Ingegneria sociale: il Fattore Umano!

La *cyber security* è un problema costante per il mondo intero, *intruders* attaccano grandi corporazioni e società con l'intenzione di accedere a risorse private e di dominio non pubblico. Un report della *"CSI Computer Crime and Security Survey"* ha dichiarato che nell'anno 2010-2011 almeno la metà degli intervistati ha sperimentato un incidente informatico, e il *45,6 % di loro* è stata vittima di un *attacco informatico mirato*.
Se si affronta il problema solamente dal punto di vista tecnico, ignorando il livello fisico-sociale degli eventi, non si potrà mai risolvere la situazione al 100%.

Scene prese dai film come *"hackers"* in cui si vedono i ragazzi in una azione di "*dumpster diving"* alla ricerca di informazioni finanziarie stampate e cestinate, oppure in "*war game*" dove *Matt Broderick* studia attentamente il suo target prima di provare il crack delle password dei sistemi militari, ci mostrano che L'ingegneria *sociale* è una minaccia *sottovalutata* dalla maggior parte delle organizzazioni, ma può essere facilmente exploitata in quanto entra in gioco la *psicologia umana* piuttosto che le *barricate tecnologiche* che circondano l'intero sistema.

Qui un esempio "classico":

"una persona riceve una e-mail nella propria casella di posta dove si dichiara che il proprio computer è stato infettato da un virus. Il messaggio fornisce un link da cui scaricare un tool per la rimozione del malware. La persona evidentemente confusa clicca sul link e scarica il tool, inconsapevole del fatto di aver garantito un accesso ad un attaccante."

Per garantire la sicurezza di una organizzazione dai *fattori interni ed esterni*, il consulente della sicurezza deve conoscere completamente il *ciclo di un attacco di ingegneria sociale*, come le tecniche comunemente utilizzate da un attaccante e le *relative contromisure* da adottare in caso di attacco per ridurne la buona riuscita dello stesso.

Definizione di Ingegneria Sociale:

Il significato di ingegneria sociale può essere definito in vari modi, wikipedia la definisce come *"... l'arte di manipolare le persone in modo che compiano azioni oppure che forniscano informazioni confidenziali."*

Altri autori forniscono altre definizioni *"un hacker usa trucchi psicologici su utenti legittimi di un sistema, in modo da ottenere informazioni che gli consentano di guadagnare l'accesso a tali sistemi" "La pratica di aggirare qualcuno, sia di persona usando un telefono, o un computer, con l'espressa intenzione di irrompere in qualunque livello di sicurezza sia personale che professionale" "L'ingegneria sociale è un tipo di attacco non tecnico, basato particolarmente sull'interazione umana che spesso inganna il bersaglio inducendolo a superare le normali procedure di sicurezza" "un attaccante usa skills sociali e interazione umana per acquisire informazioni su una organizzazione o sui suoi sistemi".*

In realtà l'I.S è tutte quante queste definizioni. Noi possiamo definirla come la *manipolazione della caratteristica tendenza umana a fidarsi e di rilasciare informazioni sensibili per acquisire l'accesso ad un sistema da parte di un hacker. L'ingegneria* sociale non prevede particolari competenze informatiche, chiede però una grande dimestichezza *nell'uso del linguaggio* e particolare attenzione all' *interazione umana*. Un hacker che spende moltissime ore nel tentativo di *rompere* una password, può risparmiare un sacco di tempo chiamando l'impiegato di una organizzazione, spacciarsi per un *helpdesk* o un *impiegato IT*, e *chiederla direttamente a lui/lei*.

Ciclo di vita dell'I.S.

Ogni attacco di I.S è unico, ma con una piccola comprensione della situazione incontrata possiamo facilmente definire un ciclo di tutte le attività che un progetto di I.S attraversa nel corso del suo svolgimento. Possiamo rappresentare un ciclo di vita dell'I.S. in 4 grandi fasi:

FOOTPRINTING

STABILIRE CONTATTO

MANIPOLAZIONE PSICOLOGICA

USCITA

1) Footprinting: è una tecnica utilizzata per raccogliere informazioni sul target e *"l'ambiente"* circostante. Il footprinting può rivelare *gli individui* del target con cui un attaccante dovrà cercare di s*tabilire un rapporto/relazione*, in modo da aumentare le possibilità di riuscita dell'attacco. La raccolta di informazioni durante la fase di Footprinting include ma non si limita a:

- Lista degli impiegati con nome e n° di telefono
- Carta dell'organizzazione
- Informazioni sui dipartimenti
- Informazioni sulla locazione

Il footprinting viene generalmente definito come una *fase di pre-attacco*, cioè azioni che si compiono prima di un attacco di I.S. Alcuni tool come *creepy, SET, Maltego* possono aiutare in questa fase.

