Capitolo 1

Uno sguardo al nuovo mondo dell'ingegneria sociale professionale

> Suppongo che la vostra sicurezza sia il vostro successo e che la chiave del vostro successo sia il vostro fine palato.
>
> *Gordon Ramsay*

Mi ricordo ancora bene quando, seduto di fronte allo schermo del mio computer, iniziai a scrivere il primo paragrafo di *Social Engineering: The Art of Human Hacking*. Era la metà del 2010. Sarei quasi tentato di dirvi che la scrittura del libro è stata un'impresa in tanti i sensi, dovendo usare una macchina per scrivere, ma non voglio essere troppo drammatico.

Al tempo, cercando in Internet il termine "social engineering", trovavate alcune pagine sulla leggenda dell'ingegneria sociale Kevin Mitnick e alcuni video su come corteggiare le ragazze o scroccare hamburger. Sono trascorsi otto anni e ora il termine ingegneria sociale suona quasi familiare. Negli ultimi tre o quattro anni ho visto applicare l'ingegneria sociale nella sicurezza, nell'amministrazione, nell'istruzione, in psicologia, in ambito militare e in ogni altra realtà che si possa immaginare.

Questa transizione impone di chiedersi il perché. Un collega mi ha detto: "È tutta colpa tua, Chris". Penso che lo intendesse come un insulto, anche se ho provato un pizzico di orgoglio nel sentirmelo dire. Tuttavia, non ritengo di essere il solo responsabile della quasi ubiquità del termine *ingegneria sociale* (*social engineering* o SE). Credo che oggi sia usato da tutti non solo perché è il più semplice fra i vettori di attacco – oggi come sette anni fa – ma perché oggi è ancora più redditizio.

In questo capitolo

- **Che cosa è cambiato?**
- **Perché dovreste leggere questo libro?**
- **Una panoramica sull'ingegneria sociale**
- **La piramide SE**
- **Di che cosa parla questo libro?**
- **Riepilogo**

Il costo di un attacco di ingegneria sociale è basso. Il rischio è ancora più basso. Il vantaggio potenziale è *enorme*. Il mio team ha raccolto informazioni statistiche sui notiziari e sul Web di attacchi di ingegneria sociale. Credo di poter affermare che nel 2017 oltre l'80% di tutti gli attacchi aveva un elemento di ingegneria sociale.
Il *Cost of Data Breach Study* del 2017 di IBM afferma che il costo medio di un attacco è di 3,62 milioni di dollari. Quando il profitto potenziale è così alto, non è certamente difficile capire perché un malintenzionato ricorra all'ingegneria sociale.

SUGGERIMENTO DA PROFESSIONISTI

Nel 2017, il *Cost of Data Breach Study* di IBM ha compiuto 12 anni. Potete trovarlo su `https://www-03.ibm.com/security/data-breach/`. Oppure potete semplicemente inserire "Cost of Data Breach Study" in qualsiasi motore di ricerca per trovare e scaricare un rapporto completo e aggiornato.

Ricordo anche una delle mie prime interviste dopo la scrittura del mio libro *Social Engineering: The Art of Human Hacking*, pubblicato nel 2010. Mi hanno chiesto: "Non temi di armare i cattivi?". Per me, l'ingegneria sociale è come un nuovo tipo di guerra. Per spiegarlo in modo più chiaro, rievoco la storia di Bruce Lee e del suo arrivo in America negli anni Sessanta. A quel tempo i pregiudizi razziali erano un problema e lui stava facendo qualcosa che nessun altro faceva: insegnare *jeet kune do* (un'antica arte marziale cinese) a persone di ogni razza, colore o nazionalità. All'università si scontrò con altri studenti che pensavano di sapere tutto sul combattimento. Ma li mise al tappeto uno dopo l'altro. Alla fine, alcuni di quegli avversari divennero persino amici o allievi di Bruce. Qual è la lezione? Gli altri dovevano adattarsi a questo nuovo tipo di combattimento, o sarebbero stati facilmente e costantemente battuti. C'era il rischio che un allievo di Bruce Lee potesse usare le sue nuove abilità per ferire gli altri e fare del male? Sì, ma Bruce sentiva la necessità di istruire gli altri, in modo che potessero difendersi.
Quindi, la mia risposta alla domanda "Non temi di armare i cattivi?" è la stessa di otto anni fa: non posso controllare come userete queste informazioni. Potete leggere questo libro e poi uscire, attaccare le persone e derubarle. Oppure potete leggere questo libro e imparare a difendervi. La scelta è vostra, ma i bravi ragazzi hanno bisogno che qualcuno insegni loro che cosa fare.
Imparare a difendersi da questo nuovo stile di attacco richiede molto più che imparare a battersi. Come con il *jeet kune do*, occorre equilibrio tra imparare ad attaccare, imparare a difendersi e sapere quando applicare l'una o l'altra cosa. Mentre imparerete a diventare ingegneri sociali, dovete essere in grado di pensare come i cattivi, ricordandovi sempre di comportarvi da bravi ragazzi. Volendo rubare un'altra analogia, dovete sentire dentro di voi la forza, ma non usarla mai per camminare nel lato oscuro.
Potreste chiedervi: "Se non è cambiato molto nella tua risposta, perché abbiamo bisogno di una seconda edizione del tuo libro?". Lasciate che ve lo dica.

