CRITICAL INFRASTRUCTURE SECURITY

I COMMON CRITERIA COME STRUMENTO DI ASSURANCE PER L'HOMELAND SECURITY

A partire dagli eventi dell'11 settembre ed a seguito di altri eventi dove spicca quello del blackout del 28 settembre 2003, si è diffusa anche tra i non addetti ai lavori la consapevolezza di quanto delicato sia l'equilibrio della nostra Società e di quanto su questo equilibrio contino i settori definiti "Infrastrutture Critiche del Paese": l'energia, l'acqua, le comunicazioni, i trasporti, la sanità.

Al di là di quanto viene già fatto per assicurare una sorta di *business continuity* relativamente a questi settori emerge oggi senza dubbio una ulteriore importantissima considerazione; le Infrastrutture Critiche sopra definite si basano a loro volta tutte su una comune infrastruttura critica, quella dell'ICT.

Oltre a questo, ricordiamo come in Italia nel 2002 il Ministero dell'Innovazione e Tecnologie ha pubblicato il documento "Linee Guida del Governo per lo Sviluppo della Società dell'Informazione" nel quale viene raccomandata e rafforzata la tendenza all'informatizzazione nella Pubblica Amministrazione (PA) definendo un impegno formale del Governo italiano a rendere il Paese un leader nel settore dell'era digitale, sottolineando il forte orientamento alla modernizzazione del paese attraverso l'uso esteso dell'ICT sia nel settore pubblico che in quello privato e la spinta a risollevare la competitività del paese accelerando l'istaurarsi dell'e-business e dell'e-government.

In ultimo ricordiamo il progetto del "Sistema Pubblico di Connettività (SPC)", definitivamente assegnato a maggio del 2006 che consente una più razionale e completa integrazione delle pubbliche amministrazioni centrali e locali, migrando quanto già esistente nella Rete Unitaria della PA (RUPA) alla nuova rete del SPC.

Non voglio dilungarmi in modo particolare sul settore privato, dove la situazione è come minimo equivalente e molto spesso anche avanzata rispetto al settore Pubblico: avanzata almeno per quanto riguarda l'uso esteso delle tecnologie a tutti i livelli dell'impresa.

L'ultimo elemento che assolutamente non deve essere dimenticato è rappresentato dai singoli utilizzatori a livello personale o professionale, che in genere vengono definiti SOHO (Small Office, Home Office).

Sicurezza: tutti attori della stessa commedia

Penso ci si possa trovare d'accordo sul fatto che l'infrastruttura ICT è la base su cui vive la nostra Società tecnologica, che è a sua volta una base fondamentale della nostra Società Civile.

Da questo ne deriva che tutto ciò che mette in crisi l'infrastruttura ICT, può molto facilmente mettere in crisi la nostra vita quotidiana.

È ovvio quindi che dobbiamo prendere tutte le precauzioni che servono, fare tutte le verifiche necessarie, analizzare tutti i rischi possibili, eliminare - al meglio - tutte le vulnerabilità di cui siamo a conoscenza allo scopo di mantenere in buona salute questa Infrastruttura e noi con essa.

Siamo sicuramente d'accordo, perchè no? Sarà comunque un problema della Grande Azienda di turno o del Ministero Tale e Talaltro mettere in piedi i corretti meccanismi e far funzionare il tutto, giusto?

Ahimé non è più così, ammesso che lo sia mai stato.

L'utilizzo di Internet e dei servizi che ogni istante vengono preparati e ci vengono messi a disposizione sulla Rete, rendono l'infrastruttura di cui stiamo parlando un elemento unico, non più banalmente separabile in grandi regni all'interno di confini protetti da firewall o piccole provincie composte da manciate di computer o magari da singoli PC: l'Infrastruttura ormai siamo anche noi, sia con i nostri sistemi in Azienda, sia con il nostro singolo PC di casa.

E se questo è vero, il significato è che il mantenimento in buona salute di questa Infrastruttura dipende anche e naturalmente in proporzione da ogni singolo Ente, da ogni singola Azienda e da ogni singola persona che utilizzino un computer connesso ad Internet.

