Sicurezza informatica: un'opportunità oppure l'ennesima incombenza da sopportare?

Enrico Cavalli
CILEA, Segrate

Abstract
La sicurezza informatica, così come codificata dallo standard internazionale ISO 17799, è un'opportunità per migliorare l'organizzazione e i processi di un'azienda oltre che la sicurezza in sé e per sé? Oppure si tratta di una fantastica utopia non realizzabile concretamente? In questo articolo cercheremo di dare una panoramica dello standard, illustrando perché, in futuro, potrebbe essere importante ottenere la certificazione ISO 17799.

Keywords: Telematica, Sicurezza, ISO 17799, USA.

Premessa

Tutti conosciamo la definizione di sicurezza informatica come mantenimento della confidenzialità, integrità e disponibilità delle informazioni. L'avremo letta almeno una dozzina di volte, e altrettante volte avremo visto scritte le tre parole cardine sulle proiezioni di qualche oratore in uno degli innumerevoli convegni che trattano l'argomento.

- Confidentiality;
- Integrity;
- Availability.

Queste tre famose proprietà compaiono nella prefazione dello standard internazionale ISO 17799: "Code of practice for information security management" [1] .
Adeguarsi ad uno standard può in certi casi essere vissuto come un problema, un obbligo dal quale per qualche motivo non ci si può sottrarre. Naturalmente il processo di adeguamento è tanto più oneroso, quanto più la propria prassi aziendale si discosta dal modello delineato dallo standard stesso. In questo senso la questione potrebbe essere ribaltata ponendosi una domanda: è giusto proseguire come abbiamo sempre fatto, oppure è bene prendere in considerazione lo standard? Non dimentichiamo poi un'altra questione fondamentale: quando e quanto sarà richiesto essere certificati ISO 17799 dai nostri clienti piuttosto che dai nostri partner? L'impressione generale che si ricava dalla letteratura disponibile è che i tempi non siano del tutto maturi. Non solo perché manca la seconda parte dello standard, ovvero quella che serve agli enti certificatori per poter svolgere il proprio compito, ma anche e soprattutto perché non è ancora largamente diffusa una vera cultura della sicurezza dell'informazione.

È pur vero che moltissime aziende hanno già affrontato o stanno affrontando vari investimenti dal punto di vista delle tecnologie per la sicurezza. Firewall e antivirus sono ormai strumenti di uso comune. Alcuni hanno persino avuto l'ardire di acquistare un IDS (Intrusion Detection System) – e forse stanno ancora cercando di capire come utilizzarlo al meglio, potrebbe aggiungere con un eufemismo qualche maligno. È anche ormai diffuso - ma forse non sempre pienamente recepito - il famoso detto: la sicurezza non è un prodotto, bensì un processo. Le riviste specializzate sono piene zeppe di articoli sulla sicurezza che cercano di diffondere un clima di terrore tra gli IT Manager: dopo tutto stiamo cercando di fare lo stesso anche in questa sede.

Il valore delle informazioni

Molto spesso nell'ambito dell'*information security,* così come in tante attività della vita umana, si adotta un processo bottom-up: si parte dal basso, dal problema, dagli strumenti tecnologici che permettono di ottenere un certo grado di sicurezza in determinati, ma ristretti, ambiti. Tanto per intenderci, dotarsi di firewall e di antivirus sono solo due piccole contromisure che un'azienda può adottare per salvaguardare il proprio patrimonio informativo. Per dirla in altri termini, è il modo di

procedere di chi costruisce una teoria partendo dall'esperienza pratica: il discorso ha sempre funzionato in varie discipline scientifiche.
Lo standard ISO 17799 offre un punto di vista completamente diverso, in quanto ha un approccio top-down alla problematica della sicurezza delle informazioni. Le chiavi di lettura dello standard sono due: da un lato il valore che le informazioni hanno per un'azienda, e dall'altro la constatazione di un dato di fatto, ovvero che molti degli attuali sistemi informativi non sono stati progettati pensando alla sicurezza.
C'è differenza tra una casa e l'informazione, a parte il fatto che l'una è di mattoni mentre l'altra è intangibile? Sicuramente hanno almeno un punto in comune: entrambe sono beni. Un bene ha valore, e tanto più alto il valore, tanto più siamo disposti – o costretti - a spendere per proteggerlo adeguatamente. Una casa ha fondamenta in calcestruzzo, ha dei muri perimetrali, ha una porta di ingresso, magari blindata. Se abitiamo al piano terra potremmo considerare la possibilità di porre delle inferriate alle finestre. E perché non installare un impianto antifurto?
Ovviamente i rischi di furto non scompaiono mai del tutto, nonostante le varie misure di sicurezza adottate: proprio per questo motivo abbiamo anche stipulato una polizza di assicurazione che ci tuteli in casi malaugurati.
Perché l'informazione, non solo quella digitale, dovrebbe essere trattata diversamente dato che anch'essa è un bene? Una formula chimica segreta, informazione assolutamente intangibile, quale enorme valore può avere per un'industria farmaceutica? Quanto è stato investito in ricerca e sviluppo per arrivare a quella formula? Se quindi il documento che contiene tale formula, una misera accozzaglia di bit, è il risultato di dieci anni di ricerca, non ha forse senso proteggerlo al meglio? Non solo per evitare che vada perso, perché butteremmo al vento un enorme investimento, ma anche affinché non cada nelle mani della concorrenza, cosa forse ancora peggiore. Intendiamoci: lo spionaggio industriale è sempre esistito e sempre esisterà. L'era digitale ha solo aggiunto nuove opportunità di spionaggio, perpetrabile attraverso i sistemi informatici: ecco che in questo contesto la sicurezza diventa un ovvio e oserei dire banale strumento per conservare un vantaggio competitivo.

