SICUREZZA INFORMATICA

MINACCE

Come evitare gli attacchi di *phishing* e *Social Engineering*

Ver.1.0, 19 febbraio 2015

Pagina lasciata intenzionalmente bianca

1. CHE COSA È UN ATTACCO DI *SOCIAL ENGINEERING*?

In un attacco di *Social Engineering* viene utilizzata l'interazione umana (competenze sociali) per ottenere o compromettere informazioni su un'organizzazione o sui suoi sistemi informatici. Spesso il malintenzionato si presenta nelle vesti di un nuovo dipendente, un addetto alle riparazioni o un ricercatore, offrendo alla vittima dell'attacco credenziali attendibili per dimostrare la millantata identità. Una volta ottenuta la sua fiducia e usando domande adeguate, può essere in grado raccogliere informazioni sufficienti per infiltrarsi nella rete dell'organizzazione. Nel caso non riesca ad ottenere immediatamente informazioni sufficienti dalla prima vittima, l'attaccante può contattare un'altra fonte all'interno della stessa organizzazione e per mezzo delle informazioni precedentemente raccolte, rendersi più credibile alle nuove vittime così da raggiungere il proprio scopo.

2. CHE COSA È UN ATTACCO DI *PHISHING*?

Il *phishing* è una forma di *Social Engineering*. Normalmente gli attacchi di questo tipo utilizzano Email o siti Web dannosi per ottenere informazioni personali fingendosi un'organizzazione affidabile. Ad esempio, il malintenzionato può inviare una Email, apparentemente provenienti da società che gestiscono carte di credito o da istituti finanziari, per richiedere informazioni sull'account della vittima con la scusa che sono stati rilevati problemi nella gestione delle transazioni. Se la vittima risponde fornendo le informazioni richieste, queste possono essere utilizzate per ottenere l'accesso all'account.

Gli attacchi di *phishing* possono presentarsi anche come provenienti, in modo ingannevole, da enti di beneficenza. In questo caso i malintenzionati fanno partire gli attacchi approfittando degli eventi di cronaca e durante specifici periodi dell'anno, come ad esempio catastrofi naturali; epidemie e pericoli per la salute; preoccupazioni economiche; importanti elezioni politiche; festività.

Una tecnica simile, detta *vishing*, sfrutta invece i servizi di telefonia dove i truffatori simulano una chiamata proveniente da un call center chiedendo al "cliente" i propri dati ed altre informazioni personali.

Diversamente dalla truffa via Email, il malintenzionato conta sulla maggiore fiducia che viene riposta quando l'essere umano si relaziona direttamente con un operatore apparentemente autorizzato a richiedere e trattare tali informazioni.

3. COME EVITARE DI ESSERE UNA VITTIMA?

Seguendo delle semplici regole di comportamento è possibile evitare di diventare vittima di attacchi di *Social Engineering* e/o *phishing* e di tutte le conseguenze derivanti dalla compromissione delle credenziali di accesso alle informazioni personali e sensibili.

L'elenco che segue non intende essere esaustivo ma rappresenta una buona prassi per l'educazione dell'utilizzatore agli aspetti della sicurezza informatica.

- Diffidate di chiamate telefoniche non richieste, visite o messaggi Email da persone che fanno domande sui dipendenti o su altre informazioni interne. Se un individuo sconosciuto sostiene di far parte di un'organizzazione legittima, verificate la sua identità direttamente presso quell'organizzazione.

- Non fornite informazioni personali o che riguardano la vostra organizzazione, incluse quelle sull'organigramma e la rete aziendale, se non siete sicuri che la persona che ve le chiede abbia l'autorità per farlo.

- Non rivelate informazioni personali o finanziarie nelle Email, e non rispondete a messaggi che sollecitano l'invio di tali informazioni anche per mezzo di link inclusi nel messaggio.

- Non inviate informazioni sensibili tramite Internet prima di aver controllato la sicurezza e l'attendibilità del sito web.

- Controllate con attenzione l'indirizzo (URL) di un sito web. Molti siti web dannosi sembrano identici a siti legittimi, ma spesso il loro URL è scritto con una differenza ortografica o con un dominio diverso (es.: ".com" invece che ".it").

- Se non siete sicuri della legittimità di una Email di richiesta informazioni, eseguite una verifica contattando direttamente l'azienda che appare come mittente e non utilizzate le informazioni di contatto presenti nella Email o nel sito web di riferimento, ma ricavatele da segnalazioni precedenti. Informazioni su attacchi di *phishing* noti sono facilmente reperibili tramite i motori di ricerca.

- Evitate di aprire allegati o cliccare su link di dubbia provenienza e non eseguite software non conosciuti e la cui legittimità sia dubbia.

- Installate e mantenete aggiornati *software*, *firewall* e filtri di posta elettronica anti-virus così da ridurre una buona parte di questo tipo di attacchi.

- Sfruttate le funzioni anti-*phishing* offerte dal *client* di posta elettronica e dal browser che utilizzate.

4. COSA FARE SE PENSATE DI ESSERE UNA VITTIMA?

Anche se si seguono le indicazioni illustrate precedentemente è possibile cadere nelle trappole che i malintenzionati costruiscono in modi sempre più ingegnosi e credibili.

Nel caso abbiate la sensazione di essere caduti vittima di attacchi di *Social Engineering* e/o *phishing* potete intraprendere alcune azioni allo scopo di mitigare le conseguenze del furto delle vostre credenziali.

- Se credete di aver rivelato informazioni sensibili sulla vostra organizzazione, segnalate l'accaduto ai responsabili della sicurezza interna e agli amministratori di rete in modo da allertare la struttura su eventuali attività insolite o sospette.

- Se credete che i vostri conti finanziari possano essere compromessi, contattate immediatamente la vostra banca e chiudete qualsiasi account che potrebbe essere stato compromesso. Controllate eventuali spese non riconducibili ai vostri normali movimenti.

- Cambiate immediatamente qualsiasi password potreste aver rivelato. Se è stata utilizzata la stessa password per più risorse, assicuratevi di cambiarla per ogni account, e non utilizzare la stessa password in futuro.

- Controllate qualsiasi altra evidenza di furto della vostra identità.

- Considerate una eventuale segnalazione dell'attacco alle autorità di polizia.

5. RICORDATE

Non fornite mai informazioni personali e sensibili a nessuno a meno che non si sia sicuri della sua identità e del fatto che abbia il permesso di accedere a tali informazioni.