

## Protezione dei dati personali: parola all'esperto

### Intervista rilasciata dall'Ing. Francesco Amendola ad Italia Imprese

Introduzione: Mai come oggi la sicurezza dei sistemi informativi e la protezione dei dati rappresentano un elemento cruciale nell'attività di un'azienda. Con la crescita esponenziale delle attività legate ad Internet, infatti, si è resa necessaria la massima allerta nei confronti di eventuali 'intrusioni'... Ma quali sono le misure di sicurezza minime che dovrebbe adottare un'azienda per proteggere i dati personali? Quanto costa risolvere in modo professionale il problema della sicurezza? Abbiamo rivolto queste ed altre domande all'Ing. Francesco Amendola, membro della Commissione Informatica e TLC dell'ordine Ingegneri di Roma e responsabile della sicurezza dei sistemi informativi per la Nextel Italia.

#### **Quale bilancio possiamo tracciare a due anni dall'entrata in vigore della nuova normativa sulla privacy?**

Premesso che la normativa a protezione dei dati personali esiste in Italia da circa dieci anni con la legge 675/96, il bilancio che si può trarre ad oggi non è certamente positivo. Questo perché sussiste nel nostro Paese una situazione di scarsa sensibilizzazione e sfiducia verso la tutela dei dati personali, sia da parte dei titolari dei trattamenti che da parte degli interessati. La visione che spesso si ha della privacy è quella di un obbligo formale, talvolta superfluo, piuttosto che un modello organizzativo che, se ben attuato, fornisce all'azienda un vantaggio competitivo.

#### **Quali sono gli adempimenti richiesti alle Aziende in materia di protezione dei dati personali aziendali?**

Entro il 31 marzo 2006 tutti i titolari di trattamenti di dati personali devono porre in essere le misure minime di sicurezza previste dal D.Lgs. 196/2003. In generale vi è l'obbligo di ridurre al minimo determinati rischi, quali ad esempio la perdita o la diffusione non autorizzata dei dati trattati, ed il dovere di adottare in ogni caso le misure minime previste. Per i titolari di trattamenti effettuati con strumenti elettronici, dunque tramite computer, è previsto, ad esempio, che si dotino di un sistema di autenticazione e autorizzazione informatica; che proteggano gli strumenti elettronici ed i dati rispetto a trattamenti illeciti, ad accessi non consentiti e a determinati programmi informatici; che implementino procedure per la custodia di copie di sicurezza e per il ripristino della disponibilità di dati e sistemi; infine che redigano annualmente un documento programmatico sulla sicurezza (DPS).

#### **Cosa comporta per un'Azienda l'obbligo di redazione del Documento Programmatico sulla Sicurezza (DPS) ?**

La redazione del documento programmatico sulla sicurezza (DPS) non termina con la produzione del documento stesso. Infatti dal nome si evince l'opportunità di programmare, quindi pianificare, gli interventi da porre in essere, in termini di adozione di misure di sicurezza, al fine di ridurre il rischio che minacce ed eventi

$$\Delta x \Delta p_x \geq \frac{\hbar}{2}$$

[www.ingamendola.com](http://www.ingamendola.com)

dannosi possano compromettere la liceità dei trattamenti di dati personali effettuati dall'Azienda. Dunque una volta analizzati i fattori di rischio ed individuati gli opportuni interventi mitigativi, bisognerà realizzare questi interventi secondo una programmazione che vede prioritarie le misure a contrasto dei rischi maggiormente incombenti sulla riservatezza, integrità e disponibilità dei dati. Così come non ha molto senso un DPS in cui tutti i rischi risultino sotto controllo, non ha neanche senso una programmazione degli interventi solo formale, che non trova poi un concreto riscontro nella realtà aziendale a cui è riferita.

### **Quali sono le misure minime operative di sicurezza che deve adottare un'Aziende per proteggere i dati personali aziendali nel rispetto delle normative vigenti?**

Una prima serie di misure riguarderà sicuramente il rafforzamento dei sistemi informativi dal punto di vista della sicurezza: quindi parliamo di un sistema operativo ed un software anti-virus costantemente aggiornati relativamente alle postazioni di lavoro; di firewall, di sistemi di intrusion prevention e detection (IPS/IDS), di reti private virtuali (VPN) relativamente all'infrastruttura di rete; di accesso ai computer con nome utente e password personali ed univoci per ogni utente; di accesso ai soli dati per cui si è incaricati del trattamento; di copie di sicurezza dei dati eseguite e verificate periodicamente; etc. A ciò però si aggiungono altre misure, di più difficile attuazione ma di maggior rilevanza, che riguardano le sensibilità degli utenti verso il problema sicurezza e la loro formazione e informazione a riguardo. Infatti i rischi maggiori per le Aziende vengono soprattutto dall'interno: un utente che non tutela la riservatezza della propria password, ad esempio, rischia di compromettere l'intero sistema di sicurezza implementato, al di là delle soluzioni tecnologiche adottate.

