possibilità teorica di valutare in maggiore profondità i pro e i contro del sistema da introdurre in azienda.

Controllo n° 10.5.4– Canali occulti e codici trojan

IL FINE DELLA SEGUENTE TIPOLOGIA DI CONTROLLO È QUELLO DI PREVENIRE L'INTRODUZIONE DI CANALI OCCULTI, ATTRAVERSO CUI, AD ESEMPIO, VENGONO PRELEVATE INFORMAZIONI RISERVATE O INSERITI SOFTWARE MALEVOLI. DI SEGUITO ALCUNI CASI DI ATTIVITÀ DI CONTROLLO IMPLEMENTABILI.

- L'acquisto di programmi provenienti esclusivamente da fonti con "reputazioni positive" (sicure e certificate) rappresenta una premessa indispensabile per la sicurezza dei sistemi informativi. Molte aziende che producono software a codice chiuso sono state spesso accusate di utilizzare cavalli di troia, programmi che all'insaputa dell'utente raccolgono informazioni personali relative a preferenze dell'utente coperte dal diritto alla privacy (es. malware). Maggiori garanzie per l'utente provengono sia dalla disponibilità del codice sorgente, sia dalla possibilità di verificare che da quel codice si possa ottenere direttamente il programma eseguibile. Queste verifiche possono essere svolte dalla comunità del Software Libero, che fornisce ulteriori garanzie sull'assenza di cavalli di troia nel codice sorgente. Il sistema di trusting ha richiesto la partecipazione di migliaia di programmatori esperti in tutto il mondo e un lungo periodo di "gestazione", allo scopo di equilibrare il sistema. Si tratta di un processo in continua crescita.
- Come precedentemente affermato, per garantirsi la massima salvaguardia dei sistemi informativi, l'azienda dovrebbe sempre acquistare software con i codici sorgenti. In considerazione di questa esigenza, alcuni produttori di software proprietario, rendendosi conto del limite del loro modello che non prevede la diffusione del sorgente, stanno distribuendo i codici secondo la logica del "guardare ma non toccare". In altre parole, offrono all'acquirente la possibilità di leggere il codice sorgente ma non di poterlo in alcun modo modificare. Da ciò risulta evidente che la soluzione migliore per garantire un controllo più efficace sulla sicurezza del software rimane quella adottata dal Software Libero.
- Una delle più valide garanzie all'individuazione di eventuali bug è la possibilità di svolgere operazioni di testing non solo da parte del produttore, ma anche da parte della comunità di sviluppatori on line e degli utilizzatori. Per questa ragione i maggiori produttori di software proprietario hanno iniziato ad avvalersi della partecipazione di utilizzatori esterni, senza però fornire i codici sorgenti, ma soltanto l'applicativo compilato.



Perciò, nuovamente, il Software Libero rimane il più sicuro dato che, per sua natura, viene continuamente testato nella sua interezza da un'ampia comunità di utenti.

- Controllo del codice sorgente prima di rendere operativa l'applicazione software. Questa è un'operazione possibile, ma molto costosa nel caso di software proprietario. Non avere il codice sorgente porta a due conseguenze: fidarsi del produttore che ci vende l'applicazione oppure pagare un professionista esterno che verifichi la correttezza del codice. Nella maggior parte dei casi, il contratto di fornitura del produttore prevede che le modifiche apportate al codice sorgente, effettuate dal cliente o da terzi, facciano decadere l'accordo di manutenzione/assistenza, con ripercussioni negative sul business aziendale.
- Controllo nel tempo sia dell'accesso, che delle modifiche al codice una volta installato (vedi punto precedente).
- L'azienda deve utilizzare personale fidato sui sistemi critici. Dal punto di vista dell'eticità del modo di operare, esistono differenze sostanziali. Se il lavoro svolto dal personale è di proprietà esclusiva dell'impresa, il personale potrebbe risultare meno motivato a svolgere con massimo impegno il proprio lavoro. Se, invece, i risultati possono essere condivisi ed entrare a far parte del bagaglio professionale del lavoratore si otterranno probabilmente risultati migliori.

Controllo n° 10.5.5 – Sviluppo del software in outsourcing

NEL CASO IN CUI L'AZIENDA AFFIDI LO SVILUPPO DEL SOFTWARE A TERZI IN OUTSOURCING, L'AZIENDA DEVE COMUNQUE EFFETTUARE ALCUNI CONTROLLI.

