

Sicurezza Fisica e Sicurezza Logica: due culture a confronto

Sicurezza: La vera sfida dell'organizzazione efficace

Alessandro Lega, CPP
Senior Partner Insigna Group



Infosecurity 2003
Milano 13 febbraio

Uno sguardo al Security Management

- Comprende tutte quelle discipline che permettono ad un'azienda di prevenire rischi di tipo non competitivo, contrastare iniziative aggressive e ripristinare i danni derivanti da azioni illecite, iniziative dolose (ed anche da processi errati)
- Può esistere solo se è conseguenza di una scelta organizzativa emanata dal top management e se viene condivisa dal senior management

Aspetti organizzativi del Security Management

- Il collocamento organizzativo della funzione Security dipende dalla missione che le viene affidata (alta o bassa visibilità – ruolo strategico/tattico/operativo)
- La struttura (ed il budget) normalmente riflette le scelte organizzative e la missione assegnata/accettata
- Il Security Manager dovrebbe saper operare come un leader del team di Security, senza necessariamente essere uno specialista
- Il suo ruolo dovrebbe essere quello di *allenatore* dell'intera squadra (non solo della sua)

Aree comuni fra Physical Security e ICT Security

- Necessità di individuare le vulnerabilità e di valutarne il rischio
- Concetto di protezione perimetrale (fisica o logica)
- Utilizzo di soluzioni di protezione *concentrica*
- Applicazione del principio *Deter, Detect, Delay, Deny*
- Ambiente fisico contrapposto a *spazio virtuale*
- Concetto di *log*, inteso come documentazione di eventi
- Effetto *badge*: accesso concesso o negato con riferimento al possesso di un documento/titolo personale (*no visual check*)
- Concetto di *User ID* e *password* per accreditare i soggetti
- Possibili soluzioni simili con tecnologie *biometriche*
- Modalità di intrusione messe in atto: visite preliminari per capire l'ambiente, per poi mettere in atto la vera intrusione

Diversità fra Physical Security e ICT Security

- Diverse le motivazioni che muovono gli aggressori (da quelle criminali a quelle ideologiche)
- Diverso concetto di proprietà dei beni e delle idee (da oggetti fisici a oggetti virtuali), dal domicilio fisico allo spazio virtuale
- Diversa la propensione degli utenti nel proteggersi
- Diverse le capacità tecniche richieste per *aggredire*
- Le competenze necessarie per mettere in atto le protezioni
- Propagazione degli effetti (fattore moltiplicatore della rete)
- Il ruolo dei *complici* (da consapevoli ad inconsapevoli)
- La diversa percezione di reato (commesso dal criminale o subito dalla vittima)

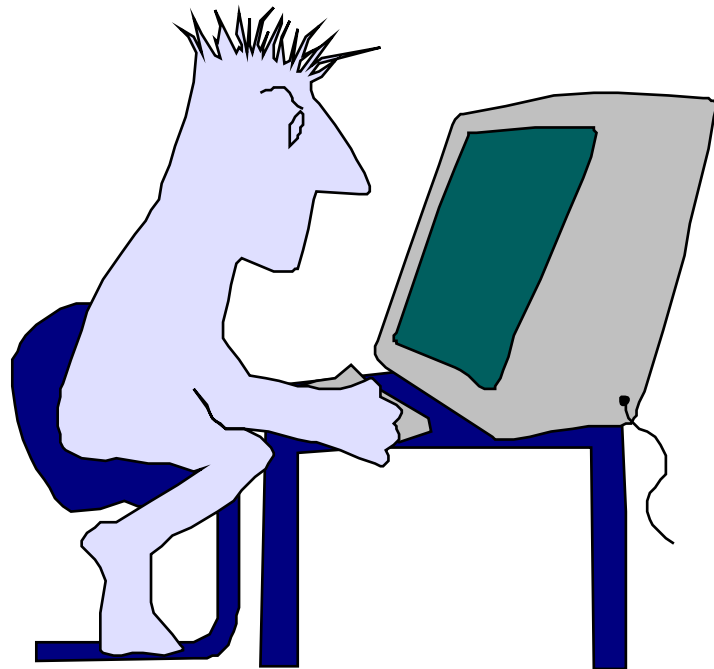
I punti deboli della Sicurezza fisica

- E' fortemente dipendente dalla conoscenza delle regole interne
- Se vuole essere efficace richiede il pieno coinvolgimento dell'intera popolazione in azienda
- Difficoltà di individuare ed ostacolare l'effetto del *triangolo* Motivazione – Desiderio – Opportunità
- Spesso percepita come un ostacolo alla operatività aziendale
- Ancora considerata solo come un centro di costo