Aumentare la consapevolezza

Ci si potrebbe quindi aspettare che le Aziende private investano sulla sicurezza ICT in modo adeguato, che la Pubblica Amministrazione faccia altrettanto e che i gestori dei servizi nei settori critici di cui si parlava inizialmente siano i migliori interpreti dell'ICT Security e di quanto ne fa parte.

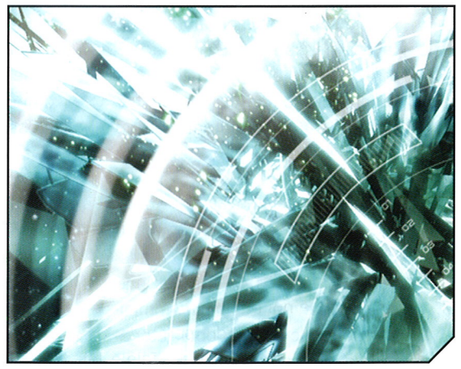
Ahimé di nuovo, non è così.

Ragioni legate al ROI (return on investment), all'attuale fase economica, al basso livello di consapevolezza e qualche volta anche alla colpevole negligenza, sono le semplici ragioni dell'attuale medio/basso livello di sicurezza nei sistemi informatici e nella rete in generale.

A parte singole nicchie di eccellenza organizzativa o magari di specializzazione nell'ICT Security, in generale il livello di sicurezza non sembra adeguato alla criticità da gestire.

Molti sforzi ed indicazioni sono stati dati in questi anni da parte di vari organismi governativi; senza pretendere di essere esaustivi vale la pena di ricordare:

- In Italia nel 2002 il Ministero dell'Innovazione e Tecnologie ha pubblicato il documento "Linee Guida del Governo per lo Sviluppo della Società dell'Informazione" nel quale viene raccomandata e rafforzata la tendenza all'informatizzazione nella Pubblica Amministrazione (PA) definendo un impegno formale del Governo italiano a rendere il Paese un leader nel settore dell'era digitale, sot-



Sandro Fontana
CISSP, L.A.BS7799, CISM
Founder Secure Edge Srl
www.secure-edge.com

È corretto dichiarare che l'ICT è l'infrastruttura critica delle Infrastrutture Critiche del Paese; è anche corretto ipotizzare che queste infrastrutture ICT possano essere correlate, interdipendenti e spesso in qualche modo connesse ad Internet e con tutte le altre infrastrutture ICT. Si può ragionevolmente supporre che una minaccia o un incidente informatico, dovunque si presenti, possa avere un impatto più o meno grande anche sulle Infrastrutture Critiche e di riflesso quindi sulla Homeland Security.
L'unica soluzione possibile: aumentare globalmente il livello di consapevolezza di tutti gli utenti ed il livello di sicurezza di tutti i sistemi.

tolineando il forte orientamento alla modernizzazione del paese attraverso l'uso esteso dell'ICT sia nel settore pubblico che in quello privato e la spinta a risollevare la competitività del paese accelerando l'istaurarsi dell'e-business e dell'e-government.

Naturalmente in questo documento ci si preoccupa della sicurezza delle reti e si introdoce un piano nazionale per la sicurezza e privacy nell'ICT.

- Sempre nel 2002 è stato inoltre costituito il Comitato nazionale della sicurezza ICT che ha preparato un documento a titolo "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni (ICT) per la Pubblica Amministrazione".
- Nel Marzo 2003, è stato istituito il Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate che ha rilasciato nell'Ottobre del 2003 il documento Protezione delle Infrastrutture Critiche Informatizzate
- Mentre in data 29 ottobre 2003 è stato approvato il decreto per l'istituzione di uno schema nazionale per la certificazione di sicurezza secondo gli standard ITSEC e Common Criteria di prodotti e sistemi ICT che non trattino informazioni relative al segreto di stato.

Pur non credendo alle bacchette magiche ed alla loro capacità di risolvere di colpo tutti i problemi, proprio quest'ultimo punto, l'introduzione di una certificazione secondo lo standard dei Common Criteria, potrebbe significativamente aiutare la crescita del livello di sicurezza.

