IL COSTO DEL MANCATO INVESTIMENTO IN SICUREZZA

Dato per assodato che la sicurezza assoluta non esiste, una corretta strategia per l'enterprise security prevede un processo ciclico che alterna: vulnerability assessment, analisi del rischio, definizione di un piano di contenimento del rischio realizzazione di tale piano. Le tecnologie che andranno implementate sono di volta in volta dipendenti dalle condizioni al contorno, oltre che dalle esigenze delle specifiche imprese.

Il problema è tipicamente fare i conti con il budget a disposizione, che troppo spesso risulta insufficiente a realizzare il sistema di sicurezza idealmente definito dal piano. Eppure, Gartner sostiene che le spese per la sicurezza, a livello mondiale, stanno crescendo a un ritmo medio (CAGR) del 28%, rispetto a un budget IT nel suo complesso sostanzialmente piatto: una situazione insostenibile destinata a esplodere già nei prossimi anni. Già oggi, come per tutti i comparti di spesa aziendale, è diventata rigida la richiesta di una misura del ROI per qualsiasi investimento. Ma se è difficile calcolare il ritorno di un investimento infrastrutturale, qual è tipicamente quello in Information e Communication Technology, come è possibile quantificare il valore di una soluzione di sicurezza, quando, se tutto va bene, non succede niente?

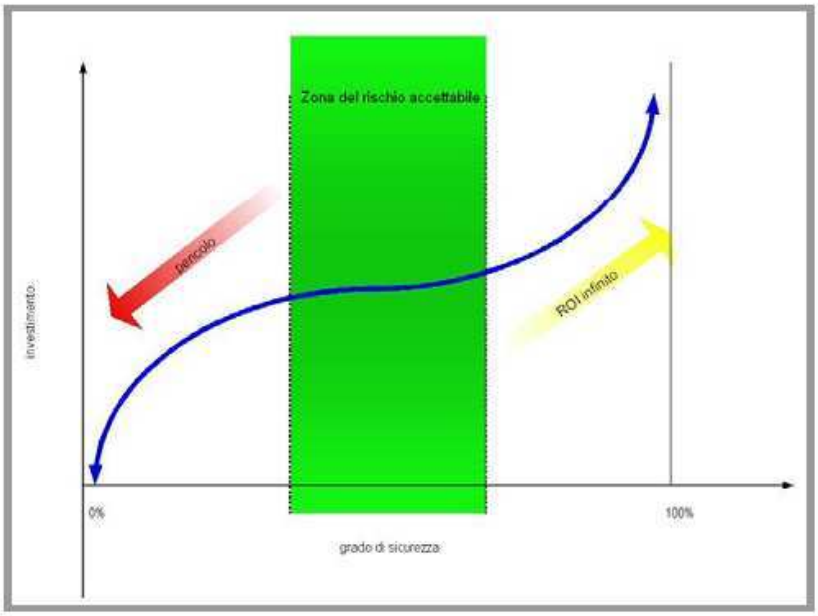
La risposta è in realtà banale nella forma, un po' meno nella pratica. Chiaramente il problema se lo sono già posto i vendor del settore che da sempre hanno trovato le loro difficoltà a vendere i sistemi di protezione contro qualcosa di impalpabile come le minacce Internet. Come si accennava precedentemente, il valore di un sistema di sicurezza deve essere correlato al livello di rischio accettabile per un'impresa. Dove per rischio s'intende il danno economico che si avrebbe in caso di un attacco andato a buon fine, di un disservizio totale o parziale e così via. Il primo passo da compiere per il calcolo del ROI coincide con quello che è necessario per definire che sistema di sicurezza implementare: effettuare un'analisi delle vulnerabilità cui è esposta l'azienda e del livello di rischio relativo.

Non si tratta di un'operazione banale, tanto che è codificata in precisi standard ISO, meglio noti con la sigla BS7799. Per effettuare tale operazione è bene affidarsi a una società indipendente, ovviamente dotata delle opportune certificazioni, poiché non di rado in questa fase si fanno vere e proprie scoperte: per esempio, applicazioni o servizi ritenuti poco importanti, se confrontati con l'impatto reale sul business, possono risultare molto più critici di quanto pensato fino a quel momento. Condotta con tutti i crismi, tale analisi produce una documentazione oggettiva che, ricordando che questa fase deve essere ciclicamente ripercorsa, sarà molto utile per valutazioni successive.

Per valutare il rischio correttamente, quindi correlando alle dinamiche e logiche di business, è necessario coinvolgere il management aziendale a vari livelli. Questo è il principale vantaggio di tutta l'operazione, nonché la vera chiave di volta per il calcolo del ROI. Infatti, costretti a riflettere sulle ripercussioni di un attacco informatico, i manager svilupperanno quella

sensibilità verso i temi della sicurezza che per anni è stata il cruccio degli addetti ai lavori.

Il risk assessment, inoltre, produce un numero, cioè il valore del danno che si potrebbe creare in funzione del grado di vulnerabilità reale determinato dall'attuale sistema di sicurezza. Un dato facilmente comprensibile anche dal consiglio di amministrazione, tanto più quando è certificato da una società indipendente.



Rappresentazione grafica degli investimenti in sicurezza

Una volta stabilito quale deve essere il piano di contenimento del rischio, quindi quali misure devono essere implementate per ridurre le vulnerabilità e aumentare il grado di protezione, è necessario realizzare un security plan dettagliato. Questo deve considerare l'evoluzione nel tempo e conteggiare il TCO (Total Cost of Ownership) di tutte le soluzioni. È importante osservare che in molti casi il prezzo di acquisto di un prodotto è solo il primo elemento di spesa: in ambito sicurezza, non vanno trascurati i costi dei servizi di aggiornamento, senza i quali le soluzioni diventano presto (praticamente immediatamente) obsolete e inutili.

Un piano della sicurezza ben dettagliato è utile per confrontarlo con un modello del rischio. Mettendo in una sorta di matrice la spesa necessaria per "tappare una potenziale falla" e il rischio economico che la "falla" lasciata aperta potrebbe causare (eventualmente ipotizzando più eventi correlati a tale vulnerabilità trascurata), si ottiene uno strumento di immediato raffronto. All'atto pratico, una soluzione di sicurezza deve raggiungere almeno uno dei seguenti obiettivi per poter dimostrare di avere un ROI sostenibile: ridurrei costi correnti, ridurre i costi futuri, ridurre il rischio finanziario, aumentare la produttività, aumentare il fatturato.

Molto spesso ci sono benefici intangibili che è difficile calcolare, ma è bene non esagerare nel cercare di aumentare il valore del sistema di sicurezza al solo fine di convincere il management a investire. Anche perché importanti argomenti sono stati forniti dal Testo Unico sulla privacy, che, unitamente alle precedenti disposizioni legislative, sta imponendo l'adozione di misure minime, spingendo molte aziende a effettuare analisi di vulnerability assessment con ottimi risultati di sensibilizzazione.