

UN APPROCCIO METODOLOGICO EXTENDED SECURITY

FLORIANO CAPRIO
Italdata S.p.A.

INTRODUZIONE

Capita spesso che alcune aree di interesse ed alcune tecnologie, presenti già da tempo sul mercato, vengano portate alla ribalta da una serie di circostanze più o meno casuali; la sicurezza e sicuramente una di queste aree. Bisogna stare attenti però a non lasciarsi trasportare dalle mode, che sembrano ridurre il tutto alla scelta di un firewall piuttosto che un altro, ma, come in tutte le attività, usare un approccio analitico e strutturato e l'unico modo che alla lunga può dare validi risultati

Motivi per i quali, ultimamente, la sicurezza informatica sta riscontrando una maggiore attenzione sono molteplici e variano dalla necessità ed opportunità di molte aziende di collegare le proprie reti aziendali con Internet fino alla recente introduzione della firma digitale considerata valida, a norma di legge, per autenticare documenti sia nella Pubblica Amministrazione sia nell'ambito privato. Inoltre, gli scenari informatici di questi ultimi anni sono sicuramente evoluti e risultano sempre più complessi, le informazioni gestite nei centri di calcolo aumentano il loro volume di giorno in giorno e risultano sempre più critiche, se non assolutamente indispensabili, per moltissimi processi aziendali. Il concetto stesso di azienda risulta essere più evanescente e sempre più difficile delineare dei confini entro i quali descrivere e limitare i sistemi aziendali, ormai organizzati con strutture distribuite sul territorio e collegate tra di loro mediante linee più o meno dedicate. Lo sviluppo tecnologico ha sicuramente offerto nuove opportunità e funzionalità nel soddisfare nel migliore dei modi le esigenze dei diversi utenti ma, contemporaneamente, l'utilizzo di tecnologie non sufficientemente mature e conosciute, ha introdotto nuove vulnerabilità all'interno dei sistemi informatici. A questo scenario va inoltre aggiunto che in Italia la necessità di "sicurezza" non deriva da esigenze interne ma anche dall'obbligo di ri-

spettare la legge n. 678 del 31 dicembre 1996 e successive modifiche, sulla "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", .

SICUREZZA LOGICA E FISICA

Vediamo di esprimere un approccio alla sicurezza informatica che tenga conto dei tre aspetti fondamentali per la sicurezza delle informazioni:

la *Riservatezza*, l'*Integrità* e la *Disponibilità*, in linea con quanto stabilito nelle specifiche standard ITSEC (*Information Technology Security Evaluation Criteria*) e CC (*Common Criteria*).

Per *riservatezza* si intende la prevenzione dalla divulgazione non autorizzata delle informazioni e quindi la *Riservatezza* di una informazione deve garantire sia un accesso controllato che una divulgazione limitata.

Per *integrità* si intende la prevenzione da una modifica non autorizzata delle informazioni e quindi l'*Integrità* di una informazione deve garantire l'accuratezza di formato (integrità fisica) e di contenuto (integrità semantica) ed inoltre l'autenticità e il non ripudio delle fonti di origine dove, per non ripudio, si intende l'impossibilità, per il creatore di un dato o l'autore di una transazione, di negarne la paternità.

Infine, per *disponibilità* si intende la prevenzione da un trattenimento non autorizzato delle informazioni e/o risorse e quindi la *Disponibilità* di una informazione deve garantire un breve tempo di accesso ed un servizio costante delle risorse.

Su questi tre fattori di sicurezza si sviluppano i criteri di analisi, valutazione ed implementazione che possono incidere sia sul sistema informativo, sia sulla struttura organizzativa, sia sulla logistica e gli aspetti fisici di una organizzazione.

Questi tre aspetti concorrono congiuntamente e pariteticamente alla definizione e

pianificazione sia della sicurezza fisica che della sicurezza logica.

La sicurezza fisica comprende le misure di protezione atte a garantire la sicurezza delle sedi e delle apparecchiature di elaborazione, la disponibilità di risorse alternative sia di elaborazione che di archiviazione e a disporre i piani di ripristino del servizio in casi di emergenza.

Le misure di sicurezza fisica sono propedeutiche a quelle di sicurezza logica in quanto non ha senso proteggere dati e programmi da accessi non autorizzati se non è garantita l'affidabilità hardware e dell'ambiente.

