PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 954 di venerdì 05 marzo 2004

Internet, posta elettronica e privacy: esigenze di sicurezza e comportamenti a rischio (1/2)

A cura del Dott. Gerardo Costabile - Iacis member. "Non c'è insicurezza maggiore che un presuntuoso senso di inviolabilità, oppure la sottovalutazione dei rischi..."

[Pubblichiamo oggi l'estratto dell'intervento del dott. Gerardo Costabile ? Member of "The International Association of Computer Investigative Specialists" - durante la conferenza "Privacy e studi legali", svoltasi a Verona il 27 febbraio 2004.]

Paradossalmente, lo scopo principale della mia presenza qui, non è quello di fornire risposte adeguate, ma far nascere dei dubbi, accrescere la consapevolezza che è necessaria una nuova mentalità per incrementare la sicurezza. Non c'è insicurezza maggiore che un presuntuoso senso di inviolabilità, oppure la sottovalutazione dei rischi, pensando di non essere un target appetibile o di non detenere dati particolarmente riservati.
Di contro, invece, la sicurezza è assimilabile ad un processo, non ad un prodotto. La forza della lunga chain of security sarà strettamente legata alla forza dell'anello più debole, che è quasi sempre l'uomo.
La nostra sicurezza e riservatezza sono strettamente ed indissolubilmente legate a quelle degli altri nostri interlocutori. Non è necessario un vero e proprio attacco informatico, ma sarebbe sufficiente un banalissimo virus informatico per compromettere la riservatezza di una confessione di un nostro amico ricevuta via posta elettronica. Peggio ancora se il computer fosse usato per attività professionali, dove il nostro Hard disk è di sovente lo scrigno di molti dati particolarmente riservati, stante anche il legame fiduciario del professionista con il proprio cliente.

Molte sono le sottovalutazioni, spesso giustificate da una scarsa informazione e da un basso livello di conoscenza dello strumento informatico e delle relative applicazioni. Anche un semplicissimo file di Office contiene molti dati, in funzione di quelli forniti durante l'installazione. Basta poco, anche un semplice salvataggio in altri formati, o l'utilizzo di apposite utility, per evitare ciò.
Un particolare riferimento, poi, ai programmi di sharing (tipo Kazaa, Winmx, Emule, etc.), dove in nome di una condivisione di gusti (spesso musicali) ci si ritrova a condividere ?più o meno coscientemente- anche altre risorse, talvolta di natura professionale se il personal computer è utilizzato in maniera promiscua.

Il punto debole, quindi, con l'accrescere prepotente della tecnologia e della sicurezza dei sistemi, appare sempre di più quel "piccolo" uomo, schiacciato da sé stesso e dai suoi errori.
La tecnica utilizzata, perciò, per ingannare ed aggirare con la psicologia i processi di sicurezza, prende il nome di "social engineering". L'ingegnere sociale è colui il quale, con particolare astuzia, riesce ad arrivare dove è difficilmente possibile con i normali strumenti di intrusione informatica, spingendo la vittima o un suo collaboratore, tramite espedienti principalmente psicologici, a rivelare informazioni apparentemente irrilevanti, ma che consentiranno un accesso abusivo, una frode o altre premeditate attività illecite (ad esempio inducendo l'utente ad autoinfettarsi con un trojan).
Le "tendenze base" della natura umana che vengono coinvolte in un tentativo di social engineering sono molteplici. Le più importanti, principalmente per le attività di diffusione dei virus, sono due: l'autorevolezza e l'ignoranza.
Per quanto concerne il primo aspetto sono numerosi i casi registrati in cui un semplicissimo messaggio di posta elettronica, ad esempio a nome di una software house oppure di un più "istituzionale" ufficio dell'FBI, abbia indotto l'utente ordinario, in particolare soggezione psicologica, ad installare un allegato infetto, ad esempio indicato come un nuovo aggiornamento del programma. In questi casi è palese la tecnica di falsificazione del mittente del messaggio di posta elettronica sfruttando, comunque, anche la seconda "debolezza": l'ignoranza. Infatti l'impossibilità di conoscere ogni recondita tecnica informatica ed ogni angolo della rete Internet, consente all'aggressore di confezionare con una certa facilità un messaggio apparentemente serio e affidabile, particolarmente tecnico nel lessico e quindi spesso incomprensibile, nonché efficace.

