Abbandonare la sicurezza basata sull'analisi dei rischi?

Il titolo di questo articolo è volutamente provocatorio, ma chi si trova a progettare, gestire, giustificare, verificare e cercare le risorse per implementare un sistema di sicurezza informatica, spesso non riesce ad ottenere dall'analisi dei rischi le risposte ed il sostegno che vorrebbe. Nella comunità degli specialisti di sicurezza informatica vi è una discussione (vedi ad esempio [1] e [2]) sulla fondatezza del modello teorico dell'analisi dei rischi che tutti ben conosciamo, per lo sviluppo di sistemi di sicurezza informatica.

Chiariamo subito che, malgrado la provocazione del titolo, vogliamo discutere in questa sede dei problemi e di cosa non funziona in pratica nel modello di sicurezza basata sull'analisi dei rischi e cosa si può provare a fare per risolvere i problemi.

Come ben sappiamo la sicurezza informatica non è una scienza esatta: ad esempio è impossibile dimostrare matematicamente la sicurezza già in modelli teorici complessi. Questo non è altro che una riaffermazione del fatto che la sicurezza assoluta non esiste. Anche a livello teorico dobbiamo sostituire ad *essere sicuro* i concetti di *rischio* e *fiducia (trust)*.

Ma quello che ci interessa in questa sede non è l'aspetto teorico dei modelli di sicurezza, ma l'implementazione pratica in azienda. Spesso in una azienda medio-grande vi è un responsabile della sicurezza dei sistemi informativi (detto Chief Information Security Officer, CISO)[1] che deve fare delle scelte per la sicurezza dei sistemi e convincere l'amministratore delegato o il management della necessità di investire alle volte ingenti fondi in sistemi di sicurezza informatica. Ovviamente gli investimenti in sistemi di sicurezza devono essere inferiori al valore di quello che si vuole proteggere, o meglio al rischio del danno che ne potrebbe venire in assenza del sistema di protezione. Abbiamo

1 Questo ruolo è spesso svolto dal responsabile dei sistemi informativi o da altra persona in aggiunta ai suoi compiti principali.

quindi un bene da difendere, il rischio del verificarsi di un danno ed il costo di un sistema di protezione che riduce il rischio.

In aziende quali quelle dei settori bancari, finanziari ed assicurativi, la valutazione e la gestione dei rischi sono il business dell'azienda o parte degli strumenti cardini del suo funzionamento. In questi casi in azienda sono presenti tutti i processi per l'analisi e la valutazione dei rischi in modo tradizionale, completo ed approfondito.

Consideriamo qui però una qualsiasi altra azienda, ad esempio manifatturiera, che non faccia della gestione del rischio il proprio business. In questo caso è molto comune che il management preferisca accettare il rischio in un settore che non sia il core business, piuttosto che spendere ulteriori somme per ridurlo. Spesso le richieste del CISO sono percepite dal management come un modo per il CISO di aumentare la propria importanza in azienda ed al contempo come un modo per ridurre le proprie responsabilità scaricandole ad esempio sul fornitore del sistema di sicurezza. Inoltre il management spesso percepisce i sistemi di sicurezza come dei vincoli alla produttività dell'azienda, di cui farebbe ben volentieri a meno.

Quali procedure dovrebbe seguire il CISO per svolgere la sua attività? Il modello generalmente accettato dice che il CISO deve svolgere una dettagliata analisi dei rischi per individuare esattamente cosa deve essere protetto ed avere argomenti oggettivi ed economici da presentare al management. Un problema frequente è che un'analisi dei rischi dettagliata è spesso troppo costosa da realizzare ed il management può sempre decidere di accettare il rischio piuttosto che svolgere l'analisi e/o implementare nuovi sistemi di sicurezza.

Vediamo subito come rendere più pratica l'analisi dei rischi. Come prima cosa, uno dei concetti fondamentali dell'analisi dei rischi è la *probabilità* del verificarsi di un evento dannoso. Per alcune situazioni molto comuni, possiamo semplificare l'approccio ad esempio perché possiamo parlare di *certezza* piuttosto che di probabilità dell'evento dannoso.

Ad esempio, qualunque sistema che crei, gestisca, riceva messaggi di posta elettronica deve essere dotato di anti-virus e anti-spam. Analogamente sistemi desk-top devono essere dotati di anti-virus, ed i server o le LAN aziendali devono essere protette da un firewall per la connessione ad Internet. Queste misure di protezione sono necessarie per:

1. la certezza dell'evento dannoso in loro assenza
2. Best-Practice di sicurezza aziendale
3. leggi (quali ad esempio il Dlg 196/03 sulla Privacy), normative, certificazioni eccetera.