La sicurezza logica è l'insieme di misure volte a garantire l'integrità delle informazioni, l'affidabilità dei dati, la segretezza degli stessi (vista come controllo dell'accesso al sistema) e la continuità del servizio in-

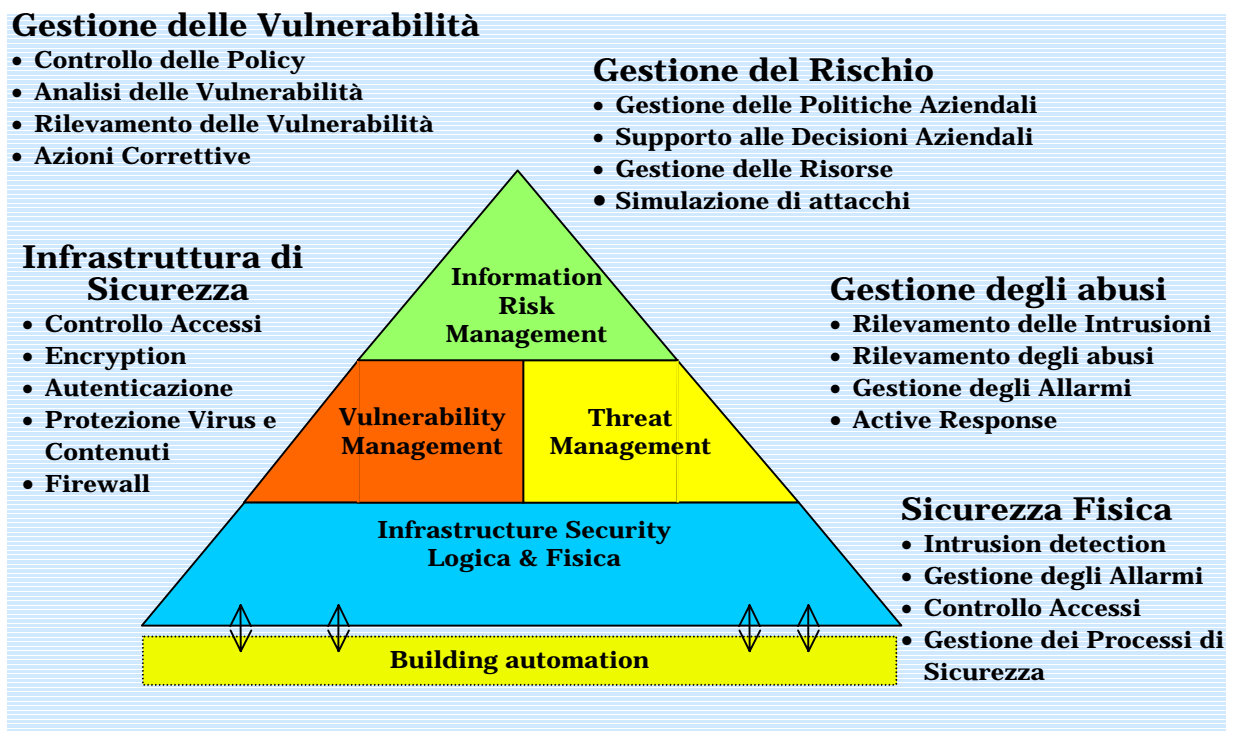
formativo. La protezione logica può venire assicurata mediante misure protettive sia hardware che software.

L'approccio metodologico globale consiste nel pianificare, costruire, e gestire allo stesso livello e con strumenti altamente integrati sia la sicurezza fisica che la sicurezza logica introducendo un *nuovo* concetto di **Building Automation** che completa pienamente il concetto di sicurezza.

Questo nuovo approccio di **Extended Security** abbraccia tutte le problematiche di una realtà complessa come quella bancaria che va dalla necessità di proteggere fisicamente le singole filiali da intrusioni e rapine, a quella di proteggere i dati e garantire la continuità e la sicurezza dei servizi.

In fig. 1 si riporta una schema riassuntivo del nuovo scenario dell'*Extended Security*

FIG. 1



SERVIZI DELL'EXTENDED SECURITY

Il nuovo approccio alla sicurezza e la visione globale che esso induce crea l'esigenza di un'infrastruttura tale che consenta di gestire e mantenere in modo omogeneo e centralizzato il controllo della sicurezza.

Il *Security Operation Center* (SOC) è l'insieme delle risorse tecniche specialistiche, delle norme/procedure comportamentali e delle piattaforme *hardware* e *software* dedicate alla gestione del sistema di sicurezza.

