Return on Security Investment

Un tema centrale per comprendere le prospettive della Sicurezza ICT in Italia e nel mondo, è relativo alla comprensione delle logiche di investimento aziendale, al modo in cui si valuta il ritorno (ROI) dei progetti e alle difficoltà di ricondurre gli investimenti in sicurezza a tali logiche, ovvero alla difficoltà di farne un calcolo matematico. Nella maggior parte dei casi essa viene assimilata ad un costo senza alcun ritorno e quindi, nella normale logica del Business, da evitare o ridurre il più possibile. Capire questi aspetti è importante per molti motivi. E' importante per il responsabile della Sicurezza ICT (il cosidetto CISO - Chief Security Information Officer) affinché possa definire delle strategie ed obiettivi coerenti e quindi sostenibili e raggiungibili; è importante per il Top Management affinché possa superare i limiti degli approcci attuali e, infine, è importante per i revisori, i sindaci, gli analisti, il pubblico e il mercato, che spesso vedono o subiscono i nefasti effetti della mancanza di sicurezza e dovrebbero agire o influire per cambiare lo status quo.

"ROSI for an enterprise is an important measure in today's cyberworld, in which hackers, computer viruses and cyberterrorists are making headlines" – ISACA

Figura 1: Return On Security Investment[1]

In questi ultimi anni osserviamo un ampio ridisegno dei sistemi informativi dovuto all'adozione di nuovi modelli di business o di go to market. Le aziende rinnovano i canali e sfruttando la tecnologia mobile, social, big data, cloud fanno utili in nuovi modi. Si parla di trasformazione digitale. In questi casi tali servizi dovrebbero essere sicuri per definizione: ad esempio sarebbe inammissibile, oggi, rendere disponibile una Payment App insicura. In tali casi il ROI viene calcolato sull'investimento complessivo e il costo della sicurezza concorre solamente a definire il montante dei costi. In pratica non viene fatta l'analisi del ROI della nuova App senza la sicurezza.

Il problema del ROSI si pone quindi nei casi in cui l'investimento in sicurezza non può essere direttamente relazionato alla trasformazione digitale. Ma questi casi sono numerosi e importanti. Il problema è che gli attuali sistemi sono ampiamente insicuri, essendo stati creati in un periodo di forte e convulsa innovazione tecnologica e nel quale il pericolo cyber non era ancora reale. Infine a ben vedere anche la trasformazione digitale non avviene nel vuoto ma i nuovi servizi si appoggiano agli attuali sistemi informativi e li accrescono; non sarebbe saggio costruire su delle scarse fondamenta, ma è sicuramente difficile attribuire al prossimo singolo progetto di trasformazione digitale tutto il costo necessario a sanare la scarsa qualità dell'intero sistema informativo.

[1] Da G41 Return on Security Investment (ROSI) Effective 1 May 2010

Fatta questa premessa, ed escluso il fortunato caso della trasformazione digitale, proviamo ad approfondire le logiche di calcolo del ROSI.

Quando si parla di investimenti ci si pone il problema di calcolarne il ritorno per poter valutare le diverse alternative. In linea di principio conviene scegliere la cosa che ha un maggiore e più rapido ritorno econonico. Una delle formule più utilizzate è quella del Return on Investment (ROI) che compara il margine con il costo necessario per realizzarlo e quindi sottrae i costi dal ricavo e divide il risultato per il costo. L'imprenditore o il manager possono quindi più facilmente decidere se effettuare una scelta A oppure B, se rinnovare la catena di montaggio oppure se realizzare il nuovo sito di eCommerce.

$$ROI = \frac{\text{Expected Return} - \text{Cost of Investment}}{\text{Cost of Investment}}$$

Figura 2: formula del ROI

Purtroppo nello specifico caso degli investimenti in Sicurezza ICT la difficoltà sta nel valorizzare i ricavi. Installare una soluzione di data loss prevention che beneficio porterà? Sicuramente non un ricavo ma semmai la riduzione di un possibile danno. Qui le cose si complicano perché è difficile calcolare tre fattori chiave: il valore del danno possibile, la probabilità di incorrervi senza la soluzione di data loss prevention e la probabilità residua ovvero quella di incorrervi ugualmente nonostante la nuova tecnologia.