Che cosa è cambiato?

Questa è una domanda fondamentale quando si parla di ingegneria sociale. Superficialmente, la risposta è "Non molto". Potete tornare indietro e trovare tanti aneddoti sull'ingegneria sociale. Per esempio, una delle prime storie documentate che ho trovato si

trova nella Bibbia, nel libro della Genesi, e si dice che sia avvenuta intorno al 1800 a.C.: Giacobbe desiderava la benedizione che aveva ricevuto il fratello maggiore, Esau. Sapendo che suo padre, Isacco, non ci vedeva e faceva affidamento su altri sensi per capire con chi stesse parlando, Giacobbe si vestì con gli abiti di Esau e gli preparò il pranzo come lo avrebbe preparato lui. Ecco la parte migliore: Esau era noto per essere particolarmente villoso, mentre Giacobbe non lo era, così si legò le pelli di due giovani capre tra le braccia e la nuca. Quando Isacco allungò la mano per toccare Giacobbe, fece affidamento sull'olfatto, sul tatto e sul gusto, i quali gli dicevano che era con Esau e non Giacobbe. Secondo il racconto della Genesi, l'attacco di ingegneria sociale di Giacobbe funzionò! Dall'alba della storia, ci vengono riportate truffe, inganni e imbrogli. In apparenza, non sembra esserci molto di nuovo quando si parla di ingegneria sociale, ma ciò non significa che le cose non cambino mai.

Un esempio è il *vishing*. Ricordo bene quando usai per la prima volta la parola *vishing*. La gente mi guardava come se stessi parlando *klingon*. Davvero, avrei potuto dire "laH yIlo' ghogh HablI' Hiv" (questo è per i fan di Star Trek). A partire dal 2015, tuttavia, la parola *vishing* è entrata nell'*Oxford English Dictionary*.

SUGGERIMENTO DA PROFESSIONISTI

Il klingon è una lingua fittizia, ma esiste un vero e proprio istituto (`www.kli.org`) dedicato all'insegnamento, alla traduzione e alla fonetica della lingua klingon. Potete anche trovare numerosi traduttori online. A oggi, tuttavia, non ho avuto notizia di attacchi di "ingegneria sociale" svoltisi in lingua klingon.

Perché è importante che oggi *vishing* sia nel dizionario? Dimostra quanto le azioni di ingegneria sociale abbiano influenzato il mondo. Parole che un tempo sembravano appartenere a una lingua "inventata", ora fanno parte del nostro vocabolario quotidiano.

Ma non è solo questo nuovo vocabolario a essere diventato ormai di uso comune. Ora esistono servizi specializzati nell'aiutare i cattivi a essere sempre più bravi nell'essere cattivi. Per esempio, mentre stavo lavorando per un cliente, mi sono imbattuto in un servizio specializzato nella correzione e verifica ortografica delle e-mail di *phishing*. Forniva un supporto ventiquattro ore su ventiquattro in lingua inglese. Provate a mettere insieme cose di questo genere con la cultura BYOD (*Bring Your Own Device*) e con il fatto che ormai molti apparecchi mobili sono in pratica mini-supercomputer e poi metteteci insieme la nuova forma di dipendenza globale dai *social media*. Quello che ottenete è la ricetta per un intero panorama di nuovi attacchi: basati sull'ingegneria sociale.

Oltre a essere cambiato il panorama, anche io sono cambiato. Quando scrissi la prima edizione di questo libro, il titolo era *Social Engineering: The Art of Human Hacking*. Ho scelto quel titolo perché sentivo che quello che stavo descrivendo nel libro era molto simile a un'arte. L'arte è soggettiva; ha significati differenti per persone differenti. Può essere applicata in modo differente e può essere utilizzata, visualizzata, apprezzata e detestata per motivi completamente differenti.

Il titolo originale inglese di questa seconda edizione è *Social Engineering: The Science of Human Hacking*. Il dizionario Merriam-Webster definisce la *scienza* come "Lo stato di conoscenza: una conoscenza distinta dall'ignoranza o dal fraintendimento". Otto anni fa, gran parte di quel che facevo era una novità nel campo della sicurezza e stavo imparando. Ora sono in uno "stato di conoscenza", grazie agli anni di esperienza che ho aggiunto al mio curriculum.

Questa esperienza, spero, renderà questo libro ancora più utile per voi, che siate esperti di sicurezza che cercano di capire che cosa sia l'ingegneria sociale o che siate appassionati desiderosi di ampliare i vostri orizzonti o anche educatori che stanno cercando di capire i problemi da considerare nelle lezioni. Qualsiasi sia il motivo per il quale state leggendo questo libro, la mia speranza è che, trattando questi argomenti a un livello più scientifico, io possa trasmettervi queste informazioni in un modo più utile e completo.