La gestione della sicurezza della rete, dei sistemi e del palazzo, è per una banca è un'attività molto dispendiosa in termini di tempo e risorse da dedicare: a seconda delle dimensioni dell'impresa occorre infatti monitorare di continuo l'attività di uno o più *firewall*, di sistemi *intrusion detection*, di sistemi *antivirus*, di allarmi sui sistemi, di impianti di accesso fisico, di impianti di antincendio.

Questo lavoro complesso richiede personale altamente specializzato e costantemente aggiornato sulle più recenti tecniche di intrusione, sugli ultimi sviluppi del software e sulle tecniche più adatte di autodifesa da applicare in ogni situazione. Ecco, quindi, perché Siemens attraverso la propria offerta consente di realizzare un *Security Operation Center* (SOC) integrato in grado di essere il centro di gestione e monitoraggio dell'intera infrastruttura di sicurezza.

I processi di gestione operativa che governano il SOC sono tali da monitorare costantemente il rischio residuo e garantiscono la protezione da intrusioni anche attraverso *Security Assessment* periodici.

La fig. 2 rappresenta schematicamente la struttura di un SOC, mentre in fig. 3 è riportato uno schema base di funzionamento del SOC in un tipico *work flow* lavorativo.

FIG. 2

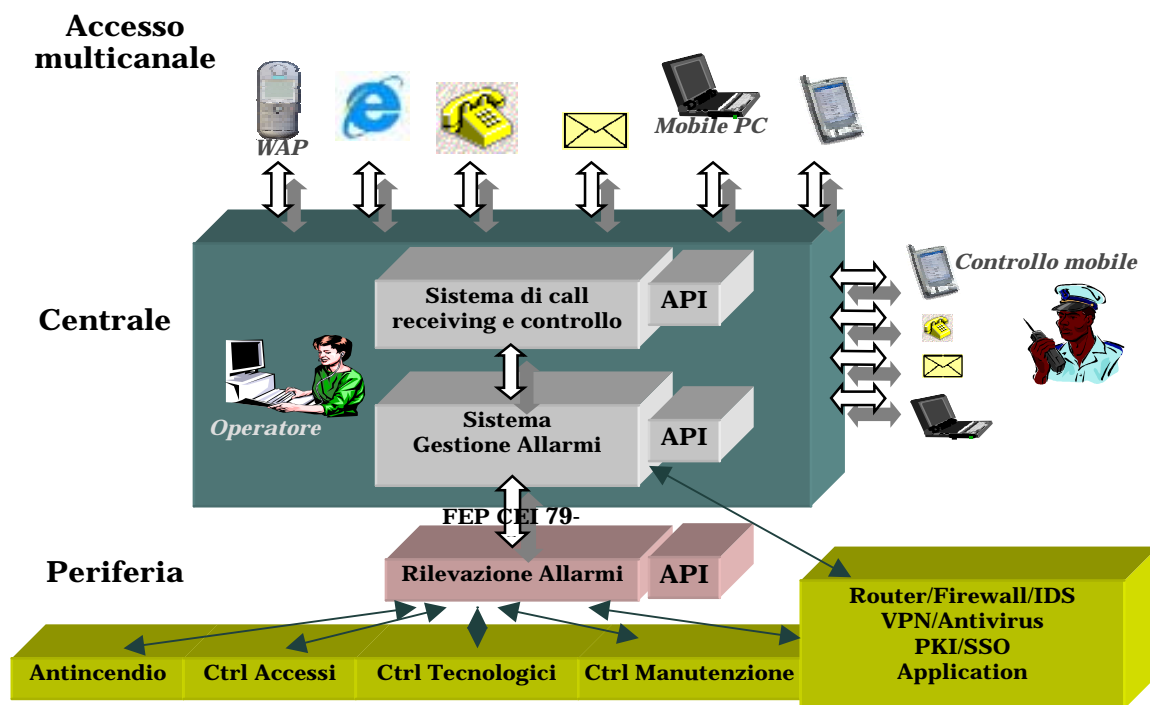


FIG. 3



CONCLUSIONI

Questo proposto è un approccio metodologico integrato alla sicurezza estesa in ambito bancario vista come un insieme di procedure, tecnologie e servizi.

La sicurezza non è sicuramente confinata nella scelta di un Firewall piuttosto che nel-

la installazione di una porta blindata e, anche se molto spesso non si è culturalmente preparati per capirlo, se realmente si ha questa esigenza, bisogna avviare un processo di analisi, valutazione, ecc. che possa portare ad un risultato concreto e dimostrabile in una visione globale e corredarlo di appositi servizi di gestione a supporto.