**L'arte dell'inganno - I consigli dell'hacker più famoso del mondo**
**di Kevin D. Mitnick e William L. Simon (2003)**
**Premessa di Steve Wozniak**
**Traduzione di Giancarlo Carlotti**
**Consulenza scientifica di Raoul Chiesa**
**Editore Italiano: Universale Economica Feltrinelli/Saggi**

**Appunti di Antonio Bonaccorso - ADI_v.1.0**

Gli autori a pag. 9 definiscono la nozione di **Ingegneria Sociale.**
Personalmente credo che si possa sintetizzare invece come lo studio e l'analisi empirica, e non frutto di conoscenze scolastiche di base, dei modelli comportamentali umani al fine di imporre in mala fede e senza alcun titolo la propria volontà agli altri ed al fine di ottenere in modo fraudolento da questi informazioni pur agendo in piena asimmetria informativa.

**Dispositivo dell'art. 640 Codice Penale Italiano (aggiornato al 4/Novembre/2021)**

Chiunque, con artifizi o raggiri(1), inducendo taluno in errore(2), procura a sé o ad altri un ingiusto profitto con altrui danno(3), è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032(4)(5).
La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549(6):

1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare(7)(8);
2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità [649](9);
2-bis) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5(10).
Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente o la circostanza aggravante prevista dall'articolo 61, primo comma, numero 7(11).

**Premessa**

Steve Wozniack chiarisce la ragione per cui un essere umano possa dedicarsi allo studio della scienza in generale o delle scienze sociali, ossia la semplice curiosità. L'ingegneria sociale è l'altra faccia della medaglia di tale ricerca, dove l'attore (definito in questo testo "attaccante") agisce per mera esternazione di capacità-intelligenza e non solo per banale fine economico, anche se queste variabili fra loro sono complementari e non succedanee per la causa dell'ingegnere sociale. Allo stesso tempo Wozniack puntualizza che Mitnick non è più ormai un ingegnere sociale e che il testo in questione possa, attraverso gli "Use Cases" citati (definiti nella trattazione "aneddoti") e le puntualizzazioni pratiche, rappresentare un valido strumento per fissare i protocolli interni di controinformazione/controspionaggio o sicurezza offensiva degli enti privati e pubblici.

[Questi appunti non intendono sostituirsi al testo in questione. Inoltre sono una mia personale visione degli argomenti trattati che esperti del settore potrebbero non condividere (autori compresi). Si consiglia pertanto, qualora fossero argomenti oggetto d'esame per un corso di studi professionalizzante, di fare esclusivamente riferimento al testo in questione ed alle lezioni del vostro corso accademico o di perfezionamento.]

**Prefazione**

Nella prefazione l'autore Mitnick descrive una breve autobiografia dove definisce alcuni concetti basilari e precisa di essere consapevole, specialmente dopo il suo arresto, degli aspetti illegali dell'ingegneria sociale. Le nozioni citate sono:
**Cracker**, o **pirata informatico**, è un esperto di sicurezza informatica che per vandalismo si introduce illegalmente in una rete e poi nei correlati sistemi informatici danneggiandoli; l'hacker invece è un esperto di sicurezza informatica che dedica le proprie competenze, secondo etica, al fine di migliorare i dispositivi informatici, nonché la loro sicurezza.
Un **lamer** è un cracker ancora in erba con conoscenze informatiche limitate e basilari, che impiega programmi realizzati da terzi seguendo le guide che circolano per il web.
**Script kiddie** è un termine dispregiativo che sostanzialmente si riferisce ai lamers che si vantano di essere grandi *guru* dell'informatica.
**BBS o Computer Bulletin Board Service o CBBS** è un programma per server che consente agli utenti di postazioni remote di effettuare delle condivisioni attraverso l'emulatore di terminale.
**Phreaking Telefonico** è una tecnica che prevede l'impiego di hardware, software ed ingegneria sociale (incluso speech tech e linguaggio aziendale per ottenere autorevolezza nei confronti dell'interlocutore) per poter eludere la sicurezza delle compagnie telefoniche per svariati fini (cracking, spionaggio industriale o semplicemente per fare delle telefonate gratuite a discapito di un utente telefonico terzo).

**Introduzione**

In questa parte gli autori espongono in breve gli argomenti anche se la trattazione in generale, nonostante lo schema sottostante, rimane piuttosto frammentata.

**Prima parte** Il Fattore Umano - Anello debole cap. 1
**Seconda parte** Fiducia e Sentirsi Utili cap. 2 a cap. 9
**Terza Parte** Infiltrazione, furto e cyberterrorismo - minacce interne ed esterne cap. 10 a cap. 14
**Quarta Parte** Addestramento alla sicurezza Cap. 15 e Vademecum
**Sicurezza in breve** Checklist

In realtà, nonostante la volontà degli autori di catalogare gli use-cases, il lettore dovrà essere piuttosto elastico e non avere fretta di assimilare le informazioni essenziali contenute nel testo. Si ribadisce pertanto che la lettura del testo in tutte le sue parti è imprenscindibile.

**Prima parte: Il Fattore Umano - Anello debole**

<<Il naturale desiderio di protezione assoluta spinge molte persone a cullarsi di un falso senso di sicurezza>> pag. 23.