Risk assessment come elemento centrale nella costruzione di un piano di sicurezza aziendale

Presa coscienza del valore delle informazioni, è necessario formalizzarlo in qualche modo, definendo innanzitutto quali siano le informazioni di valore. Queste ultime vanno quantificate sia in termini di valore intrinseco, sia in termini di possibili danni derivanti dal venire meno dei requisiti di confidenzialità, integrità e disponibilità dell'informazione in questione. Osserviamo che in questa prospettiva rientrano anche tutti gli adempimenti previsti dalle leggi, quali ad esempio la famosa legge sulla privacy italiana.
Questo è proprio lo spirito dell'ISO 17799: l'informazio-ne è un bene e come tale va protetto, non con un prodotto, ma con un laborioso processo. Il punto di partenza di quest'ultimo è il cosiddetto risk assessment.
Occorre per prima cosa inventariare le informazioni proprie di un'azienda e assegnarvi un valore, tenendo ovviamente in conto il possibile danno che un problema di sicurezza può portare, e con quale probabilità ciò possa accadere. Bisogna in pratica mettere da una parte i beni, dall'altra le possibili minacce che potrebbero intaccarli sfruttando vulnerabilità del sistema informativo, e stimare probabilità e danni potenziali. Il lavoro è enorme ma indispensabile, nonostante il concetto di inventariare le informazioni suoni un po' strano. Come è possibile inventariare ciò che è intangibile? Inoltre è sempre possibile assegnare un valore ad un'informazione? O meglio, come stabilire in termini economici i danni derivanti da un problema di sicurezza? Per non parlare dei danni indiretti, quali ad esempio la perdita di credibilità di un'azienda che opera nel settore del banking online se vittima di un incidente di sicurezza: un'azienda di questo tipo in un caso simile potrebbe addirittura fallire.
Teniamo presente che un'analisi economica accurata potrebbe essere assolutamente indispensabile se provassimo ad addentrarci in un terreno oserei dire ancora un po' minato, quello delle assicurazioni “digitali”: è possibile ipotizzare forme di trasferimento del rischio informatico? Questo discorso assicurativo ci porterebbe tuttavia lontani dal nostro tema, anche se apre notevoli prospettive per il futuro.
La valutazione economica di cui parlavamo poc'anzi non è sicuramente un'impresa semplice, specie in realtà molto complesse. Proprio per questo motivo a volte si operano valutazioni puramente qualitative, ad esempio assegnando i valori basso/medio/alto al valore di un bene, piuttosto che al rischio dovuto ad una minaccia.
In ogni caso il risk assessment è un'opportunità per razionalizzare molti processi aziendali. Dopo tutto la vera sfida sta nel considerare l'informazione nel suo ciclo di vita, da quando viene prodotta, a quando viene elaborata,

trasferita, archiviata, trasformata (ad esempio con una stampa). Tanto per intenderci, non ha senso adottare schemi di autenticazione basati su certificati, smart-card, token o chissà quale diavoleria biometrica, se poi non c'è una procedura che dica "non gettare documenti riservati nella pattumiera, senza averli pre-ventivamente distrutti con un tritacarte".
E non si creda che basti scrivere una procedura perché questa venga applicata: banalmente dovranno essere resi disponibili i tritacarte, e la gente dovrà fare proprio questo comportamento. Vi sembra assurdo? Non tanto: quante volte ci si reca alla macchinetta del caffé senza un salvaschermo protetto da password, lasciando magari sul monitor dati riservati in bella mostra per chiunque passi nei paraggi? Quanti di noi adotterebbero sistemati-camente una procedura del tipo "blank desk and blank screen", come piace dire agli americani: "scrivanie e schermi puliti quando ci si assenta dal posto di lavoro". Si noti il termine "sistematicamente". Quando si parla di procedure di sicurezza, queste vanno applicate sempre, con costanza e coscienza.
Al di là del fattore mentalità degli individui, che devono essere educati con opportuni programmi di formazione – e già questo ha un costo, indiretto se vogliamo - vi è ovviamente un discorso di tipo economico: nell'esempio originale la questione si ridurrebbe a determinare quanti tritacarte dobbiamo acquistare. Quali dipendenti devono essere dotati di tritacarte? Ovviamente coloro che stampano informazioni riservate! Chi sono costoro? Ecco che ci riconduciamo al famoso problema iniziale di inventariare correttamente le informazioni, contestualizzandole nei processi aziendali che ne fanno uso. Soltanto se sappiamo dare un valore alle informazioni, potremo paragonarlo con il costo dei tritadocumenti.
Capiti quali sono i beni intangibili da proteggere e quali le minacce che potrebbero colpirli, occorre stabilire come ridurre i rischi ad un livello accettabile, tenendo comunque presente che un rischio residuo è destinato a permanere nonostante ogni sforzo, e che questo rischio va comunque gestito in caso di incidenti di sicurezza. Lo standard ISO prescrive un percorso organico che va dalla stesura delle security policy, alle procedure operative e all'implementazione di tecnologie. La tecnologia è quindi solo una piccola parte di un processo che può prevedere modifiche alla struttura organizzativa e sicuramente implica un nuovo modo di ragionare delle persone. È fondamentale sensibilizzare gli individui verso la questione sicurezza, illustrando come quest'ultima sia costruita proattivamente da ciascuno di noi.
Avremo comunque modo di tornare sugli argomenti più propriamente operativi nella stesura di un piano di sicurezza aziendale, con una serie di articoli dei quali il presente vuole essere una sorta di introduzione.