L'analisi dei rischi non è quindi necessaria per giustificare tali misure di protezione, anche se può sempre essere utilizzata per svolgere una valutazione economica dettagliata sui costi/benefici.

L'approccio di un CISO alla valutazione di un sistema e dei suoi aspetti di sicurezza può quindi seguire una traccia alternativa.

Come sempre per prima cosa bisogna fare, ad alto livello, un censimento dei sistemi (HW/SW), dei dati e dei flussi di comunicazione. Senza questa base di informazioni nulla è possibile.

Una volta ottenute queste informazioni è già possibile verificare se le misure di sicurezza richieste da Best-Practice, leggi, norme certificazioni eccetera sono presenti o sono da implementare. Queste sono ovviamente le misure di base che devono comunque essere presenti.

Fatto ciò, per proseguire nell'analisi bisogna valutare sempre ad alto livello le minacce e le vulnerabilità dei sistemi. Anche questa parte dell'analisi è tradizionale.

Il passo successivo è invece quello che si discosta dal processo tradizionale. Invece di andare a stimare la probabilità di avvenimento, il danno economico eccetera, con le informazioni acquisite sinora è possibile capire, se vogliamo intuitivamente, quali sono i principali problemi di sicurezza.

Questo deve essere fatto in relazione all'azienda ed al suo business, e per questo è necessario ben comprendere i processi aziendali ed il loro significato ed importanza. E' chiaro che l'efficacia di una tale valutazione dipende dall'esperienza e capacità di chi la svolge, visto che non è guidata da processi automatici o procedure codificate.

In questa fase può aiutare l'adozione di uno strumento quale un *Capability Maturity Model* (CMM)[2] che permette anche di visualizzare facilmente al management le aree ove è necessario un intervento più o meno urgente.

I principi che possono essere adottati ed usati presso il management come motivazione per la realizzazione dei sistemi si sicurezza sono:

1. *Due Diligence*: un sistema informativo di cui sono note le vulnerabilità e le minacce e per il quale sono state adottate misure di sicurezza omogenee nei vari settori, riduce in maniera globale i rischi sia di danni diretti all'azienda, che di danni ai clienti o danni di immagine e la responsabilità legale degli amministratori

2. *Compliance*: l'azienda ha degli obblighi di adozione di misure di sicurezza dei sistemi informativi; questi obblighi provengono da leggi, normative anche internazionali, certificazioni eccetera, la non adozione di queste misure di sicurezza può arrecare gravi danni all'azienda

3. *Enablement*: l'adottare e seguire le Best-Practice del proprio settore aziendale è sempre visto dal management come una necessità per poter rimanere competitivi, nell'attuale mondo di informazione digitale la sicurezza dei sistemi informativi deve essere inclusa nelle Best-Practice; inoltre non è difficile trovare applicazioni ove la sicurezza informatica possa contribuire alla realizzazione di nuovi prodotti o servizi dando quindi all'azienda un contributo per la sua competitività.

2 Il CMM è nato per lo sviluppo software ma i principi principali del modello possono essere applicati in molti altri ambienti.

A ben pensarci, quanto appena descritto è in pratica quello che accade spesso, anche a chi scrive, in aziende medio-grandi ove il sistema informativo svolge un ruolo per lo più di supporto alla produzione e di comunicazione. In queste realtà non c'è spazio, risorse o tempi per poter fare un'analisi dettagliata, che in realtà quasi mai è necessaria. Un approccio più pratico, come quello qui esposto, spesso da maggiori risultati e viene meglio compreso.

Certamente quanto appena descritto può richiedere di procedere in una seconda fase ad una analisi delle vulnerabilità e dei rischi in senso tradizionale e molto dettagliata. Questo di solito capita per sistemi particolari, di importanza critica, o al contrario quando i costi coinvolti possono apparire troppo alti e devono essere giustificati dettagliatamente.

In conclusione, anche per l'esperienza di chi scrive, l'approccio descritto è spesso meglio compreso dal management e porta a risultati apprezzabili, anche se si basa molto sull'esperienza e capacità di chi lo svolge e non è supportato in pieno da procedure automatiche che diano risultati oggettivi ed imparziali in forma di puri numeri.

Andrea Pasquinucci
pasquinucci@ucci.it

Riferimenti Bibliografici

[1] D.B. Parker, *Making the case for replacing risk-based security*, ISSA Journal, Maggio 2006

[2] R.S. Lindberg, *Nimble Risk Management*, ISSA Journal, Agosto 2006