Perché dovreste leggere questo libro?

Penso che questo primo capitolo debba seguire lo stesso schema che ho seguito nel mio primo libro, quindi voglio dedicare del tempo a spiegare perché penso che questo volume sia rivolto a tutti. Sì, mi rendo conto che potrei essere "un pochino" di parte, ma seguitemi per un momento.
Siete esseri umani? Scommetto che se siete seduti di fronte a questo libro, e se state leggendo questo paragrafo, o siete una forma davvero avanzata di intelligenza artificiale o siete esseri umani. Probabilmente il 99,9999999% dei lettori di questo libro è costituito da esseri umani. L'ingegneria sociale parte dal "funzionamento standard" degli esseri umani quando prendono decisioni e nel sfruttare le vulnerabilità.
L'obiettivo di un ingegnere sociale è quello di indurvi a prendere una decisione senza riflettere. Più pensate, più è probabile che vi accorgiate di essere stati manipolati, il che, naturalmente, è contrario agli interessi dell'aggressore. Negli episodi 7 e 70 di *The Social-Engineer Podcast*, ho avuto il privilegio di intervistare la dottoressa Ellen Langer. Mi parlò di qualcosa che ha chiamato *alpha mode* e *beta mode*.

SEPodcast

Di seguito sono riportati gli URL in cui potete trovare gli episodi di *The Social-Engineer Podcast* nei quali ho intervistato la dottoressa Langer.

- L'Episodio 7 contiene la mia prima intervista con la dottoressa Langer, nella quale discutiamo della sua ricerca e dei suoi libri: `www.social-engineer.org/podcast/episode-007-using-persuasion-on-the-mindless-masses/`.
- L'Episodio 70 si svolge cinque anni dopo la mia prima intervista alla dottoressa Langer. È tornata per dirci che cosa ha imparato nel corso degli anni, che cosa è cambiato e come siamo avanzati: `www.social-engineer.org/podcast/ep-070-thinking-with-out-a-box`.

In *alpha mode* il cervello funziona a 8-13 cicli al secondo. In genere è caratterizzato dal "sognare a occhi aperti" o da quello che la dottoressa Langer ha definito "concentrazione rilassata e focalizzata".
In *beta mode* il cervello funziona da 14 a 100 cicli al secondo: è attento, vigile e consapevole di quello che gli accade attorno.
Quale stato è più vantaggioso per un ingegnere sociale? Ovviamente, la risposta è l'*alpha mode*, perché gode di una certa rilassatezza del pensiero e della consapevolezza. Questo

non vale solo per le situazioni in cui sia in atto un'aggressione. La manipolazione e alcune tecniche di influenzamento sono orientati a farvi agire senza riflettere.
Per esempio, immaginate uno spot come questo: una famosa cantante compare sullo schermo; una canzone molto triste suona in sottofondo. L'immagine cambia: vengono mostrati gattini e cagnolini che sono stati maltrattati e sono feriti e denutriti. Sembrano in procinto di morire. Ma la cantante torna sullo schermo; ora è circondata da animali sani e li sta inondando di coccole. Qual è il messaggio? Che per pochi spiccioli quegli animali denutriti e quasi morti possono diventare animali da compagnia: sani, felici e tutti vostri. Le immagini nello spot sono come quelle della Figura 1.1.

Figura 1.1 Come vi fa sentire questa foto? © Amazon Community Animal Rescue, www.flickr.com/photos/amazoncares/2345707195.

I produttori dello spot vi stanno manipolando per egoismo? Non del tutto. Quello che sanno è che se riusciranno a evocare emozioni in voi, è più probabile che donerete una somma o che intraprenderete l'azione desiderata. Il tasso di successo è maggiore di quello che avrebbero facendo ricorso semplicemente alla conoscenza o alla logica. Più emozioni riescono a innescare e meno penserete in modo razionale. Meno pensate in modo razionale e più velocemente deciderete, basandovi unicamente sulle vostre emozioni.
Quindi, tornando al punto precedente: se siete esseri umani, questo libro può aiutarvi a capire quali tipi di attacchi esistono. Potete imparare come i cattivi possono usare la vostra umanità contro di voi e potete imparare a difendervi da questi attacchi per proteggere voi e i vostri cari.
Permettetemi di iniziare da una panoramica sull'ingegneria sociale.

Una panoramica sull'ingegneria sociale

Ogni volta che parlo di ingegneria sociale, di solito inizio con una definizione che uso da dieci anni. Col tempo l'ho adattata, ma solo leggermente.
Ma prima di darvi la definizione di ingegneria sociale, devo proprio affermare un punto molto importante: l'ingegneria sociale non è *politicamente corretta*. Questa verità può essere difficile da digerire per molte persone, ma è un fatto reale: l'ingegneria sociale si basa sul fatto che esistono pregiudizi di genere, di razza, di età e di stato (oltre a tutte le combinazioni possibili).
Per esempio, immaginate di dovervi infiltrare nell'edificio di un cliente. Per farlo, dovete escogitare un pretesto che vi permetta di accedervi facilmente. Il vostro team è composto da poche persone, di diverso tipo. Se valutate che il miglior pretesto sia fingersi un addetto alle pulizie, quale dei seguenti membri del team sarebbe più efficace?