Il rischio più elevato per la riservatezza e per l'integrità dei nostri dati è proprio la subdola "infezione virale": l'attacco dei "Malware". La parola "Malware" deriva dalla fusione di "Malicious" e "Software". Questa macrocategoria racchiude le famiglie di Virus veri e propri, Worm e Trojan.
Le "antologie informatiche" forniscono numerose definizioni, più o meno appropriate, del fenomeno e delle terminologie utilizzate. La definizione che desidero invece utilizzare è quella del Codice Penale, perché poi è in tale ambito che ci si dovrà confrontare nel caso di abusi. Il malware è "un programma informatico... omissis..., avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi un esso contenuti o a esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento".
Il canale di infezione più utilizzato e quindi più "remunerativo" è la posta elettronica, che registra anche un forte incremento nell'ultimo anno 2003.
Tra i programmi della stessa macroarea si segnala anche il "Trojan Horse" (ovvero il c.d. "Cavallo di Troia") il quale, nascosto in un apparente innocuo programma o una fotografia, consente all'untore di controllare o registrare informazioni della vittima operando direttamente sull'hard disk di quest'ultimo a distanza. I Trojan vengono generalmente riconosciuti sia dagli antivirus che dai firewall (*), anche se vengono utilizzate speciali utility ad esempio per inglobare il virus in coda al programma originale oppure nascondendo le estensioni dei file. In pratica il file "caio.jpg.exe" (in realtà un eseguibile), verrà visualizzato come un più innocuo "caio.jpg" (un formato per le fotografie digitali), ma con un'icona tipica dei programmi eseguibili.
Lo scopo è molteplice: potrebbero interessare file dati (comuni, personali, sensibili, giudiziari), fotografie, numeri di carte di credito, password d'accesso, documenti personali. Un altro motivo spesso riscontrato è quello di creare una macchina "zombie", pronta ad obbedire ai comandi dell'attaccante e quindi sferrare ulteriori attività delittuose ai danni di terzi, che "leggeranno" l'azione come proveniente dalla vittima del Trojan e non dal reale attaccante.
E' palese che, anche se l'attività fosse frutto di un gioco, come spesso accade, il sistema risulterebbe evidentemente vulnerabile ad eventuali successivi attacchi di reali malintenzionati.
Nelle aziende e negli studi professionali l'approccio al problema della proporzionalità tra uso della posta elettronica ed esigenze di sicurezza informatica è fortemente dibattuto.
Certamente l'importante è una buona policy, da rispettare a partire dalle funzioni apicali della struttura interna, dove siano definite regole e responsabilità. Sarà necessario proteggere il sistema informatico interno da virus che possano compromettere l'intera rete dello studio, guardando oltre i 6 mesi (quasi ridicoli) dell'imposizione ex lege. Dovranno essere protetti i dati e informazioni confidenziali, più che i singoli personal computer: evoluzione, peraltro, che la stessa legge ha fatto dal '96 ad oggi. Il costo che si può pagare è molto alto, non solo per le sanzioni, ma per i danni economici, le responsabilità ex art. 2050 cc, le conseguenti perdite di immagine e reputazione.
A questo punto vi lascio con una provocazione: ma è davvero indispensabile il "Documento programmatico della sicurezza"? E' davvero necessaria una imposizione ex lege, che peraltro non è nuova ma risale al 1999?

[La seconda parte dell'articolo sarà pubblicata sul numero di lunedì 8 marzo]

---

www.puntosicuro.it