

# INFORMATICA & DOCUMENTAZIONE

RAPHAEL BRANDO  
LINVS IUNIOR LIPPVS

RAPHAEL BRANDO  
LINVS IUNIOR LIPPVS  
IOANNI MEDICO DA  
CŌ CAR AC PRVDĒTIS  
SIMO BONONIETHV  
CIEQ APŪICE SEDIS  
LEGATO S P D



T SINO

*dubito propter gra-  
uissimas & Bononi-  
ensis Legationis &  
Florentine Rei pu-  
blice res tui unius nutu arbitrioq; ge-  
rendas nihil tibi ocu ad agenda pri-*

rivista  
dell'

**INFORav**

Anno 7 (N. 1 e 2/2009)

## OCCORRE ALZARE IL LIVELLO DI GUARDIA!

MARCELLO PISTILLI

La sicurezza dei sistemi informatici? Oggi rappresenta una vera e propria emergenza che investe gli utenti finali al pari del core di qualsiasi organizzazione pubblica o privata, richiedendo specifiche tutele. Ma la salvaguardia da potenziali rischi e la protezione dalla violazione dei dati non sono aspetti che possono essere esclusivamente delegati all'esterno... devono piuttosto entrare a far parte del bagaglio culturale di ciascuno di noi. L'obiettivo è quello di trasformare sempre più la "tutela" in una forma di "autotutela".

Purtroppo non ci si rende conto che il pensiero dominante, che sembra essere "perché proprio a me o alla mia azienda?", può arrivare a compromettere la vita stessa dell'impresa o magari a mettere in seria difficoltà un governo... Un atteggiamento consapevole e responsabile dovrebbe andare ben oltre la pubblicazione sull'intranet aziendale delle procedure di sicurezza o la loro diffusione tramite circolare interna. Nelle aziende, così come negli enti pubblici, il management dovrebbe monitorare costantemente il livello di comprensione e accettazione delle policy di sicurezza da parte dei propri collaboratori, dotandoli magari di un codice di condotta che concorra a responsabilizzarli nella loro attività quotidiana. È tuttavia utile ricordare che politiche noiose, farraginose, di complessa attuazione o peggio ancora incomprensibili, saranno verosimilmente disattese.

Sarà opportuno organizzare dei veri e propri gruppi operativi che documentino in modo oggettivo alla dirigenza la qualità del lavoro svolto e individuino gli aspetti migliorabili mediante un'attività periodica di auditing tecnologico e di processo. A livello preliminare basterebbe adottare alcuni semplici accorgimenti... un esempio? L'offuscamento dei dati reali che ancora oggi, senza alcun tipo di restrizione, vengono impiegati dai gruppi dedicati al testing e al collaudo delle procedure. Fino a quando prevarrà la logica di condurre le attività nel minor tempo possibile e ridurre all'osso le spese per l'espletamento del progetto, la sicurezza e la tutela della privacy continueranno a rappresentare un'occasione mancata.

Considerando l'evoluzione della tecnologia nel corso degli ultimi quarant'anni emerge con chiarezza quanto essa sia stata dirompente. Al tempo delle schede hollerit nessuno avrebbe neanche lontanamente immaginato l'avvento di Internet, figurarsi facebook, youtube o twitter. Purtroppo appare altrettanto evidente come la consapevolezza dei rischi connessi all'impiego di questi strumenti, non si sia evoluta con la stessa rapidità.

Sembrano ormai distanti anni luce i tempi in cui gli operatori dei CED vestivano i camici bianchi e si muovevano come sacerdoti di una nuova e potente religione...

MARCELLO PISTILLI

*Dopo la laurea in matematica conseguita presso l'Università di Pisa e la specializzazione in calcolo automatico presso lo I.E.I. della stessa città toscana, approda al CNR. Al termine dell'esperienza in Syntax, assume incarichi di crescente responsabilità dapprima in Olivetti, successivamente in Rigel (Gruppo Itway) e Innovia. Dal 2007 è Business Development Manager Information Security di Eustema Spa.*

Da allora ad oggi è cambiato tutto! L'informatica non è più una religione per iniziati. Si è trasformata in un culto di massa che condiziona profondamente il modo di lavorare di miliardi di persone in tutto il mondo e che consente ad aziende, amministrazioni pubbliche e persone fisiche di interagire in Rete, ventiquattro ore al giorno.

Ognuno di noi affida al proprio personal computer dati vitali per sé, per il lavoro e per la famiglia, testimoniando che Internet è ormai parte integrante della nostra vita. Ma siamo davvero consapevoli della natura e dei rischi degli strumenti che utilizziamo per lavorare, comunicare, interagire? Possiamo affermare di conoscerli davvero bene e di potercene fidare? Chiunque lavori in questo settore da alcuni decenni, come il sottoscritto, molto probabilmente vi risponderà di no.