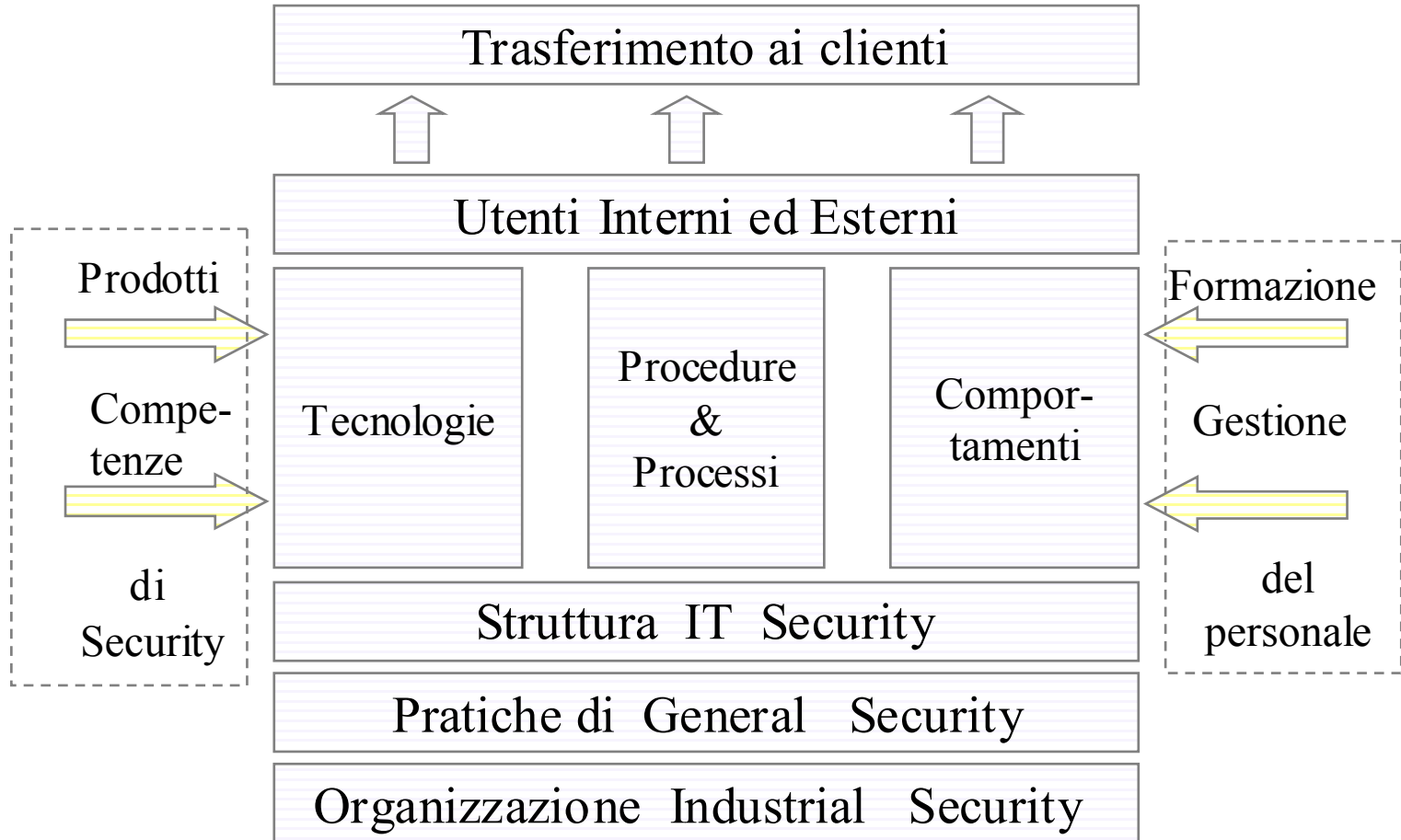


I punti deboli della ICT Security in Azienda

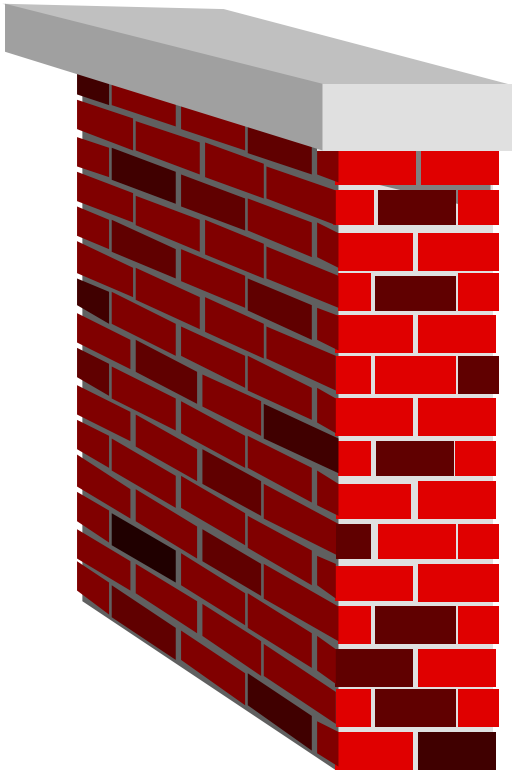
- E' fortemente dipendente dai vari comportamenti individuali
- Quasi sempre le soluzioni di protezione sono note solo agli specialisti
- La validità di una protezione è di limitata durata, se non viene frequentemente aggiornata
- Gli specialisti che se ne occupano hanno spesso un atteggiamento di indifferenza nei confronti degli utenti
- Viene dedicato un tempo limitato per far evolvere l'utente medio



Aspetti organizzativi comuni



Le tecnologie



- Quelle di tipo passivo si limitano ad un effetto deterrente
- Anche per l'ICT si applicano modalità di rilevamento delle intrusioni
- Molte similitudini nell'utilizzo di strumenti investigativi
- Non esiste tecnologia in grado di garantire sicurezza assoluta
- Specifiche peculiarità per la identificazione dei rischi, ma alcune aree sono in comune
- Possono essere acquisite sul mercato, pur con una minima personalizzazione

Le procedure ed i processi Security



- In entrambi i casi devono riflettere le effettive necessità interne
- Richiedono un'approfondita conoscenza della cultura aziendale
