Il CISO: un ruolo tra mito e realtà

Non tutte le imprese possono avere un 'vero' Chief Information Security Officer interno: le PMI in particolare dovranno delegare questo ruolo a figure consulenziali

di Andrea Pasquinucci

Senior Security Professional e Membro del Comitato Direttivo CLUSIT

La sicurezza informatica è ormai una tematica a cui quasi tutti siamo esposti, sia nel privato che in ambiente lavorativo. Nelle grandi aziende si è ormai superata la fase della risposta occasionale, tecnica e solo successiva a un danno particolarmente grave e si è incominciato a capire che la sicurezza dei sistemi informativi deve essere gestita. Un ulteriore stimolo in questa direzione è dato dalle recenti legislazioni, dalla legge sulla Privacy al decreto Pisanu, e dalle norme, standard e certificazioni internazionali quali BS7799, ISO17799 e ISO27001.

Per gestire la sicurezza sono necessarie delle Politiche di Sicurezza, e per questo nelle grandi aziende sempre più spesso compare la figura del Responsabile della Sicurezza (CSO) a livello dirigenziale. Da questa figura dipendono sia il responsabile della sicurezza fisica che di quella logica, il Chief Information Security Officer (CISO) appunto, che svolgono mansioni tra l'organizzativo e il tecnico.

La realtà industriale Italiana è però caratterizzata da una grande maggioranza di aziende medio-piccole, e in questo caso la situazione è ben diversa. Sono infatti troppo poche le realtà ove le problematiche di sicurezza dei sistemi informativi sono comprese e gestite. In realtà non è difficile intuire il perché di questa situazione.

Pensare al core business

Un'azienda medio-piccola, ancor più di una grande, deve concentrarsi sul proprio core business e fare della specializzazione in questo la leva del successo. Il poco personale deve specializzarsi sul business e non sui servizi di supporto. Giustamente l'informatica e i servizi informativi sono visti come una commodity, un servizio di supporto appunto.

Infatti il personal computer è spesso visto come l'evoluzione della macchina da scrivere e le connessioni in rete, Internet ecc. come l'evoluzione di telefono, telex e fax. Questo è logico e naturale, anche chi scrive nel lontano 1985 prese il proprio primo personal computer per sostituire una macchina da scrivere, e nulla più.

Ma i sistemi informativi sono delle commodity molto speciali, molto diverse da acqua, luce, gas, telefono eccetera. La principale differenza è che i sistemi informativi gestiscono le informazioni, spesso cruciali per l'azienda, e non solo agiscono da substrato per il loro trasferimento o trasformazione. Quindi un problema al sistema informativo non vuol dire solo la perdita di un servizio di base al cui ripristino tutto ritorna alla normalità, ma molto, molto di più.

Il problema è che pochi tra coloro che dirigono le aziende, in particolare quelle medio-piccole, sono coscienti di questa fondamentale differenza.

Cosa può fare un'azienda medio-piccola per la sicurezza del proprio sistema informativo? Non avendo risorse interne, deve affidare la gestione spesso di buona parte se non di tutto il sistema informativo esternamente e in particolare affida la gestione della sua sicurezza, compito troppo specialistico da poter essere gestito internamente, a fornitori esterni.

Chi fornisce soluzioni hardware/software alle aziende sa benissimo che oggi queste richiedono anche aspetti di sicurezza, e non solo caratteristiche e prestazioni per il compito in questione, anche se la sicurezza spesso si riduce all'usuale accoppiata 'antivirus più firewall'.

Il fatto è che la soluzione antivirus più firewall è una soluzione tecnica, buona per tutti ma in questo caso con la sola funzione di tappabuchi. Il problema della sicurezza dei sistemi informativi non viene affrontata, vengono solo tappate le falle più evidenti.

Per poter affrontare globalmente ed efficacemente la problematica della sicurezza dei sistemi informativi è necessario partire a un livello più alto all'interno dell'azienda. Visto che chi dirige un'azienda medio-piccola in genere non ha le competenze per affrontare questa problematica, l'unica soluzione è affidarsi a un consulente esterno.

Il CISO-consulente

Una soluzione che a nostro parere dovrebbe funzionare starebbe nell'esistenza di CISO - potremmo dire più generalmente CSO, ma vorremmo qui concentrarsi sui sistemi informativi, e quindi parlare più specificatamente di CISO - consulenti esterni.