Nell'esperienza degli esperti interpellati, nel 2009 (all'epoca del primo Security Summit) le aziende non calcolavano il ROI della Sicurezza, non lo facevano nel 2012 (primo Rapporto Clusit) e non lo fanno tuttora. Tutti però concordano che sarebbe utile disporre di un metodo per poterlo fare e in Internet e presso le associazioni professionali si trovano numerosi paper e guidelines. Tra gli altri segnalo una nostra pubblicazione in italiano (AIEA, Clusit, Deloitte, Ernst & Young, KPMG, Oracle e PricewaterhouseCoopers – http://rosi.clusit.it) del 2011 che ha avuto il merito di evidenziare le difficoltà e di dare qualche suggerimento comportamentale al CISO[2].

Che criterio usa allora l'azienda per decidere gli investimenti in sicurezza? Ed è utile insistere nel tentativo di calcolare il ROSI?

[2] ROSI Return on Security Investments: un approccio pratico. Come ottenere Commitment sulla Security http://rosi.clusit.it/views/Homepage.html

Le motivazioni per le quali un'azienda investe in Sicurezza ICT si possono ricondurre ad un mix di queste quattro:

1. Ridurre il Rischio
2. Garantire la Compliance
3. Proteggere il Brand
4. Ridurre i costi dei controlli

Ridurre il Rischio

Si investe per ridurre la possibilità o le conseguenze di un attacco o incidente informatico avendo la consapevolezza del valore per se e per gli altri dei beni da custodire. Quindi un investimento oculato dovrebbe essere preceduto da un'analisi del rischio, una classificazione dei dati e dall'inventario degli asset[3], tutte attività sicuramente utili ma che richiedono un salto culturale e un investimento non semplice da attuare.

In azienda i dirigenti più interessati da questo aspetto dovrebbero essere il Chief Financial Officer (CFO – direttore finanziario), il Chief Risk Manager (CRM – responsabile dei rischi) e i vari direttori di funzione, ognuno per la propria area (CxO).

Alcuni metodi per il calcolo del ROSI considerano che gli incidenti informatici siano numerosi ma nel contempo non producano singolarmente molti danni e quindi tali metodi possono permettersi di moltiplicare la probabilità di incidente con il danno causato con e senza l'investimento di sicurezza. Purtroppo essi prestano il fianco al grande evento nefasto e poco probabile[4] che produce un danno multimilionario e che è in grado di compromettere la sussistenza stessa dell'azienda[5].

Inoltre il concetto di probabilità va bene quando ci si rapporta a certe categorie di eventi, come per esempio alla probabilità di fare ambo giocando al Lotto, ma presenta dei seri limiti quando dall'altra parte c'è un attaccante che mette in gioco la sua intelligenza contro le nostre contromisure. In tale situazione sarebbe utile valutare la probabilità di essere violati anche in funzione (dello skill

[3] I primi 100 giorni del Responsabile della Sicurezza delle Informazioni; http://100giorni.clusit.it/views/Homepage.html

[4] Una lettura interessante è quella del "Il cigno nero. Come l'improbabile governa la nostra vita" di Taleb Nassim N.

[5] Numerosi degli attacchi presentati nel Rapporto Clusit degli anni passati sono costati più di 100 milioni di euro solo come danno diretto. Quale azienda italiana è in grado di permetterseli? Inoltre tendono ad essere pubblici solo quelli che compromettono i diritti di terzi (ad esempio i cittadini dei quali viene trafugata la carta di credito), mentre la perdita di segreti commerciali a favore della concorrenza (ad esempio la lista dei clienti più profittevoli) e quelli industriali (progetti, piani, altri segreti) rimangono più facilmente sconosciuti e quindi non sono stati pubblicati nel Rapporto Clusit.

dell'attaccante e) del suo impegno contro di noi visto come una funzione dell'appetibilità dei nostri asset[6].

