

SICUREZZA FISICA E SICUREZZA LOGICA: I PARALLELISMI

COSTANTINO IMBRAUGLIO

I.Net S.p.A.

SOMMARIO

1. *Introduzione*
2. *Considerazioni sul mercato della sicurezza*
 - 2.1 Adeguamento all'ordinamento legislativo
 - 2.2 Protezione dell'immagine e della reputazione
 - 2.3 Continuità di servizio
 - 2.4 Fiducia dell'utente (cliente)
3. *Sicurezza a 360°*
 - 3.1 Strumenti logico-procedurali
 - 3.2 Strumenti tecnologici

1. INTRODUZIONE

Confrontandomi con svariati professionisti operanti nell'ambito della sicurezza fisica (chi scrive opera in ambito di sicurezza logica) ho potuto evidenziare una lunga serie di parallelismi tra i nostri due mondi.

Evidentemente le analogie non riguardano gli aspetti tecnologici legati alle soluzioni di sicurezza informatica, ma, cosa assai più importante, quelli legati all'approccio metodologico con cui va affrontato il tema della sicurezza informatica.

A supporto, è importante osservare come sempre più spesso accada che importanti aziende, banche ed organizzazioni, ritengano opportuno riportare ai responsabili della sicurezza fisica anche l'organizzazione delle soluzioni di sicurezza logica. Pertanto il mio obiettivo primario risulta quello di offrirvi un insieme di strumenti culturali e concettuali utili per meglio avvicinarvi al tema.

2. CONSIDERAZIONI SUL MERCATO DELLA SICUREZZA

E' opinione comune che la crescita del mercato della sicurezza informatica vada di pari passo con la proliferazione dei crimini informatici. Chi scrive non condivide questa analisi e individua altri *driver* di mercato:

- adeguamento all'ordinamento legislativo
- protezione dell'immagine e della reputazione
- continuità di servizio
- fiducia dell'utente (cliente)

2.1 Adeguamento all'ordinamento legislativo

In questi ultimi anni il legislatore ha introdotto diverse leggi in materia di tecnologie informatiche. Queste leggi rispondono a tre precise necessità:

- tutelare gli utenti
- regolare il mercato delle tecnologie informatiche
- definire, prevenire e punire i crimini informatici

Le aziende e le istituzioni hanno il dovere di adeguarsi alle nuove disposizioni, pena l'esposizione delle stesse e del relativo management a condizioni di illegalità. In tutto questo la sicurezza informatica riveste un ruolo centrale. Un effetto collaterale dell'attività legislativa in materia informatica è il successo e la diffusione di specifiche tecnologie a dispetto di altre.

Un impianto legislativo di così recente introduzione, e la relativa scarsità di giurisprudenza in materia, aprono interessanti opportunità di business nel campo della consulenza legale.

2.2 Protezione dell'immagine e della reputazione

L'adozione di INTERNET da parte delle aziende e delle istituzioni pone problemi di protezione dell'immagine e della reputazione. I crimini informatici rappresentano in questo senso un grave problema in quanto ledono sia l'immagine sia la reputazione delle entità che ne sono vittime, con una conseguente riduzione della fiducia da parte dell'utente (cliente). La sicurezza informatica risponde efficacemente a questo problema.

2.3 Continuità di servizio

Spesso si fa riferimento ad INTERNET come ad una *comunità virtuale*. In questo senso INTERNET sfugge alle comuni definizioni di *spazio e tempo*.

Non ha dunque importanza la localizzazione geografica del sistema informativo che eroga un determinato servizio; né hanno alcuna importanza le distinzioni tra giorni feriali e festivi ovvero tra orario di lavoro e non.

Un servizio in INTERNET deve pertanto essere disponibile su base 24x7. In questo senso la fallibilità delle componenti dei sistemi informativi rappresenta un grave problema e da essa dipendono le fortune di importanti mercati quali *disaster recovery, fault tolerance, monitoring & alerting, data backup, storage, cluster, ecc.* Tali mercati rientrano nell'ambito della sicurezza informatica che dunque risponde efficacemente alla richiesta di continuità di servizio.

2.4 Fiducia dell'utente (cliente)

La fiducia dell'utente (cliente) è un elemento cruciale per il successo di qualsiasi iniziativa commerciale. Ciò è particolarmente vero in INTERNET dove viene meno il contatto umano e dove tutte le transazioni (pagamenti, contratti, ecc.) avvengono su una base squisitamente virtuale. La sicurezza informatica risponde alla domanda di fiducia garantendo la riservatezza, la autenticità e, più in generale, il buon esito delle transazioni.

