

LA SICUREZZA ICT

Intervista al dott. Claudio Telmon

Quali sono le più frequenti ed insidiose minacce che provengono dal "cyber - crime" e quali misure minime di sicurezza dovrebbe attuare un'impresa ai fini della protezione dei dati?

Nel caso di impresa di medie dimensioni che non svolge attività particolarmente critiche si configurano essenzialmente problemi di due tipi: da una parte possono verificarsi tentativi di utilizzare il sistema informativo dell'azienda per svolgere attività fraudolente che rimangono nell'ambito dell'attività informatica, ad esempio per includerla in elenchi per lo svolgimento di attività di *spamming*; dall'altra, essendo sempre più diffuso lo svolgimento di attività di tipo finanziario, possono essere portati attacchi con lo scopo di acquisire le credenziali per l'accesso a servizi di *home banking* per poter poi svolgere operazioni.

Negli ultimi due anni si è notato che gli attacchi stanno diventando sempre più mirati, sono sempre meno volti a "far danni" in generale e sempre più finalizzati a svolgere attività di effettivo interesse per l'attaccante.

Anche la tipologia dei soggetti che compiono questi atti è cambiata, si è passati dall'hobbysta a veri e propri "professionisti" reclutati dalla criminalità organizzata. Ad esempio, a New York ci sono punti di accesso *wireless* pubblici, gratuiti, gestiti dalla criminalità organizzata, il cui unico scopo è acquisire le credenziali dell'utilizzatore.

Altra problematica di cui si parla molto è quella relativa ad attacchi che provengono da paesi tipo la Cina, in genere per avviare attività di *spamming* o sottrarre segreti industriali; mentre l'attività di acquisizione di sistemi per lo *spamming* può dirsi accertata, non sono stati ad oggi ancora provati atti di spionaggio industriale.

Esiste una normativa specifica per le PMI in materia di privacy e sicurezza?

No, non esiste una normativa specifica, non è prevista una semplificazione per le piccole imprese, perché l'attenzione non è posta sul tipo di impresa ma sui dati e sul tipo di trattamento.

Tuttavia, il Garante ha prodotto dei documenti che servono per una gestione semplificata della normativa: una *Guida operativa semplificata per redigere il documento programmatico sulla sicurezza* e una *Guida pratica e misure di semplificazione per piccole e medie imprese*. Probabilmente per molte piccole imprese anche quest'ultimo è un documento eccessivo, credo che un aiuto dovrebbe essere portato dalle associazioni di categoria ai propri associati. Lo scopo di questi due documenti è quello di assistere nell'interpretazione e applicazione della normativa, ad esempio attraverso *check list* mirate, ma ritengo che la terminologia utilizzata sia talvolta eccessivamente tecnica per la piccola impresa. Non concordo con quei consulenti in materia di sicurezza informatica che sono contrari a soluzioni preconfezionate per le imprese; io, al contrario, sono convinto che per le piccole imprese possano essere molto utili.

Quali sono le difficoltà per le PMI nell'affrontare il tema della sicurezza dei propri sistemi informativi?

Il mercato della sicurezza, di questo mi sono interessato ultimamente per CLUSIT, appare "bloccato", nel senso che è concentrato su alcune grandi città, in particolare Roma e Milano, e su 30-50 grandi imprese, mentre il nostro sistema produttivo, come noto, è fatto per la maggior parte di imprese medie e piccole.

Le piccole imprese incontrano due diversi ordini di difficoltà.

La prima deriva dalle loro limitate dimensioni, nel senso che chi gestisce in prima persona l'impresa non ha spazio nella sua testa per aggiungere un problema in più, quello della sicurezza informatica. Anche sotto questo aspetto, le imprese dovrebbero poter contare su un aiuto concreto da parte delle associazioni a cui sono iscritte. Inoltre c'è un problema di formazione, duplice: da una parte, è vero che le imprese hanno bisogno di formazione, dall'altra è anche vero che chi eroga formazione per la sicurezza è abituato ad erogarla per le grandi imprese, quindi la difficoltà sta nell'entrare nell'ordine di idee della piccola impresa. La piccola impresa non ha bisogno di una semplificazione o banalizzazione di quello che si fa per le grandi imprese, ma ha bisogno che i concetti siano riportati nella sua realtà. Se in una grande impresa servono venti ruoli diversi, in una piccola impresa non si possono caricare tutti quei venti ruoli su una singola persona, ma bisogna ragionare su come è strutturata quella impresa e fornire una soluzione adeguata.