La facilità di utilizzo del personal computer è risultata direttamente proporzionale alla sua diffusione e inversamente proporzionale alla necessità di studio e di formazione per il suo impiego. In molti si sono domandati e ancora oggi si domandano "perché perdere tempo sui 'banchi di scuola' per uno strumento tanto semplice ed intuitivo?".

Forse perché la non perfetta conoscenza degli strumenti, una certa abitudine alla cultura "fai da te" e il relativo anonimato garantiti dal mondo informatico possono determinare atteggiamenti "leggeri" o sfociare, nel peggiore dei casi, in veri e propri comportamenti non etici. Dietro al proprio monitor è facile "sentirsi" irrintracciabili e, in alcuni casi, farsi tentare dall'anonimato al punto di commettere azioni al limite della legalità. Ma nascondersi dietro uno schermo può soltanto rendere l'individuazione problematica, non impossibile.

Qualsiasi individuo intenzionato ad accendere un PC e a navigare in Internet dovrebbe sapere che muoversi, operare, comunicare in Rete senza lasciare tracce è semplicemente impossibile!

Spesso anche i professionisti chiamati a scrivere stringhe di codice, o magari a definire i parametri di funzionamento di un router o di un dispositi-

vo di sicurezza, commettono imperdonabili leggerezze. Ciò accade a tutti quegli "addetti" che non considerano il proprio lavoro come un'attività dalla quale può dipendere la salute di altre persone. Una falla in un software può mettere a disposizione di individui non etici dati sensibili, favorire il furto di identità e di informazioni finanziarie. Difficilmente uno sviluppatore o un responsabile della gestione dei dati sensibili percepisce il proprio ruolo come fondamentale per la sicurezza di altri individui. Un deficit che potrebbe essere colmato ricorrendo ad azioni di sensibilizzazione e favorendo il più possibile l'adozione di strumenti tecnici e culturali per verificare la sicurezza dei prodotti informatici, sia prima del loro rilascio che a regime. Ancora oggi, nei contesti più vari, molti responsabili di prodotto prestano attenzione alle anomalie di tipo funzionale, quelle che nella maggioranza dei casi possono influenzare l'esito di un collaudo, ma difficilmente si concentrano su quelle di sicurezza.

A commettere rischiose leggerezze, comunque, non sono soltanto utenti finali e addetti ai lavori... capita di frequente che alcuni top manager, politici, magari individui con delicati incarichi di governo, si facciano rubare o smarriscano il proprio sistema portatile PC, Palm o cellulare, gonfio di dati sensibili. Dati ovviamente non protetti da robusti sistemi di accesso o di crittografia, soluzioni considerate dai più troppo complicate o troppo costose per essere impiegate.

In Italia esistono sia un Garante per la Privacy sia un codice in materia di protezione dei dati personali e sensibili che obbliga aziende, pubbliche amministrazioni e manager alla redazione e al rispetto del DPS (Documento Programmatico sulla Sicurezza), con implicazioni di carattere penale per i soggetti inadempienti. Dal DPS restano tuttavia escluse moltissime regole per la tutela dei dati sensibili necessarie alla sopravvivenza di un'azienda. La sua adozione non mette al riparo da rischi quali spionaggio industriale, furti di dati finanziari o di progetti di componenti industriali, contro i quali l'azienda dovrà comunque attrezzarsi.

---

Tutti gli aspetti considerati indicano una scarsa cultura informatica verso la sicurezza che impone, non soltanto al mondo dell'impresa, ma in prospettiva anche alla scuola, la necessità di educare alle regole di comportamento in Rete e di corretto utilizzo delle soluzioni informatiche. Sul fronte aziendale tale deficit potrà essere colmato soltanto affiancando alla formazione tecnica e manageriale, vere e proprie azioni di sensibilizzazione. Nell'era di Internet è fondamentale accettare che la sicurezza informatica travalica i confini fisici del proprio edificio, coinvolge l'educa-

zione e gli apparati dei soggetti con cui si viene direttamente o indirettamente a contatto, richiede specifiche conoscenze. Si deve acquisire la coscienza che la tecnologia, per quanto amichevole e utile, può essere impiegata anche a nostro danno, mettendo in pericolo i nostri cari e il nostro lavoro.

Si tratta quindi di un aspetto che non va delegato, ma che deve entrare a far parte del bagaglio culturale di ciascuno di noi. La tutela non deve arrivare dall'esterno ma diventare, per essere efficace, sempre più autotutela.

**INFORav**

Istituto per lo sviluppo  
e la gestione avanzata dell'informazione

Piazza Barberini, 52 - 00187 Roma

Pubblicazione in distribuzione  
gratuita ai soci ed in abbonamento

Redazione:

Piazza Barberini, 52 - 00187 Roma  
Tel. 06/88.81.21.26 - Fax 06/42.01.09.03

Autor. Trib. Roma n. 295 del 7 luglio 2003