In questa sede volutamente non affrontiamo il problema delle qualifiche che identificano un valido CISO-consulente, ma questi CISO-consulenti dovrebbero avere un elevato grado di specializzazione e di competenze con un orizzonte abbastanza ampio, a partire dalla comprensione dei processi aziendali sino agli aspetti tecnici di sicurezza informatica. In fondo queste non sono altro che le competenze di un buon CISO: comprendere il funzionamento della propria azienda ed essere in grado di fare le appropriate scelte tecniche in sicurezza informatica in modo da supportare il business dell'azienda.

Nel caso delle aziende medio-piccole, a nostro parere il CISO-consulente dovrebbe seguire l'azienda per un lungo periodo di tempo, magari in modo non molto frequente ma regolare, per poter comprendere i rischi e guidare le scelte, implementazioni e uso delle tecnologie. Il tutto però partendo dall'alto, dall'approccio strategico e non dal basso, dal punto di vista tecnico.

Ma esistono questi CISO-consulenti? In linea di principio si, e chi scrive potrebbe esserne uno, ma il problema è che chi gestisce un'azienda medio-piccola, oltre al rifiuto viscerale per 'un altro consulente...', come abbiamo detto difficilmente comprende la differenza tra 'macchina da scrivere più fax' e sistema informativo, e quindi il perché dovrebbe spendere qualche cosa in più per andare oltre al binomio antivirus più firewall.

Quindi al momento il mercato per la figura professionale del CISO-consulente per le aziende medio-piccole sembra non esistere o essere ristretto ad alcune realtà molto particolari. Purtroppo però l'assenza di qualcuno che sappia veramente consigliare l'azienda nelle scelte relative agli aspetti di sicurezza del sistema informativo troppo spesso viene pagata con la mancanza di sistemi di sicurezza oppure acquisti sbagliati, progetti fuori budget o destinati al fallimento.

Questione di cultura...

Migliorerà la situazione in futuro? Tutti ovviamente speriamo di sì, anche se le indicazioni sono contrastanti.

Da una parte l'informazione e l'educazione che si sta facendo sulle problematiche della sicurezza informatica porterà sicuramente a un aumento della percezione del problema. D'altra parte, in particolare noi italiani, siamo portati a prendere atto e agire solo a seguito di un fatto che ci ha colpiti direttamente e profondamente, come una grossa perdita economica, anche se eravamo già a conoscenza della pericolosità e dei rischi e avremmo potuto fare qualche cosa per mitigare il problema. A volte neanche le imposizioni di legge vengono applicate nell'ottica del 'tanto non se ne accorgerà mai nessuno'! Non è chiaro quindi quanto la presa di coscienza del problema corrisponderà ad un'azione più articolata dell'acquisto dell'antivirus più firewall.

Inoltre, se da una parte tutti i produttori e fornitori di sistemi informativi hanno preso seriamente a cuore il problema della sicurezza e tutti ci auguriamo che il numero e la gravità delle vulnerabilità diminuisca nel prossimo futuro, dall'altra l'interconnessione delle reti e il mondo delle informazioni digitali cresce in complessità, interrelazioni e pericolosità/rischi in modo molto più veloce.

Il problema 'umano'

Infatti un possibile futuro vedrà le componenti dei sistemi informativi, ormai servizi di supporto o commodity, di per sé molto più sicure, ovvero con poche vulnerabilità intrinseche. La tecnica e gli strumenti saranno molto più affidabili e sicuri, facili da gestire e da interconnettere. Antivirus e firewall saranno inclusi in ogni device e non avranno bisogno di interventi esterni per funzionare.

Ma come stiamo già vedendo oggi ad esempio con le truffe on-line, il problema si sposterà sempre più e sarà sempre più drammatico sul fronte umano, ovvero della gestione delle informazioni scambiate e immagazzinate nei sistemi informativi.

In maniera quasi unanime gli esperti concordano nel ritenere che per questo tipo di problemi la tecnologia da sola sia di poco aiuto, se non addirittura nullo o controproducente. Ecco quindi che, malgrado i miglioramenti tecnologici, si ripropone la necessità anche per aziende medio-piccole di una gestione delle problematiche di sicurezza dei sistemi informativi già a livello dirigenziale, tipicamente tramite la figura del CISO-consulente.