- Possono essere utili anche esperienze esterne, non è possibile “copiare” da altri
- Dopo la loro messa a punto devono essere disponibili per coloro che devono applicarle/i
- Devono essere mantenute aggiornate/i

I comportamenti



- Dovranno essere indicati quelli attesi
- Devono essere resi noti tramite una comunicazione efficace
- E' una specifica responsabilità del management
- La consulenza esterna può essere utile, ma è richiesto un diretto coinvolgimento interno
- L'importanza dell'esempio che *viene dall'alto*
- Devono intervenire azioni correttive nei confronti di comportamenti errati

Conclusioni per ricercare una organizzazione di Security efficace

- Meglio se riusciamo a far convivere le due responsabilità sotto un unico *ombrello*
- Sono necessarie specializzazioni diverse che però non sono incompatibili
- Le tre fasi di *prevenzione, contrasto, ripristino* possono avere tempificazioni diverse anche se ognuna, nella maggioranza dei casi, può influenzare le altre
- La fase di pianificazione di *budget* potrebbe vederle ancora unite. Comunque ciascuna non deve sottrarre risorse all'altra

Grazie per la vostra attenzione,



Alessandro Lega, CPP

alessandro_lega@tin.it

Senior Partner INSIGNA Security srl

<http://www.insigna-group.com>