3. SICUREZZA A 360°

La sicurezza informatica non è perseguibile solo attraverso la tecnologia. In realtà i *fattori abilitanti* sono tre:

- **Consapevolezza e formazione** – Non è possibile garantire la sicurezza di un sistema informativo prescindendo dal fattore umano. Sia gli utenti del sistema informativo sia i suoi amministratori devono infatti considerare gli aspetti legati alla sicurezza non già come degli ostacoli, bensì come una necessità e, al contempo, una opportunità. E' dunque necessario sviluppare nelle persone una adeguata consapevolezza. Ciò è possibile attraverso la comunicazione e la formazione.

- **Procedure** – La messa in sicurezza di un sistema informativo è possibile solo attraverso la definizione e la applicazione di un insieme di procedure operative (*security policies, incident handling procedures, ecc.*). Tali procedure regolano sia le attività legate alla tecnologia (scelta e configurazione degli apparati, ecc.) sia i modelli comportamentali degli individui.
- **Tecnologia** – Naturalmente la tecnologia è ciò che rende possibile la implementazione di gran parte delle soluzioni di sicurezza informatica.

D'altra parte, se l'approccio al problema della messa in sicurezza dei sistemi informativi non può essere solo di tipo tecnologico, ne consegue evidentemente che gli strumenti da utilizzare non saranno solo le tecnologie. In particolare è possibile individuare due distinti insiemi di strumenti:

- strumenti logico-procedurali
- strumenti tecnologici

3.1 Strumenti logico-procedurali

Questi strumenti rispondono alla necessità di formalizzare le procedure operative e creare consapevolezza negli individui e possono essere così riassunti:

- Asset Analysis
- Risk Management
- Vulnerability Assessment & Penetration Test
- Security Policy
- Incident Handling Procedures
- Certificazioni
- Consulenza Legale
- Polizza Assicurativa
- Seminari Informativi e Corsi di Security Awareness

Asset Analysis

La definizione e l'applicazione delle politiche di sicurezza non può prescindere da una conoscenza completa del sistema informativo e degli *asset* che lo compongono. Le attività di *asset analysis* sono funzionali a questo obiettivo e vengono svolte con l'ausilio di strumenti automatici. Esse, come già anticipato, si prefiggono l'obiettivo di raccogliere informazioni dettagliate circa la struttura del sistema informativo e gli *asset* che lo compongono. Gli *asset* sono: risorse di rete, risorse di calcolo, componenti applicative e risorse dati. Evidentemente, si tratta di una

attività che interessa esclusivamente le imprese di medie e grandi dimensioni, ossia quelle che dispongono di sistemi informativi di grandi dimensioni e, magari, distribuiti geograficamente sul territorio (banche, assicurazioni, grande distribuzione, ecc.).

Risk Management

Gli obiettivi del *risk management* sono molteplici:

- individuazione delle aree di rischio che possono minacciare il sistema informativo e i singoli asset che lo compongono
- classificazione degli asset in funzione della criticità in termini di rischio ad essi associato
- discriminazione tra rischio accettabile e non

Questa attività non può essere svolta in assenza di una precedente attività di *asset analysis*. Quest'ultima è dunque propedeutica alla *risk analysis*. In generale le attività di *risk management* possono essere svolte con l'ausilio di strumenti automatici in ausilio alle più tradizionali tecniche basate sulle interviste e la compilazione di moduli. Inoltre, tali attività devono essere considerate alla stregua di un processo aziendale con caratteristiche di ciclicità (ossia vanno ripetute periodicamente per tutta la vita del sistema informativo).

Vulnerability Assessment & Penetration Test

Per ogni singolo *asset* che compone il sistema informativo è importante conoscere le vulnerabilità a cui è soggetto e le possibili soluzioni per eliminarle. Le attività di *vulnerability assessment* sono funzionali a questo obiettivo. E' altresì importante conoscere la effettiva sfruttabilità di una vulnerabilità da parte di un malintenzionato. Le attività di *penetration test* sono funzionali a questo obiettivo.

Vulnerability Assessment

Come già evidenziato, l'obiettivo delle attività di *vulnerability assessment* è quello di individuare le vulnerabilità che affliggono i singoli *asset* costituenti un sistema informativo e le possibili soluzioni per eliminarle. A tal proposito è importante sottolineare che un sistema informativo è una realtà dinamica, ovvero un sistema la cui struttura cam-

bia nel tempo (sia dal punto di vista dei servizi offerti, sia da quello delle componenti tecnologiche che lo costituiscono). Inoltre non passa giorno senza che vengano scoperte nuove vulnerabilità. Pertanto le attività di *vulnerability assessment* devono essere ripetute periodicamente. Le attività di *vulnerability assessment* vengono normalmente svolte con l'ausilio di strumenti automatici.