- Uomo bianco, biondo, di 40 anni.
- Donna asiatica, di 43 anni.
- Donna latina, di 27 anni.

Se valutate che il miglior pretesto sia fingersi un addetto alla cucina, quale dei seguenti membri del team sarebbe più efficace?

- Uomo bianco, biondo, di 40 anni.
- Donna asiatica, di 43 anni.
- Donna latina, di 27 anni.

In realtà, se i tre fossero tutti ingegneri sociali esperti, potrebbero provare e avere successo. Ma quale dei tre solleverà il minor numero di pensieri? Ricordate, i pensieri sono nemici dell'ingegnere sociale.
Con questo in mente, torniamo a come definisco l'ingegneria sociale: *l'ingegneria sociale è ogni atto tendente a influenzare una persona, per spingerla a intraprendere un'azione che non necessariamente è nel suo migliore interesse.*
Perché una definizione così ampia e generale? Perché credo che l'ingegneria sociale non sia *sempre* negativa.
Ci fu un tempo in cui si poteva dire "Sono un hacker" senza che tutte le persone normali cercassero di correre ai ripari, staccando ogni dispositivo elettronico circostante. Essere hacker, un tempo, significava essere qualcuno che aveva *bisogno* di sapere come funzionavano le cose. Un hacker non si accontentava delle conoscenze di base; doveva scavare in profondità nel funzionamento di qualsiasi cosa. Una volta compreso il funzionamento di una cosa, l'hacker avrebbe cercato un modo per aggirare, migliorare, sfruttare o modificare lo scopo originale di quella cosa.
Quando iniziai il mio primo libro, volevo assicurarmi di poter definire l'ingegneria sociale in un modo che non implicasse necessariamente la presenza di un perfido artista della truffa o un imbroglione o un furfante. Gli stessi principi usati dai cattivi possono essere applicati per buoni propositi e voglio che lo sappiate.
Spesso uso questo esempio. Se venite da me e mi dite: "Ehi, Chris. Voglio fare una festa per principesse: tu ti siedi qui e ti dipingo le unghie mentre indossi una sciarpa rosa e parliamo delle principesse Disney", non solo riderei di voi, ma tenterei di allontanarmi lentamente, cercando l'uscita più vicina. Eppure, devo ammettere che potrebbero esserci situazioni in cui non disdegnerei questo tipo di cose.

In che senso, direte? Mia figlia mi ha chiesto di fare una festa per principesse con lei. Ora, prima che diciate "Ehi, ma non vale come paragone: è tua figlia!", ammetto che questo piccolo particolare ha influenzato non poco la mia decisione di stare al gioco, ma mi interessa che riflettiate sui principi psicologici che erano in gioco quando ho preso questa decisione. Per accettare una cosa che avrei assolutamente rifiutato, in un nanosecondo, se mi fosse stata proposta da qualcun altro, ho dovuto ignorare il mio normale processo decisionale e rispondere "Sì".

Un dettaglio assolutamente inutile

Considerando che un nanosecondo è un miliardesimo di secondo e che una persona, in media, parla a un ritmo di 145 parole al minuto, letteralmente non potevo "dire" la parola "no" in un nanosecondo. D'altra parte, la luce, che viaggia a 300.000 chilometri al secondo, percorre 30 centimetri in un nanosecondo.

Se comprendete in quale modo vengono prese le decisioni, potete iniziare a capire come un aggressore malintenzionato possa usare "grilletti" emotivi, principi psicologici e applicare l'arte e la scienza dell'ingegneria sociale per farvi "intraprendere un'azione che non necessariamente è nel vostro migliore interesse".
Il dottor Paul Zak è apparso nell'Episodio 44 di *The Social-Engineer Podcast*. Ha scritto il libro *La molecola della fiducia: all'origine della prosperità economica e sociale* (Scuola di Palo Alto, Milano 2015). In quel libro, e nel nostro podcast, Zak parlava della sua ricerca relativa a un ormone chiamato *ossitocina*. La sua ricerca ci ha aiutato a vedere quanto l'ossitocina sia strettamente legata alla fiducia, perché fece un commento molto importante sul modo in cui viene rilasciata nel nostro sangue quando sentiamo che qualcuno si fida di noi. Vi prego di comprendere questo punto molto importante: il vostro cervello libera ossitocina non solo quando voi vi fidate di qualcuno, ma anche quando *sentite* che qualcun altro vi dà fiducia. Secondo la ricerca di Zak, questo fenomeno si verifica di persona, al telefono, via Internet e anche quando non è possibile vedere la persona in questione.

SEPodcast

L'Episodio 44 di *The Social-Engineer Podcast* include l'affascinante conversazione con il dottor Zak sul lavoro della sua vita. Potete trovarlo su `www.social-engineer.org/podcast/ep-044-do-you-trust-me/`.