Normalmente chi investe in sicurezza per ridurre il rischio lo fa senza appoggiarsi ad un'analisi formale dello stesso, senza alcuna data classification e senza un inventario degli asset, con la sola marginale eccezione di qualche istituto bancario che piano piano vi ci si avvicina. Inoltre si tende a proteggere la parte più esposta ad internet dell'infrastruttura IT, in quanto questi incidenti sono molto visibili e più facilmente comprensibili dal management e quindi ricevono più facilmente le risorse necessarie, ma ciò lascia l'azienda vulnerabile agli attacchi che partono (o che transitano) dall'interno.

Garantire la Compliance

Si investe in specifiche misure di sicurezza per obblighi imposti da terzi. Questi possono essere gli Stati tramite le leggi, varie autorità locali o internazionali come quella per la Protezione dei Dati Personali (la Privacy), l'Unione Europea tramite la definizione di regolamenti e direttive da declinare localmente in modi differenti, oppure tra soggetti economici collegati con regole concordate o forzate commercialmente (ad esempio quelle sulla protezione delle carte di credito). Inoltre possono essere obblighi auto-imposti, per esempio dalla capogruppo oppure per scelta di business per ottenere alcuni vantaggi come quelli legati ad una certificazione ISO. Limitando queste considerazioni al primo caso (obblighi esterni), si osservano due cose: la prima è che normalmente le compliance tendono a definire regole per proteggere i diritti di terzi che interagiscono con l'azienda. E' il caso della Privacy che definisce come proteggere i dati personali dei propri clienti, delle regole sull'accesso ai sistemi di controllo delle infrastrutture critiche per evitare danni ai cittadini e sulla qualità dei crediti della banca per proteggere il sistema economico intero. Questo implica che la compliance non si preoccupa della salute di un'azienda in quanto tale, ma che si limita a proteggere i soggetti con i quali l'azienda interagisce e quindi è normale che alcuni aspetti di sicurezza molto importanti siano lasciati alla discrezionalità del management, che deve o dovrebbe preoccuparsene (per ridurre il rischio).

La seconda cosa osservata è che fortunatamente le compliance stanno lentamente migliorando nella loro formulazione grazie ad un certo grado di concertazione effettuato tramite le consultazioni pubbliche, i forum industriali, i gruppi di interesse e il riferimento alle best practice internazionali. Compliance scritte all'inizio degli anni 2000 includevano prescrizioni del tipo "La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito" mentre quelle più moderne possono recitare "progettando, sviluppando e manutenendo i servizi di pagamento via internet, i fornitori (...) dovrebbero prestare attenzione speciale ad una adeguata separazione (dei compiti) degli ambienti IT di sviluppo, test e produzione e ad una precisa implementazione del principio del minimo privilegio alla base di una robusta gestione delle identità e dell'accesso"[7].

---

[6] Ringrazio Sergio Fumagalli – Zeropiù e Andrea Longhi - ConsAL per i loro commenti e rimando ad una interessante lettura di Bruce Schneier http://bit.ly/ROSIBRUCE

[7] http://www.ecb.europa.eu/pub/pdf/other/recommendationsforthesecurityofinternetpaymentsen.pdf?d9d3c572d5484d0767b39d8d84c7d2c9

Queste nuove formulazioni possono consentire ad una azienda di trasformare un obbligo in opportunità, ovvero di poter utilizzare, con un minimo sforzo aggiuntivo, le stesse misure adottate per obblighi di compliance (diritti di terzi) con quelle adottabili per considerazioni di rischio operativo (diritti propri). Una ricerca realizzata l'anno scorso dal PMI-NIC (Project Management Institute, Northern Italy Chapter) e da Clusit, già riportata nel Rapporto Clusit 2014 indicava che il 48% degli investimenti in Sicurezza IT[8] viene realizzato per motivazioni di compliance e che il 47,7% per motivazioni di rischio. Questo indica che si fa ancora molto sulla compliance e che vale la pena approfittarne.

