Security aziendale: aspetti di Computer Forensic

***Pasquale Soccio**, Dottore Commercialista, Revisore Contabile, CFE (Certified Fraud Esaminer), Senior Manager per la divisione Forensic Services di KPMG Audit S.p.A.*

***Rudi Triban**, CISM (Computer Information Security Manager), Senior Manager nella struttura di Information Risk Management di KPMG S.p.A.*

***Alessio De Paoli**, Project Leader in KPMG S.p.A.*

Dipendenza dai servizi IT

Si immagini che i servizi IT della propria azienda vengano improvvisamente a mancare a causa di un incidente di sicurezza e ci si ponga ora le seguenti domande:

- Quali processi aziendali sarebbero in grado di proseguire? Quelli maggiormente critici sarebbero tra questi?
- I dipendenti sarebbero ancora in grado di svolgere le proprie mansioni e con quale produttività?
- Quale sarebbe il costo che l'azienda dovrebbe accollarsi a causa di processi aziendali e personale parzialmente produttivo?

Le risposte a queste domande saranno note unicamente nel caso in cui sia stato portato a termine un progetto di *business continuity*; ad ogni modo, lo scopo di questo piccolo esercizio d'immaginazione, è attirare l'attenzione sulla sempre crescente dipendenza dai servizi IT delle aziende indipendentemente dal settore di appartenenza.

L'elevatissimo livello di penetrazione delle tecnologie ICT (*Information Communication Technology*) è documentato anche dalla recente indagine prodotta dall'ISTAT sull'uso di tali tecnologie nelle aziende italiane; l'indagine riporta che il 96,4% del campione d'aziende con 10-250 dipendenti e il totale delle aziende con oltre 250 dipendenti utilizzano personal computer e servizi IT per il proprio business.

Sensibilità sul tema sicurezza e compliance normativa

Sebbene la sensibilità sul tema sicurezza informatica sia cresciuta ed i sistemi di difesa si siano evoluti e diffusi negli anni, l'undicesimo sondaggio redatto congiuntamente da CSI e FBI[1] riporta che, nell'anno appena trascorso, le perdite stimate, legate ad incidenti di sicurezza informatica, sono state pari a $ 52 milioni e che le principali tipologie di incidenti che hanno causato tali perdite sono, nell'ordine:

- infezioni virali;
- accessi non autorizzati;
- furti di personal computer o altri dispositivi mobili;
- furti d'informazioni riservate.

La *compliance* rispetto a normative nazionali ed internazionali ha contribuito a dare un nuovo impulso al tema della sicurezza informatica. In ambito internazionale, si possono citare le seguenti normative: *Sarbanes-Oxley Act* per le aziende quotate o controllate SEC, quindi anche per società italiane, e Basilea II per gli istituti di credito.
In ambito nazionale, si può citare la normativa sulla *privacy* che è stata uno dei principali fattori nello sviluppo di strategie di sicurezza informatica. Inoltre è plausibile affermare che la *compliance* normativa continuerà ad essere prioritaria e ad attirare significativi investimenti anche nel corso degli anni a venire.

Sicurezza informatica

Come spesso si evidenzia, la sicurezza informatica non è un prodotto che si possa acquistare, togliere dalla confezione e mettere in funzione; dal sondaggio redatto da CSI-FBI risulta che il 98% ed il 97% delle aziende intervistate utilizzi, rispettivamente, *firewall* ed anti-virus mentre il 79%, 70% ed il 69% utilizzi, nell'ordine, software *anti-spyware*, controllo degli accessi centralizzato e sistemi di *intrusion prevention*. Queste percentuali confermano che, in generale, le soluzioni tecnologiche non siano sufficienti a scongiurare il rischio d'incidenti di sicurezza, ma possano solamente ridurne il rischio, minimizzando probabilità e impatto.

La sicurezza informatica si poggia su tre caratteristiche ben conosciute:

---

[1] Computer Security Institute e Federal Bureau of Investigation.

- confidenzialità, riservatezza delle informazioni e delle risorse;
- integrità, attendibilità delle informazioni e delle risorse;
- disponibilità, possibilità di accedere a informazioni e risorse.