### **Esistono rischi per la sicurezza dei sistemi informativi aziendali in caso di utilizzo di nuove tecnologie, come il WIFI o il VoIP?**

Sicuramente esistono rischi intrinseci nelle tecnologie come la possibilità di violare in poche ore una rete senza fili Wi-Fi mediamente protetta oppure di ascoltare le chiamate VoIP che transitano sulla rete aziendale con strumenti reperibili gratuitamente su Internet. Tuttavia, ancora una volta, i rischi maggiori vengono dalla componente umana che implementa ed utilizza queste tecnologie. Infatti spesso per entrare in una rete Wi-Fi è sufficiente accendere un PC portatile con una scheda di rete senza fili e spostarsi per strada fino a che il sistema non segnala la presenza di una rete sprotetta nelle vicinanze: questo perché l'utente inconsapevole acquista il router wireless, lo accende, si accerta che funzioni in base alle sue esigenze di connettività e non fa null'altro per implementare tutti quegli accorgimenti che servono per rendere quanto meno vulnerabili possibili le soluzioni implementate, ricordando che il rischio zero non esiste. Per questo è importante la consapevolezza dei rischi esistenti legati alle diverse tecnologie adottate, in modo da ridurre al minimo gli impatti dannosi che potrebbero conseguire da una non corretta implementazione.

### **Costa molto per una piccola e media azienda mettere in sicurezza i propri sistemi informativi e rispettare la normativa sulla protezione dei dati personali?**

Il costo ovviamente è molto legato alla volontà dell'imprenditore di limitarsi ai soli adempimenti formali previsti dalla normativa, oppure di intraprendere il percorso di adeguamento dei propri processi aziendali agli

$$\Delta x \Delta p_x \geq \frac{\hbar}{2}$$

[www.ingamendola.com](http://www.ingamendola.com)

standard di sicurezza, partendo dai requisiti obbligatori per legge, ma certamente non arrendendosi là. Attualmente per la mera redazione di un DPS vengono richieste poche centinaia di euro da parte dei professionisti del settore a cui va aggiunto il costo delle soluzioni da adottare come misure, minime o idonee, di sicurezza per garantire trattamenti di dati leciti e corretti. Per poter realizzare invece un sistema completo di gestione della sicurezza delle informazioni vengono richieste cifre dell'ordine delle migliaia di euro solo per la consulenza organizzativa, restando esclusi i costi degli strumenti tecnologici adottati (es. server, software, firewall, IDS, etc.). C'è comunque da osservare che oggi i costi tecnologici si sono drasticamente ridotti, rendendo disponibili a molte tecnologie una volta ad appannaggio solo di pochi; inoltre avere un'azienda adeguata che non interrompa il proprio business al primo virus diffuso su Internet è certamente un vantaggio molto forte, che ben ripaga le spese sostenute.

### **Che consigli può dare ad un'azienda che volesse risolvere in modo professionale il problema della sicurezza?**

Occorre anzitutto trovare il giusto compromesso tra la propensione alla spesa verso la sicurezza dei sistemi IT, le aspettative sul ritorno degli investimenti (R.O.I.) e l'adozione di nuove tecnologie. In questa fase preliminare, così come in quelle successive di implementazione e verifica, è buona norma affidarsi ad una azienda specializzata con solide esperienze maturate non solo nel Networking ma anche in tutte le tecnologie emergenti basate su Internet come VoIP, VDSL, WIFI e VPN. In questo caso il vantaggio per il committente nasce dalla tutela e dalle garanzie che egli può avere da un lavoro svolto da un'azienda specializzata e caratterizzata professionalmente dalla presenza di ingegneri iscritti all'Albo, con competenze tecniche naturalmente non settoriali, che permettono di essere in grado di affrontare e risolvere qualsiasi tipo di problema si presenti.

L'ing. Francesco Amendola si è laureato in **Ingegneria Elettronica con Lode** presso l'Università degli Studi di Roma Tre ed è un laureato del **Collegio Universitario "Lamaro-Pozzani"**; è inoltre **relatore a convegni e seminari** sulle tematiche della sicurezza delle informazioni e della tutela della *privacy*. Attualmente ricopre la carica di **responsabile per la sicurezza della Nextel Italia s.r.l.** e precedentemente è stato funzionario addetto alla **sicurezza ICT ed alla protezione dei dati personali (D.Lgs. 196/03) presso la Pubblica Amministrazione**. Ha inoltre conseguito il **Master** in "*Tecniche di Management, Organizzazione e Gestione Aziendale*" presso la Helyos Executive Master Management ed il **Master** di II livello in "*Ingegneria ed Economia dell'Ambiente e del Territorio*" presso l'Università degli Studi di Roma Tre. Si segnala, tra le esperienze professionali di maggior rilievo, l'attività di consulenza prestata presso uno dei maggiori player del mercato delle telecomunicazioni mobili di terza generazione (**H3G s.p.a.**).

**Ing. Francesco Amendola**

[www.ingamendola.com](http://www.ingamendola.com)