- Nel caso del software proprietario, al momento della definizione delle licenze e quindi dei diritti di utilizzo, è necessario il coinvolgimento di esperti in campo legale che definiscano tali diritti in modo specifico in relazione alle caratteristiche peculiari dell'azienda cliente. Il Software Libero semplifica la gestione di queste problematiche, utilizzando il modello standard, descritto nella licenza GNU/GPL.
- Le aziende produttrici del software (sia Libero, che proprietario) devono certificare la qualità e l'accuratezza del lavoro svolto e i processi rispetto agli standard di riferimento (es. ISO 9001).
- L'azienda cliente può sostituire, in qualsiasi momento e senza problemi, il produttore di Software Libero poiché è già proprietaria dei diritti necessari. Invece, nel caso del software proprietario, il passaggio potrà avvenire forse solo dopo una lunga trattativa legale col vecchio produttore, che potrebbe avvalersi della facoltà di cedere i diritti sul software a terzi, senza alcuna autorizzazione da parte del cliente.

L'AZIENDA DEVE AVERE IL DIRITTO DI FARE AUDIT DI QUALITÀ SUL LAVORO SVOLTO DAL PRODUTTORE, ATTRAVERSO:

- accordi contrattuali per verificare la qualità del codice;
- testing delle applicazioni per verificare l'assenza di cavalli di troia.

Controllo n° 12.1.2.2 – Copyright del software

La fornitura del software proprietario è regolata dalle politiche commerciali delle aziende, che studiano apposite licenze di distribuzione ed utilizzo, volte a limitarne l'uso presso determinate macchine, determinati utenti, e la copia di backup per salvaguardare gli originali. Questa metodologia prevede un forte coinvolgimento di avvocati specializzati che preparano la licenza del software sulle indicazioni del cliente.

I diritti sul Software Libero sono regolamentati in maniera standard dalla licenza GNU/GPL, creata dalla Free Software Foundation, che ne tutela il rispetto e si fa carico delle spese legali. Questa licenza si basa sul principio opposto al copyright o "diritto d'autore". Si tratta del copyleft o "permesso d'autore", che promuove l'uso del software secondo un principio di permesso e non di limitazione.

Conclusioni

In sintesi, abbiamo portato evidenti punti a favore della tesi secondo la quale l'utilizzo del Software Libero implica un maggior livello di sicurezza delle informazioni. È stato messo in evidenza, infatti, come la sua adozione costituisca di per sé una facilitazione al rispetto di alcune delle indicazioni previste dalla ISO/BS17799. Nonostante queste considerazioni, non deve essere dimenticato che la sicurezza informatica deriva comunque dall'attuazione di un processo integrato e dinamico. Quest'ultimo, indipendentemente dal software impiegato, deve sempre essere impostato e gestito nell'azienda seguendo un approccio organico e pragmatico.

In ultima analisi, nella scelta fra Software Libero e proprietario, il fattore sicurezza diventa strategico, insieme al costo, alle prestazioni, alla compatibilità, alla facilità di utilizzo e di manutenzione. Tale scelta, tuttavia, non è necessariamente esclusiva: è possibile far convivere in azienda entrambe le tipologie di software usufruendo dei vantaggi di ciascun tipo, a seconda delle singole operazioni da effettuare.

Link utili

GNU/GPL:

<http://www.gnu.org/licenses/gpl.txt>

Sicurezza Informatica e Software Libero - Renzo Davoli:

http://www.yacme.com/eventi/2002_COMPA/abstract_davoli.html

ISO 17799:2000:

<http://www.bsi-global.com>

Geer, Pfleeger, Schneier, Quarterman, Metzger, Bace, Gutmann, "Cyber-insecurity: the cost of monopoly. (How the dominance of Microsoft's products poses a risk to security", Sep 2003:

<http://www.ccianet.org/papers/cyberinsecurity.pdf>

Free Software Foundation Europe:

<http://www.fsfeurope.org/index.it.html>

SINCERT

(Sistema Nazionale per l'Accreditamento degli Organismi di Certificazione):

www.sincert.it

Firenze Tecnologia – Azienda Speciale della Camera di Commercio:

www.firenzetecnologia.it