Il calcolo del ROSI nella compliance potrebbe interessare al Chief Executive Officer (CEO – direttore generale) e al Chief Compliance Manager (CCM) e dovrebbe considerare gli effetti negativi della mancanza di compliance (valore economico delle multe comminabili, effetti personali sugli individui apicali, effetti sull'azienda in forza della responsabilità delle persone giuridiche per il decreto legislativo 231/01 ed infine sull'immagine aziendale) ed eventualmente anche quelli positivi diretti (poter dichiarare il rispetto di una compliance aumenta la fiducia dei propri interlocutori e l'immagine aziendale). Essere certificati ISO 27001 può costituire un vantaggio competitivo e ridurre i costi derivanti dagli audit interni e/o di terze parti.

Negli anni passati, in Italia, numerosi investimenti in sicurezza ICT sono stati guidati dall'operosa produzione dell'Autorità Garante dei Dati Personali di Provvedimenti o Linee Guida generali (ad esempio Amministratori di Sistema[9]) o di industry (ad esempio FSE[10] e Tracciamento operazioni bancarie[11]). Negli ultimi due anni sono state dedicate molte attenzioni da parte delle banche al quindicesimo aggiornamento della circolare 263 della Banca d'Italia che recita nella premessa "A tal proposito, le banche valutano l'opportunità di avvalersi degli standard e best practices definiti a livello internazionale in materia di governo, gestione, sicurezza e controllo del sistema informativo." Il settore finanziario sarà in futuro ancora oggetto di accresciute compliances generali o specifiche che avranno un forte impatto sui sistemi informativi. Per tutti i settori industriali, invece, siamo in attesa del nuovo Regolamento europeo sulla Privacy che, tra altre importanti cose, nella corrente formulazione, pone molta enfasi sulla Privacy by Design e sulla notifica obbligatoria agli interessati dei data breach (fughe di dati). Infine i grandi temi legati alla mobilità (e ai pagamenti in mobilità), al (public) cloud, ai big data, ai social e all'internet delle cose, saranno affrontati dal legislatore e dalle aziende con nuove compliance e con nuove regole contrattuali. La compliance accompagnerà per molti anni gli investimenti IT nell'industria.

[8] in Italia, secondo i 286 project manager certificati che hanno risposto. Risposta singola.

[9] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1577499

[10] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1634116 e http://fse.clusit.it/views/Homepage.html

[11] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1813953

Proteggere il Brand

Si investe in certe misure di sicurezza per proteggere il marchio, la fama della propria azienda e aumentare o mantenere la fiducia che i consumatori o i clienti hanno verso la stessa. Le aziende italiane, secondo l'esperienza diretta e la sopra citata ricerca PMI-NIC / Clusit, non sono quasi interessate a proteggere il proprio brand tramite la sicurezza ICT. Il nesso tra le due cose non è ancora stato da loro pienamente compreso. E' però probabile che la situazione in futuro cambi e la cosa possa interessare sia al Chief Executive Officer (CEO – direttore generale) sia al Chief Marketing Officer (CMO) per via degli effetti della nuova Privacy europea menzionata in precedenza, unitamente ad un generale aumento delle capacità relazionali globali dell'azienda (per via di un incremento dell'eCommerce e dell'uso del canale Social-Mobile per attrarre clienti). In diversi settori industriali, in presenza di una riduzione costante della marginalità, è infatti necessario creare i presupposti di fiducia nel brand per poter attuare strategie di upsell e cosell. Un eventuale calcolo del ROSI dovrebbe riuscire a dare un valore economico al danno di immagine a fronte di un incidente di sicurezza ICT considerando la probabilità che tale incidente diventi di pubblico dominio e stimando la reazione (spontanea o meno[12]) dei consumatori e di altri attori su Internet.

1. Ognuna delle quattro motivazioni all'investimento presenta caratteristiche e problematiche diverse di calcolo del ROSI. Raccogliere e definire gli elementi per il calcolo è molto complesso.