L'altro problema che hanno le piccole imprese deriva dal fatto che non hanno competenze interne, ma quasi sempre si appoggiano a fornitori esterni, che spesso

sono poco preparati, ma soprattutto sono poco propositivi. Il fornitore si limita a soddisfare le richieste dell'azienda, ma l'azienda non sa bene cosa deve chiedere; inoltre, il fornitore informatico della piccola impresa deve necessariamente essere un generalista, un "tuttofare", per cui può non avere le competenze specifiche necessarie per risolvere un determinato problema.

Quali sono i rischi connessi all'utilizzo di tecnologie *wireless* e quali strumenti per la sicurezza dovrebbero essere adottati?

Il *wireless*, come molti sapranno, è una tecnologia che consente a qualsiasi computer che si trovi nell'area coperta di connettersi ad una rete, anche interna, di una azienda. I rischi sono di due tipi.

Il primo riguarda l'utilizzo del *wireless* in azienda. Da questo punto di vista l'esigenza è avere dei buoni meccanismi di autenticazione sull'*access point*, cioè sul *router* che dà l'accesso al *wireless*, che normalmente per una piccola impresa è il *router ADSL* con cui si connette anche a internet. Tutti gli apparati moderni offrono dei meccanismi di autenticazione sufficientemente robusti, fermo restando che va comunque sempre evitata l'autenticazione *WEP*, perché ha un difetto congenito ed è violabile. Lo svantaggio è che ogni singola macchina deve essere configurata per l'autenticazione, ma d'altra parte è ovvio che se così non fosse chiunque potrebbe accedere.

L'altro problema è legato all'utilizzo di connessioni *wireless* quando si è fuori dall'azienda, ad esempio in viaggio per lavoro, e si utilizza la connessione dell'albergo. Spesso queste connessioni non sono adeguatamente protette, nel senso che da parte di chi fornisce l'accesso c'è sempre una certa cura nell'evitare l'accesso a chi non paga, ma molto meno nel cercare di evitare possibili intercettazioni fra macchine. In questi casi è quindi essenziale assicurarsi, ad esempio per attività di *web mail*, che la connessione che si intende utilizzare sia "sicura", cioè *https*.

Quali raccomandazioni si sente di formulare agli utilizzatori di *smart card* per l'apposizione della *firma digitale*?

Il problema principale non è assolutamente tecnico. E' bene rendersi conto che la *smart card* permette di apporre una firma che è in tutto e per tutto equivalente a quella manuale e che pertanto dare ad un'altra persona la propria *smart card* equivale a darle il proprio potere di firma. Come noto, nel caso di imprese medio piccole molto spesso la *smart card* è consegnata al commercialista: questo, oltre a non essere

proprio corretto dal punto di vista delle procedure, attribuisce davvero troppo potere ad un altro soggetto.

Un altro problema sta nel fatto che, per quanto la *smart card* costituisca uno strumento che ha delle notevoli caratteristiche dal punto di vista della sicurezza, neanche una *smart card* è in grado di proteggerci se il nostro computer è stato compromesso. Se nel nostro computer si è insinuato un programma che attribuisce il controllo a qualcun altro, è vero che questo soggetto non riuscirà ad estrarre le credenziali dalla *smart card* per utilizzarle altrove, però sul nostro computer potrà utilizzare la nostra *smart card*, quando inserita, per effettuare operazioni apponendo la nostra firma. In definitiva, anche se sembra paradossale, per una piccola impresa l'attenzione maggiore dovrebbe essere posta sulla sicurezza del computer non del titolare, ma della segretaria o della persona che si occupa dell'amministrazione, quando è attraverso quel computer che si trattano i dati personali, si tengono i rapporti col commercialista, si svolge attività di *home banking* e così via.

Claudio Telmon è consulente nel campo della Sicurezza ICT.

Membro del Comitato Direttivo di CLUSIT (Associazione Italiana per la Sicurezza Informatica).

Socio fondatore e membro del Comitato Direttivo di AIPSI (Associazione Italiana Professionisti della Sicurezza Informatica).