Un'altra sostanza chimica prodotta dal nostro cervello è la dopamina. La *dopamina* è un neurotrasmettitore che il nostro cervello rilascia nei momenti di piacere, felicità ed eccitazione. La miscela di ossitocina e di dopamina genera un cocktail cerebrale con il quale un ingegnere sociale può aprire qualsiasi porta.

La dopamina e l'ossitocina vengono rilasciate nel nostro cervello durante i momenti di intimità, ma possono essere rilasciate anche durante le normali conversazioni. Esattamente quelle conversazioni sono al centro dell'ingegneria sociale.
Credo che tutti usiamo questi stessi principi quotidianamente – il più delle volte inconsapevolmente – con il nostro coniuge, con il capo, coi colleghi, coi sacerdoti, coi terapeuti, con il personale di servizio e con tutti quelli che incontriamo. Di conseguenza, sapere che cos'è l'ingegneria sociale e come comunicare con i propri simili è imperativo per tutti. In un mondo in cui la tecnologia ha facilitato le comunicazioni utilizzando *emoticon* o meno di 280 caratteri, è sempre più difficile imparare a usare le capacità comunicative e ancor più difficile capire quando quelle abilità vengono utilizzate contro di noi. Facendo un ulteriore passo avanti, i *social media* hanno creato una società in cui raccontare a tutti tutto quello che ci accade è accettabile e addirittura valutato positivamente.
Quando parlo dell'ingegneria sociale intesa in senso malevolo, la suddivido nei seguenti quattro vettori.

- *SMiShing* - Sì, esiste: è il *phishing* via SMS o tramite messaggi di testo. Quando Wells Fargo è stata violata nel 2016, ricevetti l'attacco *SMiShing* mostrato nella Figura 1.2.

Figura 1.2 In questo attacco SMiShing sono cadute parecchie persone.

  Quello che è pazzesco è che non uso nemmeno Wells Fargo, ma ho comunque ricevuto questo attacco (e no, non vi dirò che banca uso… per chi mi avete preso?). Con un semplice clic, questi attacchi erano finalizzati a sottrarre credenziali o a caricare *malware* sul dispositivo mobile e a volte a fare entrambe le cose.
- *Vishing* - Come ho già detto, si tratta del *phishing* vocale. È aumentato drasticamente, come vettore, dal 2016. È facile, economico e molto redditizio per chi svolge l'attacco. È anche quasi impossibile localizzare e poi catturare un malvivente, che impieghi numeri falsi e chiami dall'estero.
- *Phishing* - L'argomento più discusso nel mondo dell'ingegneria sociale è il *phishing*. In effetti, l'editor tecnico di questo libro, Michele, e io abbiamo scritto il libro *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails* (Wiley, 2016). Esatto: ho "infilato" nella pagina, senza vergogna, un altro dei miei libri. Il *phishing* è stato utilizzato per chiudere stabilimenti produttivi, per hackerare partiti, per violare la Casa Bianca e decine di grandi aziende e rubare milioni di dollari in diverse truffe. Il *phishing* è di gran lunga il più pericoloso tra i quattro grandi vettori.
- *Impersonificazione* - Lo so, dovrei trovare una qualche forma di "ishing" anche per questo, ma il meglio che posso fare è elencarlo per ultimo, perché è differente. Tuttavia, la sua collocazione in questo elenco non indica affatto che non dobbiate preoccuparvene quanto gli altri. Negli ultimi dodici mesi, abbiamo raccolto centinaia

di storie di persone che si spacciano per poliziotti, incaricati del gas e colleghi per commettere crimini davvero orribili. Nell'aprile del 2017, si parlò di un tipo che si fingeva poliziotto e fu catturato. La sua specialità era la pornografia infantile e tutto si basava su quella sua imitazione.

Altre informazioni

Potete trovare questa storia disgustosa in: `www.sun-sentinel.com/local/broward/pembroke-pines/fl-sb-pines-man-child-porn-20170418-story.html`.

Ogni attacco di ingegneria sociale di cui si legge rientra in una di queste quattro categorie. Più di recente, stiamo vedendo quello che possiamo chiamare attacco combinato: gli ingegneri sociali utilizzano una combinazione di queste tecniche per raggiungere i loro mezzi.
Quando analizzo questi attacchi, comincio a individuare schemi che non solo identificano il tipo di strumenti e passaggi utilizzati, ma che possono anche aiutare un esperto di sicurezza a definire in modo più chiaro come vengono svolti questi attacchi e quindi a utilizzare i risultati per istruire e proteggere il sistema. Ho chiamato questo sistema *la piramide SE*.

La piramide SE

Permettetemi di presentarvi subito la piramide prima di definire il motivo per cui sono giunto a questa simbologia e di spiegare il significato di ogni sua sezione. La piramide è rappresentata nella Figura 1.3.