2) Stabilire un contatto: una volta che il *possibile target* è stato individuato, l'attaccante dovrà cercare di stabilire un contatto con esso. Generalmente il target è un *impiegato* o qualcuno che *lavora all'interno* dell'organizzazione, e con lui si deve *instaurare un buon rapporto*. La confidenza che l' ingegnere sociale sta guadagnando sarà usata successivamente per svelare informazioni confidenziali che possono causare gravi danni.

3) Manipolazione psicologica: in questa fase l'ingegnere sociale *manipola la confidenza* e il rapporto instaurato nella fase precedente in modo da estrarre più *informazioni possibili* o ottenere informazioni sulle operazioni *"sensibili"* che l'impiegato compie sui sistemi in modo da *penetrarli* più facilmente in seguito. Una volta che tutte le informazioni sensibili sono state raccolte, l'attaccante può muoversi verso il target successivo oppure *exploitare il sistema attualmente esaminato.*

4) Uscita: ora, dopo che sono state estratte tutte le informazioni necessarie, l'attaccante deve compiere una *"uscita pulita"* in modo da non attirare su di se *inutili sospetti*. Ci si deve assicurare che non siano rimaste *prove della sua visita* che possono ricondurlo alla sua vera identità oppure collegarlo in qualche modo ad una *intrusione non autorizzata* sul sistema preso come target.

Il comportamento umano

Ogni ingegnere sociale si concentra su tratti comportamentali specifici del target in esame in modo da estrarne più informazioni possibili. Questi tratti comportamentali includono ma non si limitano a:

- **Eccitamento per una vittoria:** Il sig. X riceve una mail in cui viene informato della *vincita di 1 milione* di dollari, controlla il documento in allegato e inoltra una mail all'indirizzo xxxxx@yyyy.com. Seguendo le istruzioni che riceverà per e-mail *dovrà disattivare l'antivirus* in quanto potrebbe causare problemi al download, dovuto al fatto che il documento *è firmato digitalmente con una forte cifratura*. Preso dall'eccitazione, esegue *diligentemente* le istruzioni, *disattiva l'AV*, scarica il documento cifrato ma all'apertura lo trova *danneggiato*. Inutile dire che in questo modo ha *scaricato un malware* sulla propria macchina che concede al mittente della mail un *accesso remoto* al proprio sistema.