Per garantire tali caratteristiche, è necessario impiegare la giusta miscela d'elementi tra i quali:

- procedure organizzative, composte da un insieme di norme, regole e comportamenti da attuare per portare a termine le attività di un determinato processo aziendale;
- politiche, che descrivano, a vari livelli, come le aziende intendano proteggere i loro asset informativi;
- soluzioni tecnologiche, in grado di implementare ed imporre il rispetto di politiche definite in precedenza.

Approccio Top-down

Secondo l'*IT Governance Institute*, alcune delle principali sfide che un'azienda deve affrontare sono:

- allineare la strategia IT con quella di business;
- far permeare strategie ed obiettivi ad ogni livello aziendale;
- fornire strutture organizzative che facilitino l'implementazione della strategia di business ed il conseguimento degli obiettivi;
- fare in modo che un framework di controllo IT sia adottato ed implementato;
- misurare le performance del sistema informativo.

Per far fronte alle problematiche d'implementazione di un sistema informativo in grado di supportare in modo efficace il proprio business rispondendo a specifici requisiti, si è sviluppata una disciplina che prende il nome di *IT Governance*; con questo termine si indica quella parte della Corporate Governance che si focalizza sui sistemi informativi, le relative performance ed i rischi connessi all'utilizzo di tali sistemi. L'IT Governance si pone come obiettivi quello di assicurare che gli investimenti IT generino valore per l'azienda oltre a gestire e mitigare i rischi associati all'impiego dell'IT stesso.
Grazie anche all'esperienza maturata da vari enti, sono stati definiti diversi framework che consentono di avere un corretto approccio ai temi dell'IT Governance, tra i più rinomati possiamo citare i seguenti:

- **ITIL** (*IT Infrastructure Library*), sviluppato dall'United Kingdom's Office of Government Commerce in collaborazione con l'IT Service Management Forum;
- **CobiT** (*Control Objectives for IT*), sviluppato dall'ITGI (IT Governance Institute);
- **ISO/IEC 27001** sviluppato dal BSI (British Standard Institution).

Confrontiamo ora i succitati framework per tassonomia, destinatari, focus, obiettivi, completezza e possibilità di certificazione.

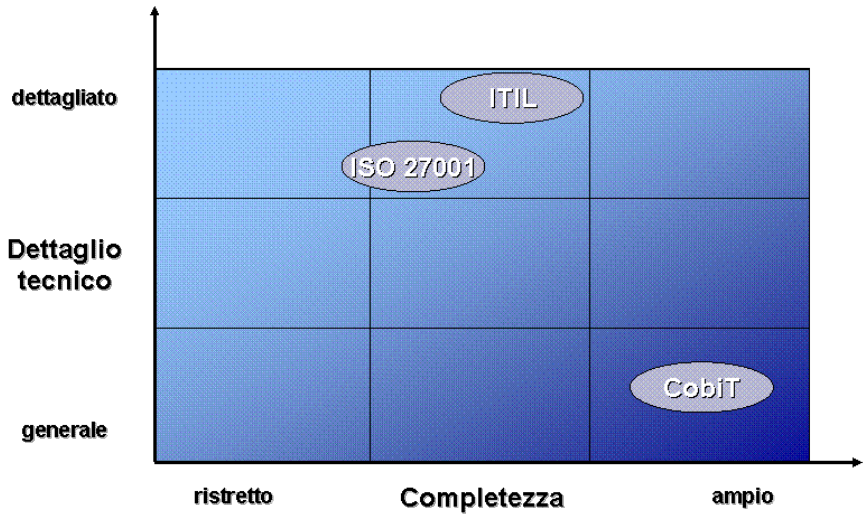
ITIL è una best practice per l'IT Service Management ed ha come destinatari i responsabili IT; il focus è quello della gestione dei servizi IT. L'obiettivo è quello di sviluppare un approccio *vendor indipendent* per la gestione dei servizi IT. La completezza è adeguata anche se si denotano carenze nell'IT management e governance. E' disponibile la certificazione del personale, ma non è possibile certificare l'azienda.

CobiT è una best practice per l'IT Governance ed ha come destinatari management, auditor e utenti di servizi IT; ha come focus qualsiasi tema correlato all'IT Governance. L'obiettivo è lo sviluppo di un modello che supporti la definizione, l'adeguamento e il monitoraggio del sistema di controllo IT e della IT Governance. In termini di completezza, comprende tutte le parti maggiormente significative dell'IT Management. E' una metodologia e non uno standard e, quindi, non consente la certificazione.