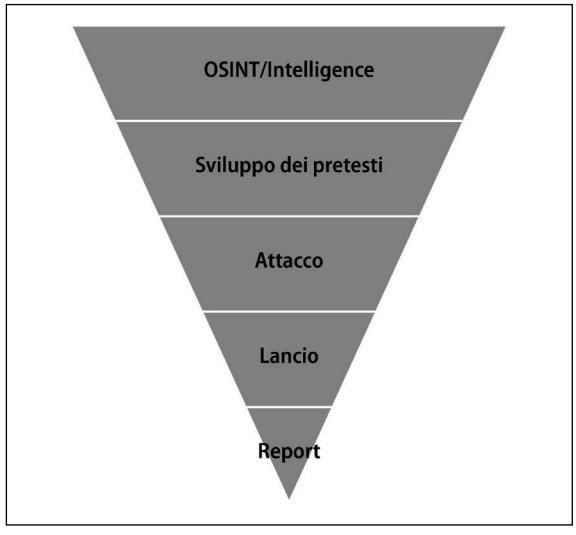

Figura 1.3 La piramide SE.

Come potete vedere, la piramide è suddivisa in poche sezioni e rappresenta l'ingegneria sociale dal punto di vista di un professionista, che utilizza l'ingegneria sociale non per fini malevoli, ma per aiutare i clienti e i consumatori.
Ora definirò ogni sezione della piramide. Nei prossimi capitoli entrerò più in dettaglio dei vari strati.

OSINT

L'OSINT (*Open Source Intelligence*) è la linfa vitale di ogni impegno di ingegneria sociale. È anche la parte che dovrebbe richiedere più tempo. Occupa pertanto la prima e la più grande parte della piramide. Una sezione di questa parte della piramide viene affrontata solo raramente: la documentazione. Come documenterete, salverete e catalogherete tutte le informazioni che avete raccolto? Questo fattore chiave verrà affrontato nel prossimo capitolo.

Sviluppo del pretesto

Sulla base di tutti i risultati della parte OSINT, il successivo passo logico consiste nell'iniziare a sviluppare il pretesto. Questa è una parte cruciale, che è meglio eseguire con l'OSINT bene in mente. Durante questa fase, potete decidere quali modifiche o aggiunte apportare per garantire il successo dell'attacco. È qui che diventa chiaro quali supporti e/o strumenti sono necessari.

Piano d'attacco

Avere un pretesto in mano non significa essere pronti. Il passo successivo è pianificare il che cosa, il quando e il chi.

- Qual è il piano? Che cosa vogliamo fare e stiamo cercando di ottenere? Che cosa vuole il cliente? Queste domande aiuteranno a sviluppare la prossima parte.
- Quando può essere il momento migliore per sferrare l'attacco?
- Chi deve essere disponibile, senza preavviso, per offrire supporto o assistenza?

Attacco

Ora arriva la parte divertente: il lancio dell'attacco. Dopo la preparazione del piano di attacco, siete pronti per procedere a pieno ritmo. È importante essere preparati, ma non al punto da non essere dinamici. Sono convinto che avere un piano scritto possa farvi risparmiare molti mal di testa. Il dubbio che ho è che se elaborate ogni parola che dovrete pronunciare o azione che dovrete prendere, potreste incontrare problemi nel caso di un imprevisto. Il vostro cervello si accorge di non aver predisposto nulla di utile, iniziate a balbettare, a innervosirvi e a mostrare segni di agitazione. Questo può davvero pregiudicare le vostre capacità di successo. Invece di scrivere, suggerisco di strutturare le reazioni, in modo da avere un percorso da seguire ma anche la necessaria libertà d'azione.

Report

Ehi dove andate? Non saltate questo paragrafo. È proprio il caso di leggerlo. Sì, la creazione di report non è divertente, ma pensatela in questo modo: il vostro cliente vi ha appena pagato la somma *x* per un determinato servizio e, molto probabilmente, siete stati dannatamente bravi in questo attacco. Ma il cliente non vi ha pagato solo perché questa è la moda del momento.Vi ha pagato per capire che cosa può fare per risolvere il suo problema. Questo è il motivo per cui la fase di segnalazione si trova al vertice della piramide: è l'apice sul quale poggia *tutto* il resto della piramide.
Le cinque fasi di questa piramide, se ben seguite, vi porteranno al successo non solo come ingegneri sociali, ma come professionisti che offrono servizi di ingegneria sociale ai vostri clienti. Il fatto è che, con l'eccezione del *reporting*, questi sono i passaggi seguiti dagli ingegneri sociali malintenzionati in tutto il mondo.
Nel 2015, Dark Reading ha riferito di un attacco che ha coinvolto proprio questa piramide (potete leggere l'articolo *CareerBuilder Attack Sends Malware-Rigged Resumes to Businesses* su `https://www.darkreading.com/vulnerabilities---threats/careerbuilder-attack-sends-malware-rigged-resumes-to-businesses/d/d-id/1320236`).

