Il professionista dell’inganno: l’ingegnere sociale

L’attività di un ingegnere sociale fonda le proprie basi essenzialmente sull’**inganno**. Indurre la vittima designata a intraprendere azioni inconsuete a proprio beneficio (per ottenere informazioni riservate e sensibili), magari sfruttando ed enfatizzando l’uso dell’autorità, dell’urgenza e della pressione psicologica, sono solo alcuni tra gli *escamotages* adottati.

Le azioni criminali basate sull’ingegneria sociale, di cui abbiamo notizie fin dalla notte dei tempi, possono concretizzarsi con o senza l’ausilio di tecnologia. Purtroppo è un dato di fatto che l’ingegneria sociale si è evoluta nel tempo da una tecnica di attacco che puntava esclusivamente sul carisma e l’abilità dell’attaccante verso una **strategia ibrida**, ancora più incisiva e subdola che sfrutta sia le abilità cognitive che quelle informatiche. Questo è stato reso possibile negli ultimi anni grazie alla crescita della digitalizzazione della comunicazione con la diffusione dei social (fucina inesauribile di informazioni) e dei vari servizi di messagistica. L’ingegnere sociale sfrutta, per l’appunto, la percezione distorta che l’utente medio ha di questi strumenti, ritenendoli puramente virtuali, privi di insidie e scollegati dal mondo reale.

Anatomia di un attacco

Qualunque sia il *modus operandi* adottato, è possibile suddividere l’anatomia di un attacco in quattro fasi principali:

Fase 1. *Footprinting*. Raccogliere quanto più informazioni

sulla vittima è il primo passo fondamentale e propedeutico. Ogni dato anche apparentemente insignificante è indispensabile per focalizzare il contesto da colpire. È in questa fase che si definiscono le modalità di attacco da intraprendere. Lo scopo è acquisire familiarità con il target e definire l'obiettivo criminale, modalità e strategie;

Fase 2. Instaurare una relazione. Il passo successivo consiste nel guadagnare fiducia e complicità con la vittima, stabilendo una relazione in modo diretto o attraverso una catena di conoscenze e relazioni di terze parti;

Fase 3. Manipolazione psicologica. È questo il momento di allestire un inganno verosimile. Grazie alle informazioni reperite e alla relazione instaurata, si procede all'abbattimento delle difese per sferrare l'attacco definitivo;

Fase 4. Esecuzione. In quest'ultima fase, che dipenderà dall'abilità dell'ingegnere sociale nell'eliminare ogni rischio o traccia, si consolida il risultato ottenuto.

Tecniche di ingegneria sociale

Alla luce di quanto detto, oggettivamente risulta più semplice e meno dispendioso sfruttare un *bug* umano piuttosto che spendere del tempo alla ricerca di una falla in un sistema informatico. Volendo colpire un'infrastruttura, la domanda che potrebbe balenare a un criminale è: "perché cercare di forzare i sistemi di sicurezza più o meno complessi, se è possibile sfruttare le vulnerabilità intrinseche dell'elemento umano?"

In questo modo è la stessa vittima prescelta a rappresentare – inconsapevolmente – il vettore per l'adempimento dell'azione fraudolenta, magari allestita con la commistione di *malware*, persuasione umana ed empatia, tutti gli ingredienti (fondamentali e interscambiabili tra loro) preferiti dall'ingegnere sociale.

Di seguito si elencano alcune delle tecniche più comuni, tecnologiche e non.

Intercettazione delle comunicazioni

Ascoltare telefonate personali, conversazioni tra addetti ai lavori o intercettare chat o messagistica istantanea, rappresentano tutti un buon punto di partenza per il progetto preliminare dell'ingegnere sociale.

Shoulder Surfing

È una tecnica non invasiva che consiste, ad esempio, nello spiare la digitazione di credenziali d'accesso, o semplicemente nello sbirciare estremi o documenti quando si è in coda agli sportelli, oppure seduti in luoghi o mezzi di trasporto pubblici.

Dumpster Diving

È un'azione che consiste nel cercare nella spazzatura dell'azienda o del target informazioni riservate e utili per l'allestimento dell'inganno. Si pensi a cosa usualmente si può gettare nell'immondizia (estratti conti, ricevute fiscali, solo per citarne alcuni!)

Tailgating

Con questo termine si classificano le modalità di attacco che consentono all'ingegnere sociale:

- di accedere a un luogo fisico protetto, fingendo di aver dimenticato la chiave di sicurezza oppure chiedendo una cortesia a un utente autorizzato, o ancora fingendosi un tecnico (telefonico, elettricista…) per operare indisturbato sulla rete aziendale;
- di sfruttare il rapporto di fiducia instaurato con la vittima per chiedere in prestito un dispositivo elettronico e approfittare del tempo a disposizione per violare dati sensibili o installare software dannosi.