ISO/IEC 27001 è uno standard internazionale ed ha come destinatari i responsabili IT; il focus è quello della sicurezza. L'obiettivo è quello di fornire raccomandazioni sulla gestione della sicurezza informatica. Sono forniti controlli generici per la gestione dell'Information Security con l'imperativo della conformità alla legge. Essendo uno standard è disponibile una certificazione per le aziende e per il personale.

Volendo confrontare i tre framework in termini di dettaglio tecnico e completezza si può dire che:

- per completezza, la trattazione di CobiT è maggiormente ampia rispetto quella di ITIL e dell'ISO/IEC 27001 che risulta più ridotta;
- per dettaglio tecnico, ITIL e ISO/IEC 27001 sono comparabili mentre CobiT risulta meno dettagliato.



Inoltre, è corretto sottolineare che i tre framework non sono mutuamente esclusivi e non è strettamente necessario adottarne solamente uno ma bensì è possibile integrare questi ultimi secondo le esigenze e le peculiarità della specifica realtà.

Confronto tra i framework		
ITIL	CobiT	ISO17799
• Fornisce best practice per i processi IT ma non è forte in sicurezza. E' limitato nello sviluppo di sistemi e sicurezza	• Fornisce controlli IT e metriche IT ma non definisce il "COME". Inoltre non è forte nella parte di sicurezza	• Fornisce controlli di sicurezza, ma non definisce il "COME" (Process Flow)

Approccio Bottom-up

L'adozione e la corretta implementazione di uno dei suddetti framework consente di definire ed implementare procedure organizzative, politiche e soluzioni tecnologiche allineate con la strategia di business; tuttavia, le attività necessarie per la definizione e l'implementazione di un framework di questo tipo, sono articolate e richiedono una rilevante quantità di tempo.

Per identificare le aree di maggior scopertura in termini di sicurezza informatica e porre rimedio alle principali vulnerabilità, può essere opportuno prevedere di svolgere una valutazione del rischio dovuto all'utilizzo del sistema informativo con un approccio di tipo bottom-up; si partirà quindi da un'analisi dei sistemi e dell'infrastruttura di telecomunicazione impiegata per realizzare il sistema informativo valutandone le vulnerabilità alle quali sono soggetti i suoi componenti.

E' possibile ipotizzare lo svolgimento di una verifica di questo tipo nei seguenti scenari:

- prima dell'adozione di un framework di governance, per identificare e mitigare le vulnerabilità più rilevanti e supportare l'implementazione del framework;
- durante l'adozione e l'implementazione del framework, dal momento che, in tale periodo, l'azienda è ancora soggetta a rischi dovuti alle vulnerabilità del proprio sistema informativo;
- a seguito dell'implementazione del framework, per identificare ulteriori vulnerabilità o disallineamenti tra quanto definito dalle procedure e dalle politiche e quanto implementato nel sistema informativo;
- a seguito dell'implementazione del framework, come attività periodica finalizzata alla verifica del mantenimento di un adeguato livello di sicurezza.

Più in generale, si può affermare che un'attività di valutazione della sicurezza dovrebbe essere svolta ogniqualvolta un sistema sia esposto in un ambiente ostile, sia questo Internet, una Extranet o una Intranet.
Una valutazione dell'implementazione della sicurezza informatica e quindi delle vulnerabilità del sistema informativo può essere svolta utilizzando una delle seguenti attività:

- penetration test;
- security assessment.

Entrambi sono metodi per valutare la sicurezza di un sistema informativo o un suo sottoinsieme; la principale differenza è nell'approccio con il quale si raggiunge l'obiettivo.