1. Gli aggressori effettuarono indagini attaccando alcuni bersagli e, durante la loro fase OSINT, scoprirono che essi utilizzavano un noto sito: CareerBuilder.
2. Dopo aver completato la fase OSINT, gli aggressori iniziarono a sviluppare il pretesto. Ciò li portò a elaborare una falsa ricerca di lavoro, una persona che stava cercando di farsi assumere in qualunque posizione offerta dagli obiettivi. Scoprirono che gli strumenti di cui avevano bisogno erano alcuni file ben preparati e alcuni curriculum dall'aspetto realistico.
3. Iniziarono a pianificare gli attacchi, rispondendo ad alcune delle domande che ho appena esposto.
4. Iniziarono quindi a lanciare gli attacchi caricando i loro documenti non sul sito dell'obiettivo, ma su quello di CareerBuilder. Le aziende che avevano pubblicato offerte di lavoro sarebbero state informate via e-mail che c'era un nuovo richiedente e tale e-mail conteneva gli allegati caricati dagli aggressori.
5. Non seguì alcuna fase di reporting, ma ci sono alcuni report su questo attacco redatti da alcuni ricercatori di Proofpoint.

Questo attacco ebbe successo perché l'obiettivo ricevette un'e-mail con allegati da una fonte affidabile e attendibile (CareerBuilder). Di conseguenza, l'obiettivo aprì l'allegato senza preoccuparsene troppo. Ed esattamente questo è l'obiettivo di un ingegnere sociale: far sì che l'obiettivo intraprenda un'azione che non è nel suo miglior interesse senza riflettere sui potenziali pericoli coinvolti.

Di che cosa parla questo libro?

Quando iniziai a pianificare questo libro, volevo assicurarmi di mantenere il profilo della prima edizione, in modo che ne godessero anche coloro che avevano già tratto beneficio dalle sue pagine. Allo stesso tempo, volevo cambiare il libro e aggiornarlo per descrivere alcuni nuovi attacchi e argomenti di cui non avevo parlato nel libro precedente.

Volevo assicurarmi di aver considerato tutti i suggerimenti che mi erano arrivati da sostenitori, ricercatori, lettori e revisori, nella speranza di poter scrivere un libro ancora migliore del primo. Permettetemi quindi di delineare i contenuti del libro, in modo che sappiate che cosa vi troverete.

Seguendo il percorso della piramide, il Capitolo 2, *Vedi anche tu quel che vedo io?*, descrive le attività di OSINT e tratta alcune delle tecniche normalmente utilizzate. Mi astengo dall'usare troppi riferimenti a strumenti reali, anche se ne menziono alcuni che sono rimasti nella mia cassetta degli attrezzi nell'ultimo decennio.

Nel Capitolo 3, *Profilare le persone attraverso la comunicazione*, esaminerò un argomento cui ho appena accennato nella prima edizione, approfondendo gli strumenti avanzati di modellazione e creazione di profili di comunicazione.

Il Capitolo 4, *Impersonare chiunque*, è il punto in cui comincio a tuffarmi nel pretexting. Questo è un argomento di cui pochi parlano al di fuori dell'ambito dell'ingegneria sociale.Vi tratto i suggerimenti, i trucchi e molte delle esperienze (successi e fallimenti) che ho avuto nel corso degli anni.

Nel Capitolo 5, *Come cercare di farsi accettare*, raccolgo informazioni tratte da molti podcast, newsletter e conversazioni con alcuni dei più grandi esperti del mondo, come Robin Dreeke, e applico all'ingegneria sociale i principi della creazione di relazioni. Robin Dreeke è capo dell'unità di analisi comportamentale dell'FBI e mio buon amico. È un maestro nel costruire relazioni e nel conquistare la fiducia e ha definito i passaggi necessari per conseguire entrambi gli obiettivi.

Il Capitolo 6, *Sotto la mia influenza*, descrive il lavoro di uno dei leader nello studio dell'influenza, Robert Cialdini, nel campo dell'ingegneria sociale. Il capitolo prende i principi che ha sviluppato nel corso dei suoi anni di ricerca e mostra come vengono utilizzati dagli ingegneri sociali.

Il Capitolo 7, *Realizzare la propria opera d'arte*, definisce i concetti di quadro di riferimento e sollecitazione e mostra come chiunque possa impadronirsi di tali tecniche.

Nel Capitolo 8, *Vedo anche quello che non mi hai detto*, torniamo a uno dei miei argomenti preferiti: le comunicazioni non verbali. Scavo in profondità in questo argomento nel mio libro *Unmasking the Social Engineer: The Human Element of Security* (Wiley, 2014), ma questo capitolo è una guida introduttiva alla comunicazione non verbale.

Nel Capitolo 9, *Hacking degli esseri umani*, prendo gli otto capitoli precedenti e li applico a cinque diversi tipi di attacchi di ingegneria sociale. Questo capitolo mostra quanto sia importante per voi, in quanto professionisti dell'ingegneria sociale, applicare i principi presentati in questo libro.

Quasi al termine del libro, il Capitolo 10, *Avete un MAPP?*, tratta gli aspetti di prevenzione e di riduzione dell'impatto. In un libro sull'ingegneria sociale professionale è opportuno che questo capitolo descriva i quattro passaggi utili per imparare a contrastare tutti gli attacchi.