Penetration Test

Non tutte le vulnerabilità sono facilmente sfruttabili per condurre attacchi e non tutti gli attacchi possono portare ad una grave compromissione del sistema informativo. Per comprendere se una condizione di vulnerabilità è effettivamente sfruttabile, è opportuno condurre un *penetration test*. Si tratta di un'attività che viene condotta direttamente e manualmente da parte di personale altamente qualificato e che abbia dimestichezza con le tecniche di attacco. In generale un *penetration test* dovrebbe essere autorizzato direttamente dal *management* e condotto da entità esterne all'azienda, possibilmente tenendone all'oscuro gli amministratori di sistema. L'attività di *vulnerability assessment* è propedeutica ai *penetration test*.

Security Policy

Il termine *security policy* ha più di un significato. In generale le *policies* rappresentano le direttive del *management* per la realizzazione di un programma per la messa in sicurezza dei sistemi informativi, la formalizzazione degli obiettivi del programma stesso e l'attribuzione delle responsabilità personali. D'altra parte il termine *security policy* è applicato anche per descrivere specifici aspetti di configurazione delle componenti tecnologiche. Più in generale la *security policy* è un documento teso a formalizzare in senso lato sia le direttive che le procedure tese al perseguimento di un adeguato livello di sicurezza.

Incident Handling Procedures

Con questo termine si fa riferimento a quei documenti che formalizzano le attività da intraprendere in caso di incidente e le relative responsabilità personali. Generalmente le *Incident Handling Procedures* fanno parte delle *security policies*, ma possono essere

formalizzate anche in assenza di queste ultime e dunque vengono considerate come una attività a sé stante. La necessità di formalizzare le procedure di gestione degli incidenti informatici deriva dal fatto che in assenza di tali procedure, le azioni conseguenti ad un incidente possono portare alla involontaria cancellazione delle informazioni necessarie a ricostruire l'incidente stesso oltre ad eventuali ritardi nel ripristino dei servizi.

Certificazioni

Dopo aver provveduto alla messa in sicurezza di un sistema informativo (sia attraverso l'impiego di prodotti e servizi consulenziali, sia attraverso l'impiego di quelli tecnologici), può essere opportuno certificare l'aderenza ad un insieme di standard riconosciuti a livello internazionale (ISO17799 e BS7799). Si tratta dunque di una attività di certificazione che dovrebbe essere propedeutica alla sottoscrizione di eventuali polizze assicurative.

Consulenza Legale

Come abbiamo già avuto modo di osservare, l'impianto legislativo in materia di sicurezza informatica è di recente introduzione. Conseguentemente è assai scarsa la giurisprudenza in materia. Questa situazione apre interessanti opportunità di business nel campo della consulenza legale. Poche sono infatti le aziende o le istituzioni che dispongano di un adeguato know-how in materia di legislazione informatica.

Polizza Assicurativa

Consapevolezza degli utenti, procedure operative e tecnologia non garantiscono la sicurezza assoluta. Inoltre, le attività di *risk management* possono portare al riconoscimento di aree di rischio accettabili e che dunque non vengono affrontate né con strumenti organizzativi né con quelli tecnologici. Per colmare questo *gap* è possibile ricorrere ad opportune polizze assicurative. Naturalmente la possibilità di sottoscrivere simili polizze dovrebbe essere vincolata al raggiungimento di determinati standard qualitativi certificabili da organismi indipendenti (ISO e BS). Il meccanismo della polizza renderebbe possibile l'offerta di SLA pari al 100%.

Seminari Informativi e Corsi di Security Awareness

Come abbiamo già avuto modo di sottolineare non è possibile garantire la sicurezza di un sistema informativo prescindendo dal fattore umano. Sia gli utenti del sistema informativo sia i suoi amministratori devono infatti considerare gli aspetti legati alla sicurezza non già come degli ostacoli, bensì come una necessità e, al contempo, una opportunità. E' dunque necessario sviluppare nelle persone un'adeguata consapevolezza. Ciò è possibile attraverso la comunicazione e la formazione.

3.2 Strumenti tecnologici

La tecnologia mette a disposizione delle aziende e delle pubbliche amministrazioni numerosi strumenti per la messa in sicurezza dei sistemi informativi:

- Firewall
- Antivirus
- IDS (Intrusion Detection System)
- VPN (Virtual Private Network)
- Strong Authentication
- System Hardening
- Applications & Infrastructures Monitoring & Allerting
- Data Backup
- Fault Tolerance
- Disaster Recovery

Non è questa la sede adatta per descrivere le tecnologie in questione. Ciò che in realtà è importante sottolineare è il fatto che un adeguato livello di sicurezza può essere raggiunto soltanto impiegandone il maggior numero possibile.

D'altra parte si tratta di tecnologie complesse che richiedono elevati livelli di competenza per poter essere efficacemente dispiegate. In questo senso le aziende e le pubbliche amministrazioni dovrebbero seriamente considerare l'opportunità di rivolgersi a un partner di fiducia che possa accompagnarli nella messa in sicurezza dei sistemi informativi vuoi con l'ausilio di strumenti logico-procedurali, vuoi con l'ausilio di quelli tecnologici.