** **

**Master Universitario di II Livello in “Homeland Security Sistemi, metodi e strumenti per la security e il crisis management”VII edizione (A.A. 2014/2015)**

**Candidato: Dott. D’Aliesio Matteo**

**Titolo: Il Social Engineering, Il fattore umano nella cyber security**

**ABSTRACT**

Nella sicurezza informatica, firewall e protocolli di criptazione sembrano non essere più sufficienti a fornire un’adeguata protezione da minacce e vulnerabilità aziendali, questo non solo perché il rischio zero è impossibile, ma anche perché negli anni si è andato sempre più diffondendo da parte di malintenzionati l’uso di strategie alternative e più economiche per sottrarre importanti dati aziendali.

Una di queste strategie è il Social Engineering o Ingegneria Sociale che, grazie all’utilizzo di tecniche psicologiche molto avanzate, riesce a sottrarre a persone/organizzazioni informazioni riservate o sensibili, che comunque non dovrebbero essere a disposizione di soggetti terzi all’azienda.

Nello specifico, l’ingegneria sociale fa ricorso a tecniche di persuasione (prima utilizzate dai soli operatori del marketing) che sfruttano bisogni ed emozioni connaturate in ogni persona.

Yarix, è una società italiana leader nella sicurezza informatica con sede in Montebelluna, tra i suoi numerosi compiti vi è anche il contrasto del Social Engineering.

La società, nel mese di settembre, ha ricevuto dall’impresa beta (un azienda di grandi dimensioni, denominata beta per motivi di riservatezza), l’incarico di verificare, tramite una campagna di Social Engineering, eventuali falle di sicurezza nella gestione del sistema informatico aziendale.

La campagna ha previsto un mio attivo coinvolgimento e si è articolata in 4 fasi.

1 Fase: Ricerca di dati e di vulnerabilità

La prima fase si è occupata di sondare la presenza e la visibilità aziendale nel mondo web, ricercando al contempo dati pubblici con elementi di possibili vulnerabilità (verbali di riunioni, accordi sindacali, organigramma, rapporti economici con fornitori e subfornitori, documenti programmatici, bilanci, firme in calce).

2 Fase: Preparazione mail phishing e invio

La seconda fase ha riguardato la raccolta di elementi utili alla creazione della mail di phishing. Una volta effettuata la stessa, si è poi provveduto all’invio delle mail di phishing agli indirizzi acquisiti.

3 Fase: Preparazione scenario telefonico e intrusione

Nella terza fase, si è creato una sorta di canovaccio, che servisse come bussola e punto di riferimento per le successive intrusioni telefoniche.

Le telefonate hanno cercato di far rivelare al ricevente le username e le password di accesso di alcuni terminali aziendali.

4 Fase: Verifica risultati e report aziendale

L’ultima fase è servita per analizzare i risultati e comunicarli all’azienda.