- **Paura delle autorità:** Alcune persone sono *intimidite* alla presenza di persone che percepiscono come una *figura autoritaria*, non tanto dalla persona in se, ma piuttosto *dalla posizione e dal potere*. L'attaccante si attribuisce un ruolo di *figura autoritaria*, come un poliziotto, un avvocato, un dottore o qualcuno che ha potere all'interno della compagnia in modo da estrarre *informazioni dalla vittima*.
- **Desiderio di essere utili:** Keith A. Rhodes, capo tecnologo presso U.S. General Accounting Office, il quale ha un mandato dal congresso per testare la sicurezza delle reti in 24 differenti agenzie governative e dipartimenti ha dichiarato in una sua intervista che "*Le società istruiscono i propri dipendenti ad essere servizievoli, ma difficilmente li istruiscono ad essere parte del processo di sicurezza. Usiamo la connessione tra le persone e il loro desiderio di essere utili*". Le persone nel loro desiderio di essere utili e di risolvere le richieste di altri, forniscono molte informazioni che altrimenti non dovrebbero essere fornite ad un estraneo, questo fornisce ad un attaccante la possibilità di ottenere un accesso non autorizzato sul sistema target causando possibili perdite.
- **Paura di una perdita:** Il sig. X riceve una mail in cui viene indicato come il *vincitore* di una grossa somma di denaro, prima di ottenere tale somma *deve depositare $ 75.000* sul conto n° XXX-YYY-ZZZ, in caso contrario entro 10 giorni dalla ricezione della mail *se non dovesse depositare* la somma, la vincita verrà dichiarata non reclamata e quindi verrà estratto *un altro vincitore*. Il sig. X per paura di poter perdere tale opportunità, effettuerà il deposito sul conto fornito. Quando in futuro non riceverà più mail di risposta, e nessuna vincita accreditata sul conto, si accorgerà di essere stato *raggirato*.
- **Pigrizia:** Tutti noi abbiamo intrapreso lavori che ci consentivano solo un *limitato numero di azioni* senza la possibilità di trovare altri modi per compiere tali attività. Questo *causa noia* nelle persone che compiono il medesimo lavoro r*ipetutamente e quotidianamente*, si imparano così delle *scorciatoie* per fare i compiti con sforzi minimi e comunque ottenere il *raggiungimento* degli obiettivi. Tali individui *diventano pigri* e il loro *atteggiamento rilassato* verso il lavoro li rendono *target sensibili* in quanto potrebbero *rivelare informazioni* senza troppa *fatica.*
- **Ego:** a volte un attaccante cerca di rendere l'obiettivo più *emotivamente sicuro* di se stesso/stessa e perciò questo abbassa *inconsapevolmente le difese logiche*, nascondendo il fatto che un attacco sta per essere messo in atto. Il risultato è che tale persona *non si allarma* del fatto che è in corso un hack, fornendo all'attaccante *ciò che vuole.* La ragione per cui un simile attacco ha successo è che l'hacker è *ricettivo, ascolta ed esalta le conoscenze del target*. Si invoglia il target a *mettere in mostra* le proprie conoscenze, che di fatto sono le *informazioni* di cui noi *abbiamo bisogno.*
- **Insufficiente conoscenza:** la conoscenza del sistema target è uno dei fattori principali che *differenziano* l'attaccante da un qualsiasi impiegato dell'organizzazione. A volte, dovuto ad una *carenza di preparazione*, gli impiegati stessi non si sentono *sicuri delle proprie conoscenze* in merito al proprio lavoro/prodotto e quindi un ingegnere sociale tenta di prendere vantaggio da questa situazione creando *un senso di urgenza*, non concedendo all'impiegato molto tempo per *pensare e capire* che di fatto sono *sotto attacco.*

Le armi di un ingegnere sociale

La vecchia moda di *irrompere* in un sistema con un attacco di *"forza-bruta*" sul login di un utente è stata *sostituita* da metodi sofisticati che *non solo* sono più semplici, ma che portano *risultati migliori* e più velocemente, e che sono basati sulla *psicologia umana*. Questi attacchi aiutano un attaccante ad ottenere un *accesso* su sistemi *indipendentemente* dalla piattaforma, software o hardware utilizzato.

Qui c'è una lista delle tecniche *più popolari* usate per svolgere un attacco di I.S:

SHOULDER SURFING (*spiare da dietro le spalle*)