Infatti:

- nel primo caso (penetration test), personale espressamente formato simula le azioni illecite che sarebbero intraprese da un malintenzionato che desideri entrare nel sistema informativo impiegando l'infrastruttura di telecomunicazione. E' possibile verificare i rischi dovuti a personale esterno o interno all'azienda, dotato di capacità tecniche più o meno elevate.
  Si può concordare di non fornire al personale incaricato informazioni sull'infrastruttura in analisi, cercando così di identificare le vulnerabilità che potrebbero essere sfruttate da un individuo che non conosca l'azienda ed il suo sistema informativo; oppure è possibile fornire informazioni generali che consentano di ridurre il tempo richiesto dall'attività e di

ottenere risultati di dettaglio. Infine, è possibile fornire informazioni di dettaglio che consentano di identificare in breve tempo gli obiettivi che possono essere maggiormente sensibili e soggetti ad attacchi mirati.
L'ambito considerato può essere l'infrastruttura informativa interna alla società, quindi sistemi e Intranet che collega le sedi, piuttosto che l'infrastruttura esterna alla società, sia questa una rete wireless, Extranet o i sistemi esposti su Internet. Infine si può concentrare l'attenzione dell'analisi su specifiche reti, sistemi o applicazioni considerate critiche.

- Nel secondo caso (security assessment), si valuta la sicurezza del sistema informativo senza simulare azioni illecite bensì svolgendo attività d'analisi che prevedono colloqui con i principali referenti al fine di comprendere la struttura e l'organizzazione del sistema informativo, oltre ai principali asset ed il loro valore. Successivamente, si verificherà la documentazione delle procedure e delle politiche predisposte dall'azienda che descrivono il sistema informativo e le regole che ne controllano il funzionamento. A completamento dell'assessment, si valuterà l'implementazione di procedure e politiche svolgendo un'analisi tecnica delle vulnerabilità del sistema informativo allo scopo di ottenere una fotografia oggettiva dello stato di salute di questo ultimo.

Differenti enti, non-profit e governativi, hanno definito metodologie che forniscono standard comuni e condivisi; oltre a tali metodologie ciascuna società di servizi che svolga attività di IT Security ha affinato le metodologie esistenti contribuendo con il lavoro del proprio personale e con l'esperienza maturata.
Le aziende che svolgono le suddette attività impiegano personale con background informatico, espressamente formato su tale tipologia di incarichi e che ha avuto modo di fare esperienza ed affinare le proprie capacità lavorando in appositi team. Inoltre, poiché durante tali incarichi è possibile che il personale abbia accesso ad informazioni riservate, si richiede che il personale impiegato aderisca ad un codice etico che fornisca ulteriori garanzie ai clienti.
Le carenze evidenziate dall'attività di assessment sono quindi riassunte in due distinti documenti:

- il primo è rivolto al management, ha lo scopo di consentire la corretta comprensione dei rischi ai quali è soggetta l'azienda e riassume le attività svolte, le conclusioni ed i suggerimenti sulle azioni richieste per minimizzare le criticità rilevate;

- il secondo è rivolto al personale IT, ha lo scopo di consentire la corretta comprensione di quanto evidenziato e contiene il dettaglio delle verifiche svolte, i risultati delle verifiche comprensivi di vulnerabilità, i rischi e l'impatto oltre a raccomandazioni tecniche per mitigare le vulnerabilità.

Conclusioni

L'accresciuta sensibilità sul tema della sicurezza informatica e le più recenti soluzioni tecnologiche non hanno ridotto l'impatto economico dovuto agli incidenti di sicurezza avvenuti nell'anno appena trascorso.

Per predisporre procedure organizzative, politiche e soluzioni tecnologiche in grado di rispondere ai requisiti di business definiti dall'azienda e garantire il livello di sicurezza desiderato, è necessario adottare ed implementare framework di governance per il sistema informativo; tuttavia, anche le migliori procedure, politiche o soluzioni tecnologiche non possono essere realmente efficaci qualora queste non siano state correttamente implementate. Quindi, per conoscere il livello d'implementazione della sicurezza nella propria azienda, è possibile svolgere un'attività di assessment in grado di verificare che:

- le principali tematiche siano state considerate nel governo del sistema informativo;
- le procedure organizzative siano state definite propriamente e ne sia controllato il continuo rispetto;
- le politiche siano state implementate correttamente;
- le soluzioni tecniche impiegate siano in grado di rispondere alle specifiche esigenze della propria azienda.

Sia per l'implementazione di un framework di governance sia per attività di assessment della sicurezza, è possibile avvalersi della competenza e dell'esperienza di aziende e/o società di consulenza che operano giornalmente su queste tematiche e sono in grado di supportare efficacemente un processo di riorganizzazione che tenda a migliorare la gestione del sistema informativo ed innalzare il livello di sicurezza.