Certificarsi o non certificarsi: questo è il problema

Ha senso allora certificarsi? È veramente necessario oppure basta imparare la lezione e applicarla in modo ragionato? Se vogliamo porci un'altra domanda, forse più difficile, potremmo poi chiederci: quando certificarsi? Appena possibile o tra cinque anni?
Non esistono evidentemente risposte univoche e bisognerebbe valutare caso per caso, anche e soprattutto in relazione alle disponibilità economiche che un piano di sicurezza può richiedere per essere studiato seriamente ed implementato con efficacia, in osservanza dello standard ISO.
Tradurre quelli che in fondo non sono altro che tanti buoni consigli e il banale buon senso della ISO 17799 in implementazioni concrete, non sempre può essere economicamente fattibile, specie in realtà medio-piccole. Il punto importante che tuttavia rende la normativa interessante per chiunque si occupi di informazioni, è la metodologia che fornisce, la prospettiva di alto livello sul problema sicurezza che forse è troppo spesso trascurata.

Se invece volessimo spendere due parole in favore di una futura certificazione, potremmo iniziare a riflettere su questa frase: "IT security professionals, and IT security associations and organizations, should explore approaches to, and the feasibility of, establishing a rigorous certification program, including a continuing education and retesting program".
Chi l'ha scritta sembra proprio deciso ad incoraggiare i destinatari dei consigli a muoversi verso qualche forma di certificazione. Si tratta di una raccomandazione, ritenuta Priorità Nazionale, che compare nel draft "*National Strategy to Secure Cyberspace*".
Nonostante la parola cyberspace possa far sorridere, visto l'uso e l'abuso che ormai ne viene fatto, la fonte del documento, in stato di bozza nel momento in cui scriviamo, è sicuramente poco propensa all'ironia: si tratta infatti di un ufficio della Presidenza degli Stati Uniti d'America, il *President's Critical Infrastructure Protection Board* [2].
È un documento che mostra una netta presa di coscienza ed una precisa volontà strategica di

migliorare la sicurezza del cyberspazio, ad ogni livello. Al suo interno viene trattata la sicurezza dal punto di vista dell'utente domestico, della pubblica amministrazione, della grande multinazionale: vengono delineate strategie e suggerite raccomandazioni per vari settori della società. L'idea alla base del documento è che il cosiddetto cyberspazio è una realtà sempre più radicata nella nostra vita quotidiana, sempre più pregnante in ogni attività umana. Ognuno di noi, a vario titolo, fa uso e fa parte del cyberspazio, che deve perciò essere un ambiente ragionevolmente sicuro.
Nel documento si legge tra le altre cose: "States should consider creating Cyber Corps scholarship for service programs at State universities, to fund the education of undergraduate and graduate students specializing in IT security and willing to repay their grants by working for the States". Questo passaggio evidenzia una forte volontà di investire in formazione, fin dalla scuola e dalle università. L'educazione, la formazione, sono elementi essenziali per la sicurezza dell'informazione, tanto quanto gli investimenti necessari in tecnologia, anzi forse ancora di più.

Cerchiamo allora di riassumere con uno slogan la ricetta americana: consapevolezza collettiva, formazione dei giovani e codici di autoregolamentazione, ovvero standard accettati da tutti, per le aziende: componenti essenziali di una ricetta più ampia ed articolata. È vero che si tratta di una ricetta targata USA, e non è frutto del made in Italy, in generale dedito a questioni più frivole, ma forse qualcosa possiamo recepirlo fin d'ora per prepararci ad un futuro più sicuro, almeno nel mondo delle informazioni.

Bibliografia

[1] ISO/IEC 17799, *Information Technology – Code of practice for information security management*.
URL: http://www.iso.ch/, oppure, per gli abbonati:
http://www.cilea.it/Virtual_Library/wss/home.htm
[2] URL: http://www.whitehouse.gov/pcipb/