2. Ogni motivazione interessa un diverso insieme di attori aziendali e ciò complica l'approvazione degli investimenti perchè non c'è un singolo budget dal quale attingere per i progetti più impegnativi

3. Fortunatamente, soprattutto grazie ad una compliance più matura, le misure di sicurezza stanno convergendo portando valore in più punti

Ridurre i costi dei controlli

In quest'ultima categoria si includono quegli investimenti in sicurezza tesi a ridurre il costo dei controlli o per aumentare la qualità e l'efficacia degli stessi. Si pensi per esempio alla produzione manuale di report di audit in cui devono essere censiti tutti gli utenti abilitati ad accedere ad un certo insieme di sistemi informativi verificandone nel dettaglio i privilegi e le incompatibilità (segregation of duties). Quanto lavoro si è disposti a pagare per ottenere una certa qualità dei controlli?
Per il primo aspetto, ovvero quello della riduzione del costo, il ROSI è facile da calcolare utilizzando la classica definizione del ROI (Figura 2: formula del ROI); per il secondo, le cose si complicano nuovamente.

Valutare il risparmio di costo è interessante per chi normalmente lo deve sostenere e in quest'area di solito si pensa al Chief Information Officer (CIO – il responsabile dei sistemi informativi) o al CEO (Direttore Generale) e al CFO (Direttore Finanziario). Quest'ultimo in particolare quando, come capita, i controlli siano relativi all'area contabile e amministrativa sulla quale insistono alcune compliance (per le aziende quotate in borsa) e dove maggiore è il rischio di frode legata direttamente al denaro. Esiste purtroppo, nella grande maggioranza dei casi, una netta sproporzione tra il costo del progetto (licenze software, forza lavoro e manutenzione) e il suo ritorno economico e raramente un'azienda trova conveniente investire solamente per questa motivazione.

[12] Un modello completo dovrebbe tenere conto anche dei comportamenti dei concorrenti e delle autorità.

Considerazioni finali sul ROSI

Vista la complessità del calcolo, è difficile investire in Sicurezza ICT sulla base di sole considerazioni economiche come talvolta viene chiesto dal Top Management. Le aziende che investono in sicurezza lo fanno per un accresciuta consapevolezza di quello che può avvenire senza sicurezza. In questi anni la crescente interconnessione dei sistemi informativi, la scomparsa del perimetro aziendale e la consumerizzazione hanno sottoposto le nostre aziende a nuove sfide di sicurezza. Purtroppo a volte esse sono state danneggiate senza neanche essersene accorte, come quando hanno subito un furto di segreti e di proprietà intellettuale. Ormai nessuno dovrebbe più credere “a me non capita”, “i miei dati non sono interessanti per un attaccante”.

Utilizzando un approccio pratico, invece che calcolare matematicamente il ROSI dei singoli investimenti in sicurezza sarebbe meglio definire dei criteri per l’ottimizzazione nel lungo periodo, per capire quali sono le aree maggiormente vulnerabili e dove destinare un budget che deve essere sicuramente incrementato. Ovvero trovare dei criteri per allocare in maniera intelligente le risorse disponibili nel breve e nel medio-lungo periodo.

E’ molto importante capire che bisogna implementare un ecosistema organizzativo e tecnologico in grado di proteggere l'azienda dagli attacchi e dagli incidenti che possono comprometterne la disponibilità (abbastanza riconosciuti perchè sono molto visibili, ad esempio un distributed denial of service), ma anche l’integrità (una frode condotta utlizzando in maniera illecita un’applicazione) e la riservatezza (la più difficile da scoprire; data breach, furto di segreti industriali) e che le misure per proteggere e monitorare le risorse vanno distribuite in profondità, dal perimetro di rete, ai dispositivi, i server, lo storage, le basi dati e i file system, i sistemi operativi, le App e le applicazioni...

Non credo che le aziende agiscano per motivazioni esclusivamente razionali ed esclusivamente economiche. In realtà il comportamento del soggetto collettivo è frutto dell’interazione di molteplici interessi e convinzioni da parte dei dipendenti e di altri stakeholder. E’ quindi necessario continuare a parlare del ROSI[13]: il ritorno sarà che l’azienda potrà continuare ad operare nel mercato, rispettata e attenta ad impedire che altri possano danneggiare le terze parti collegate.

L’autore
Alessandro Vallega
Security Business Development, Oracle Europe South
Chairman di Oracle Community for Security
Clusit Board of Directors
alessandro.vallega@oracle.com

[13] http://bit.ly/ROSIALE