Come tutte le belle cose, anche questo libro deve avere una fine. Quindi il Capitolo 11, *E ora?*, conclude il volume.

Ecco alcune promesse che vi faccio.

- Prometto di non citare Wikipedia come fonte preziosa, specialmente quando si parla di ricerca (ho imparato dai miei errori).
- Prometto di raccontarvi molte storie tratte dalle esperienze che ho avuto negli ultimi sette o più anni. A volte vi racconterò una storia da più punti di vista, per aiutarvi

davvero a chiarire tutti gli aspetti. Ma cercherò di mescolare le varie storie, così da non annoiarvi.

- Quando descriverò le ricerche o il lavoro di alcune delle più grandi menti nei rispettivi campi, presenterò tutti i riferimenti disponibili al loro lavoro, così che possiate approfondire ogni argomento.
- Proprio come ho fatto con il mio primo libro, accoglierò tutti i contatti, i commenti, i suggerimenti e le critiche che mi giungeranno.

Tutto quello che vi chiedo in cambio è che leggiate questo libro per l'uso cui è destinato. Se siete alle prime armi, può aiutarvi a capire che cosa è necessario per diventare professionisti nel campo dell'ingegneria sociale. Se siete esperti, spero che le storie, i suggerimenti e i trucchi che condivido vi diamo nuovi strumenti utili per il vostro arsenale. Se siete appassionati, spero che leggiate questo libro con la stessa eccitazione che avevo io mentre lo scrivevo. E se siete scettici, allora leggetelo pensando che non pretendo di essere l'unico e il solo messia dell'ingegneria sociale. Sono solo un ingegnere sociale appassionato, con molti anni di esperienza, che intende condividere con voi nella speranza di rendere questo mondo un luogo un po' più sicuro.

Riepilogo

Nessuno dei miei libri sarebbe completo senza un'analogia culinaria, quindi eccola qui. Dietro ogni ottimo pasto c'è molta pianificazione. Una grande ricetta richiede ingredienti freschi e poi un'esecuzione allo stesso tempo artistica e scientifica. L'ingegneria sociale, nonostante la sua natura semplice, non è una ricetta per principianti. Bisogna capire il modo in cui gli esseri umani prendono le loro decisioni, che cosa li motiva e come controllare le proprie emozioni sfruttandole invece negli altri.

L'argomento di questo libro è attuale oggi come lo era otto anni fa e forse ancora di più. Negli ultimi otto anni ho visto molte persone crescere come professionisti dell'ingegneria sociale. Ho visto emergere e poi schiantarsi anche molti malviventi dell'ingegneria sociale. Dal momento che la natura degli attacchi poggia così pesantemente sull'elemento umano, è imperativo che tutti i professionisti della sicurezza comprendano l'argomento dell'ingegneria sociale. Ma c'è molto di più. Ricordo che quando iniziai a lavorare come chef (in un'altra vita, molto tempo fa), il mio maestro prendeva gli ingredienti e mi diceva di assaggiarne piccoli pezzi, uno per uno. Ma perché?

Mi disse che non potevo sapere che cosa significasse "assaggiare" se non avessi capito veramente qual era il gusto di ogni ingrediente. Se so che la ricetta richiede un po' di rafano e voglio che sia un po' più piccante, capisco che potrei aggiungerne un pizzico di più. Capire che un certo ingrediente ha anche un gusto salato potrebbe farmi correggere il sale per la ricetta, in modo che il piatto non sia troppo salato. Insomma… avete capito. Anche se lavorate nel settore della sicurezza, è importante che conosciate il "gusto" di ognuno di questi ingredienti, in modo da proteggervene. Che cosa significa costruire un legame con qualcuno e come può essere sfruttato per ottenere del denaro? Lo vedremo nel Capitolo 5. In quale modo l'influenza, quando viene usata in una conversazione di richiesta, obbliga qualcuno a comunicarvi la sua password al telefono? Lo vedremo nei Capitoli 6 e 7.

Ognuno di questi ingredienti può aiutarvi a raffinare il vostro "gusto". Una volta che li avrete assaggiati, potrete riconoscerli quando qualcuno tenterà di metterli in atto con voi e così sarete più sicuri. Se percepirete che qualcosa non va, potrete prendere le necessarie azioni difensive.

Avete mai assistito a una gara di cucina con Gordon Ramsay? Quando assaggia un piatto che detesta, identifica il problema specifico: "Questo piatto ha troppo pepe e ci hai messo troppo olio". Un inesperto, al contrario, potrebbe dire: "È troppo piccante e unto". Queste due descrizioni sono davvero uguali? Io penso di no. Il mio obiettivo è quello di aiutarvi a diventare un Gordon Ramsay del mondo dell'ingegneria sociale, ma… forse usando un linguaggio un po' meno volgare.

Detto questo, saltiamo nel primo capitolo "sostanzioso" e parliamo dell'OSINT.