Baiting

Con questa tecnica si utilizza come esca, opportunamente armata con un *malware*, un supporto informatico quale una chiavetta USB, un hard disk, un CD lasciato volutamente incustodito, come se fosse stato smarrito e contare sulla curiosità della vittima di volerne conoscere il contenuto, per eseguire il codice malevolo nascosto.

Pretexting

Il criminale induce l'utente a commettere determinate azioni, creando un falso contesto, cercando di entrare in empatia con la vittima, di interpretare un ruolo di autorità credibile oppure di intimare delle gravi ripercussioni: la truffa del falso CEO [1] e le campagne *sextortion* [2] ne sono tipici esempi.

Phishing

Il *phishing*, di cui ho ampiamente parlato in un precedente articolo [3], è una tecnica fraudolenta caratterizzata dall'abilità di ottenere informazioni confidenziali con pretesti fuorvianti attraverso l'uso combinato di strumenti tecnologici/digitali e maestria ingannevole. Solitamente l'attaccante invia alla vittima una mail oppure un SMS (in tal caso si parla di ***Smishing***) impersonando, anche con loghi contraffatti un ente, un istituto di credito o azienda legittima, con l'invito a cliccare su di un link (che porta verso un sito "farlocco") o a scaricare degli allegati (contenenti un payload malevolo).
È comunque ancora in voga anche una versione telefonica della tecnica di *phishing* (***Vishing***), in cui l'ingegnere sociale, con la scusa di offrire un servizio o prestare un intervento tecnico, cerca di ottenere indirettamente delle informazioni riservate inducendo il malcapitato a eseguire delle operazioni mirate alla realizzazione della truffa stessa.

Conclusioni

Dall'ultima edizione del rapporto Clusit emerge che il **63% degli attacchi totali**, nel primo semestre 2019, è stato messo a segno attraverso tecniche semplici e a basso costo, tra le quali primeggia quella adoperata dal professionista dell'inganno: l'ingegneria sociale (con un aumento del **+104%** rispetto al medesimo periodo del 2018).

Per riconoscerla in tempo ed evitarla occorre, soprattutto, averne consapevolezza.

A tal proposito, ecco alcune ***best practices*** valide sia per privati che aziende:

- è buona norma diffidare dall'installazione di app di cui non possiamo verificare con certezza la fonte e in ogni caso valutare sempre quali permessi concedere;
- prestare attenzione agli URL dei siti;
- dubitare sempre delle mail che richiedono dati riservati o che promettono offerte imperdibili;
- seguire le procedure di sicurezza secondo le politiche aziendali, evitando di intraprendere procedure inusuali;
- richiedere sempre un riconoscimento ufficiale prima di ogni consenso;
- utilizzare in modo consapevole e responsabile i social network, senza condividere in rete informazioni personali o riservate;
- evitare l'uso di servizi di messaggi in risposta automatica in caso di assenza da lavoro;
- evitare connessioni wifi aperte e pubbliche.

Non meno importanti e trascurabili, le regole di buona pratica **non tecnologiche**:

- adottare una metodologia di distruzione documenti (aziendali/privati) in modo da evitare un eventuale riassemblaggio se prelevati dai rifiuti;
- adottare una più attenta politica di sicurezza fisica

degli accessi, che consenta l'accertamento della legittimità degli ingressi;
- evitare di diffondere informazioni private e riservate, di trascrivere password su appunti o biglietti volanti;
- evitare d'installare dispostivi di dubbia provenienza (trovati/non autorizzati) sui propri pc di lavoro o privati.

Note

[1] https://www.cybersecurity360.it/nuove-minacce/la-truffa-del-falso-ceo-cose-come-funziona-come-difendersi/

[2] https://www.ictsecuritymagazine.com/articoli/sextortion-analisi-di-una-mail-del-ricatto/

[3] https://www.ictsecuritymagazine.com/articoli/phishing-consigli-utili-per-attenuare-il-rischio-di-adescamento/

Riferimenti

Articolo a cura di **Salvatore Lombardo**

Salvatore Lombardo è laureato in Ingegneria Elettronica orientamento Telematico. Ha frequentato un Master in Information and Communication Technologies – Internet Software Engineering.

Da oltre dieci anni svolge l'attività di funzionario informatico presso la Pubblica Amministrazione, curando in particolare la sicurezza informatica e l'amministrazione di rete.

In qualità di esperto ICT, iscritto all'albo dei docenti della ex Scuola Superiore dell'Amministrazione dell'Interno, ha

tenuto vari corsi di formazione e aggiornamento per il personale.

È autore del libro La Gestione della Cyber Security nella Pubblica Amministrazione.

https://www.ictsecuritymagazine.com/articoli/il-professionista-dellinganno-lingegnere-sociale/