DUMPSTER DIVING *(frugare tra la spazzatura)*

ROLE PLAYING

CAVALLI DI TROIA

PHISHING

NAVIGARE CONTENUTI IN LINEA

INGENIERIA SOCIALE INVERSA

- **SHOULDER SURFING:** può essere tradotto come *spiare* da dietro le spalle, qui ci troviamo nel caso in cui un attaccante usa *tecniche di osservazione*, come appunto spiare da dietro le spalle mentre qualcuno sta compiendo qualche azione volta a*ll'uso visivo esplicito* di informazioni sensibili. Può essere compiuta sia da *persone vicine* a noi sia a distanza con l'utilizzo di binocoli o di strumenti visivi.
- **DUMPSTER DIVING:** può essere tradotto come *frugare tra la spazzatura*, molte volte le grosse organizzazioni cestinano dati come elenchi telefonici, manuali, policy della compagnia, calendari, agende, eventi, stampate di dati sensibili, *login e password*, stampate di codice sorgente, dischi, carta intestata, memo, hardware contenente ancora dati utili. L'attaccante può usare questa *"spazzatura"* per ottenere una grossa quantità di informazioni sulla natura dell'organizzazione e sulla struttura della rete.
- **ROLE PLAYING:** è una delle *armi principali* di un ingegnere sociale. Consiste nel persuadere o nell'*ottenere informazioni* grazie all'uso di chat online, email, telefono, o qualsiasi altro strumento che la compagnia usa per *interagire* con il pubblico, impersonando un helpdesk, un impiegato, un tecnico o un qualsiasi altro utente autorizzato a ricevere *informazioni confidenziali.*
- **CAVALLO DI TROIA (trojan):** è uno dei metodi predominanti *attualmente* usati da un hacker, consiste nel *convincere* la vittima a scaricare un file malevole sul proprio sistema e una volta eseguito crea una *backdoor* sulla macchina che concede all'attaccante il *completo accesso* in qualsiasi momento.
- **PHISHING:** consiste nella *creazione* di siti web e email molto simili a quelli legittimi, inducendo un ignaro utente a *rivelare* informazioni private, quali per esempio i dati di login, o di una carta di credito, grazie all'utilizzo di *siti clonati* e creati appositamente per ingannare l'utente.
- **NAVIGARE CONTENUTI IN LINEA:** una grossa quantità di informazioni sulla struttura dell'organizzazione, email, numeri di telefono etc sono *disponibili liberamente* sul sito della compagnia. Queste informazioni possono essere usate per *rifinire al meglio* l' approccio dell'attaccante oppure per *creare un piano* di attacco o un metodo da utilizzare per *ingannare* il target
- **INGENIERIA SOCIALE INVERSA:** un attacco di ingegneria sociale inversa consiste nel convincere il target di avere un problema oppure che nell'immediato futuro avrà un problema, e l'attaccante è pronto a risolverlo. Questo attacco si divide in 3 parti:

    1. **sabotaggio:** dopo che l'attaccante guadagna un *semplice accesso* al sistema, tenta di *sabotare* il sistema o di *dare l'apparenza* che il sistema sia stato corrotto. Quando il target si accorge *dello stato* del sistema, comincerà a cercare aiuto o qualcuno che risolva il guaio.
    2. **marketing:** per essere sicuri che il target si *rivolga all'attaccante* per risolvere il problema, esso deve spacciarsi come *l'unico in grado* di poter risolvere la situazione.
    3. **supporto:** in questa parte, si guadagna la *fiducia* del target e si *ottiene accesso* alle informazioni sensibili.

Difendersi dall'ingegneria sociale

Non ci sono *metodi efficaci* per proteggersi da un attacco di I.S, in quanto *non importa* quanti controlli vengono implementati, ci sarà sempre un *"fattore umano"* che influenza il comportamento di un individuo. Possiamo però cercare di *ridurre l'efficacia* di un attacco e quindi di ridurne la riuscita. Alcuni controlli che dovrebbero essere *curati* sono:

- Installare e *mantenere aggiornati* firewall, antivirus, antispyware, *filtri email.*
- Non lasciarsi *"spiare"* dalle persone.
- Creare una *strategia* di risposta agli incidenti informatici.
- *Prestare attenzione* agli URL dei siti. Spesso i siti clonati sono *identici nell'aspetto* ma gli URL hanno piccole variazioni, *lettere differenti* o domini *completamente* diversi.
- Dettagli confidenziali o critici, come caselle email, non dovrebbero essere consultati in *luoghi pubblici* dove *non è possibile* stabilire la *sicurezza* della rete.
- *Non inviare* informazioni sensibili attraverso internet *senza* aver prima *controllato la sicurezza.*
- Non rivelare informazioni personali o finanziarie nelle email, e *non rispondere* a email che sollecitano la richiesta di tali informazioni.
- Usa *tastiera virtuali* quando disponibili.
- Assicurarsi di *aver distrutto* ogni documento che contiene dati sensibili *prima di cestinarlo.*

Conclusioni

In questo articolo abbiamo compreso che *qualunque* sia la sicurezza delle nostre applicazioni, siamo sempre *vulnerabili al "fattore umano"*. Questo fattore umano è il *collegamento più debole* in ambito sicurezza e non può essere *risolto* in un unica volta ma deve rientrare in un *processo continuo* di miglioramento.
Spesso si deve assicurare l'interazione tra *dati e persone* piuttosto che *dati e server*, il punto *debole* è la *persona* non la macchina.

Qui c'è il formato pdf se vuoi scaricare la lettura.

Stay tuned stay hack! Happy hacking folks!!!!

under_r00t crew