PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3735 di mercoledì 09 marzo 2016

Social engineering: che significa?

L'informatica, e soprattutto il crimine informatico, offre occasione per sviluppare in continuazione nuove espressioni: una nuova tecnica di attacco. Di Adalberto Biasiotti.

Non credo valga la pena di tradurre questa espressione, perché "ingegneria sociale" mi sembra davvero ridicola.
La **social engineering** è un tipo di attacco che consiste nell'ingannare qualcheduno, ad esempio un navigatore Web, inducendolo a violare le normali procedure di sicurezza.
Il malvivente sviluppa una serie di trucchi, che fanno appello alla vanità del navigatore, oppure al suo rispetto dell'autorità od infine ancora ai suoi istinti fraudolenti, inducendo il soggetto attaccato a comportarsi in maniera impropria.
Nello stesso quadro va inserito anche una tecnica esattamente contraria, che è quella di sollecitare il navigatore ad aiutare un collega in difficoltà, stimolando quindi i suoi istinti positivi, invece di quelli negativi.

Le tipologie di attacco sono talmente numerose che occorre elencarle successivamente per punti:
? **Baiting**: questa tecnica di attacco fa riferimento ad un malvivente che lascia uno strumento informatico, come ad esempio una memoria USB, in un luogo ove egli è certo che il soggetto attaccato potrà trovarla. Il soggetto attaccato è tutto contento perché si è trovato in possesso, gratuitamente, di questa chiavetta USB e non vede l'ora di utilizzarla, infettando così inavvertitamente il proprio computer.
? **Phishing**: questa pressione, ormai ben nota, consiste nell'inviare un messaggio di posta elettronica fraudolento, mascherandolo come un messaggio legittimo; spesso il messaggio sembra essere stato inviato da un soggetto, con cui il navigatore attaccato ha già un rapporto regolare, come ad esempio la propria banca. Il messaggio induce il soggetto attaccato a condividere alcune informazioni riservate o cliccare su un link, che immediatamente installa del malware.
? **Spear phishing**: si tratta di una forma più raffinata dell'attacco precedente, che è mirato ad attaccare specifiche categorie di persone, nei confronti delle quali l'attaccante ha approfondite conoscenze.
? **Pretexting**: questo tipo di attacco si realizza quando l'attaccante esige di conoscere dati personali o finanziari del soggetto attaccato, per consentirgli l'accesso a specifiche risorse od informazioni privilegiate.
? **Scareware**: ricordo che in lingua inglese "to scare" significa spaventare. Questo tipo di attacco consiste nell'ingannare la vittima, facendogli credere che il suo computer è stato infettato da un virus o che ha scaricato, seppur inavvertitamente, del materiale proibito, che potrebbe comportare l'avvio di azioni legali.
L'attaccante offre una soluzione a questo problema ma in realtà la soluzione consiste in un programma fraudolento che inquina in vario modo il computer del soggetto attaccato.

A questo proposito, gli esperti di sicurezza raccomandano che gli addetti alla sicurezza informatica non solo effettuino regolarmente dei controlli sulla presenza di questi tipi di attacchi, ma che educhino anche il personale coinvolto nella gestione del sistema informativo, educandolo a ignorare questo tipo di attacchi o, meglio ancora, a segnalarli al responsabile della sicurezza informatica.
Purtroppo oggi si dedica assai più tempo ad educare gli addetti alla gestione sistema informatico su procedure informatiche vere e proprie, che non su queste sempre più evolute raffinate tecniche di attacco.

Adalberto Biasiotti

www.puntosicuro.it