Indubbiamente l'Infrastruttura ICT ha una forte necessità non solo di sicurezza, ma di un tipo di sicurezza certificata, cioè definibile a seconda delle necessità e fondamentalmente misurabile; questo è quanto "promettono" i Common Criteria:

la possibilità di comparare i risultati di processi di valutazioni di sicurezza indipendenti, per mezzo di un comune gruppo di requisiti dedicato sia alle funzioni di sicurezza dei sistemi e dei prodotti IT sia alle misure di assicurazione che ad essi si applicano durante il processo di valutazione della sicurezza.

In pratica con l'aiuto dei Common Criteria sarà possibile sia definire i requirements dei sistemi e dei prodotti che si vuole utilizzare, sia misurare il livello di sicurezza di un prodotto o di un sistema in modo indipendente quanto possibile dal valutatore.

Ma adeguare i propri sistemi o quelli che si vendono ovvero pretendere che quelli che si comprano abbiano un Evaluation Assurance Level (livello di garanzia) secondo i Common Criteria anche minimale, diciamo almeno EAL2 introduce almeno inizialmente un ulteriore costo.

Come convincere allora Fornitori, Clienti e Pubblica Amministrazione ad intraprendere questa strada virtuosa? Come si potrà introdurre un simile comportamento in tutti i partecipanti?

Il modello potrebbe prendere spunto da una precedente ed in quel caso non sempre felice esperienza: quella dei sistemi certificati in Qualità secondo la norma ISO 9001 (attualmente) Visio 2000.

A chi è la battuta?

Come per molti altri processi nel passato, in Italia il primo attore di questo genere di rappresentazioni è tipicamente la Pubblica Amministrazione.

Un modello plausibile vede l'ingresso della certificazione Common Criteria, tramite tre differenti step:

1. Nelle prossime gare la PA dichiarerà la sua volontà di valutare con favore (nessun obbligo per il fornitore) le offerte nelle quali i sistemi proposti siano certificabili secondo i Common Criteria con un EAL2 secondo il Protection Profile che può essere richiesto da chi partecipa alla gara.
2. Dopo un periodo di tempo che va dai 12 ai 18 mesi e con un'adeguata campagna di informazione precedente, la Pubblica Amministrazione richiederà obbligatoriamente ai propri fornitori sistemi che siano certificati secondo i Common Criteria ancora con un EAL2 ed in alcuni casi EAL3, sempre secondo il Protection Profile relativo alla specifica fornitura.
3. Dopo un'ulteriore periodo di 18/24 mesi e sempre dopo un'adeguata campagna di informazione anticipatrice, fermo restando il punto 2 la Pubblica Amministrazione non potrà più acquistare da fornitori che non abbiano il proprio sistema informativo certificato secondo la ISO 27001 e nei casi dove questo sia necessario, i cui sistemi informativi non siano stati certificati secondo i Common Criteria anche i questo caso EAL2 ovvero EAL3, il cui Protection Profile sia pubblicamente analizzabile allo scopo di valutare la sua adeguatezza.

Vantaggi

Un modello di questo tipo permette di obbligare le aziende, non per coercizione, ma per concorrenza: sarà quindi un investimento giustificabile in quanto requisito o vantaggio in fase di gara.

Inoltre a differenza della certificazione in Qualità ISO 9001, la certificazione secondo i Common Criteria è distinta in due fasi:

1. la valutazione di quanto prodotto ai fini della certificazione, che viene effettuata da un Laboratorio di verifica (LDV) indipendente, che comporta la produzione di un report;
2. la certificazione vera e propria, basata sul report realizzato nel passo 1) ed effettuata a discrezione da OCSI in modalità centralizzata;

Il controllo e l'erogazione centralizzata delle certificazioni, assicura senza dubbio il valore della certificazione stessa, che ne viene così irrobustito.

Una volta entrato a regime questo modello, se pur neppur esso una "bacchetta magica", potrà fare sicuramente da volano per l'aumento della consapevolezza generale sulle tematiche di sicurezza e dare un forte contributo alla crescita generale del livello di sicurezza ICT del Paese. ■