In questa prima parte gli autori evidenziano come l'affidamento a sistemi o protocolli di sicurezza invalicabili possano illudere i bersagli di essere esenti da minacce. Si chiarisce pertanto un primo caposaldo fondamentale per qualsiasi sistema di sicurezza, ossia: tutto ciò che è stato costruito dall'uomo può essere smontato, ricostruito e personalizzato. In questa parte inoltre vengono evidenziate le falle dovute al fattore umano. Spesso al riguardo (e non solo) serie televisive o cinematografiche citano le seguenti frasi fatte:

<<Distrazione, diversivo, divisione>> per l'attacco
<<Posizione, controllo, dominio>> per la difesa offensiva

In "decifrare il codice" nel 1978 l'attore Rifkin, un impiegato di una banca, sfrutta la debolezza del personale della sua stessa società di appuntare con un bigliettino su una bacheca un codice di sicurezza interno. Oggi computer e smartphone sono dotati di tecnologie o pellicole per oscurare lo schermo ed impedire la vista periferica onde evitare sguardi inopportuni di terzi posizionati dolosamente vicino alla postazione del bersaglio (in gergo questo tipo di attacco si chiama "*shoulder surfing*"). Questa fase può essere associata alla "distrazione", anche se in questo caso non è stata indotta dall'attaccante. L'attaccante si finge un altro impiegato interno della società per ingannare un'impiegata vittima del suo raggiro. Quando la vittima chiede un ulteriore codice interno per confermare la transazione fra reparti distinti della società, l'attaccante mantiene la sua "posizione" ed attua un "diversivo" chiedendo di poter richiamare per controllare la "documentazione sui protocolli interni in suo possesso". Quindi sfruttando "la divisione" interna dei reparti, l'attaccante contatta un altro impiegato sotto un altro alias e con ulteriore scusa gli chiede l'informazione necessaria per assumere il "controllo" sulla prima vittima. Ricontattata la prima vittima assume definitivamente il "dominio" sulla società perpetrando una truffa informatica da 10 milioni di dollari, di fatto sottomettendo i protocolli di sicurezza interni e di riflesso gli altri impiegati e la stessa società.
Se siete degli amanti delle frasi fatte il soprastante esempio può essere sintetizzato in:

<<Distrazione, posizione, diversivo, divisione, controllo, dominio>>

Le tecnologie utilizzate genericamente come contromisure aziendali sono: strumenti di autenticazione (verifica dell'identità); controllo dell'accesso (files e risorse del sistema) e sistemi di rilevamento delle intrusioni.

La sorgente della "distrazione" può essere un pretesto attuato nel tempo con pazienza, carisma, insistenza, disinformazione, suggestione, manipolazione, ecc. L'attaccante, abile nei rapporti umani, per perpetrare il raggiro sfrutterà della sua vittima il "rapporto fiduciario", la "presupposizione di buona fede", "il credo religioso", "l'immotivato senso di colpa", "la logica del grado", ecc. Per difendere l'informazione pertanto occorre essere consapevoli dei pericoli, vigili ed aggressivi nella protezione della propria privacy.

<<La sicurezza aziendale è questione di equilibrio. Una scarsa sicurezza lascia vulnerabile l'impresa, ma un eccesso intralcia gli affari, bloccando la crescita e la prosperità dell'azienda stessa. Il problema è come ottenere un bilanciamento tra sicurezza e produttività>> pag 31

**Parte Seconda - Fiducia e Sentirsi Utili cap. 2 a cap. 9**

**cap. 2 Il valore dell'informazione ritenuta inutile**

Come può un ingegnere sociale giungere alla sua meta? Deve necessariamente trattarsi di un bene materiale o virtuale con "Diritti di proprietà intellettuale" oppure di "un segreto industriale"? In realtà un ingegnere sociale può essere chiunque anche: un tagliatore di teste che cerca di acquisire illegalmente informazioni sul personale con esperienza già impiegato in un'azienda concorrente per poi proporgli un incarico; un investigatore privato o un agente di polizia che illegalmente (in gergo "in libera iniziativa") tenta di carpire informazioni sulla vittima (anche quelle che sembrano banali) per sfruttarle contro terzi o contro lo stesso bersaglio. L'ingegnere sociale pertanto sfrutta "tutta l'informazione" che può estorcere dalle sue vittime,

persino quella ritenuta innocua come ad esempio l'organigramma del personale di un'azienda. Quindi un banale termine tipico del linguaggio aziendale della società A come "Merchant ID" può essere fondamentale per fingersi un impiegato della società A ed ottenere autorevolezza e fiducia da parte di un impiegato della società B. Difatti non conta il mero codice associato al "Merchant ID" bensì l'accenno al termine tecnico del linguaggio aziendale della società A in sé. Tra l'altro il "Merchant ID" è solitamente un codice identificativo assegnato ad ogni membro del personale. E come si fa ad ottenere informazioni apparentemente banali? Semplicemente fingendo di essere: un rappresentante di una società di statistica; uno studioso; uno scrittore; uno scolaretto desideroso di apprendere l'antica arte perduta dall'egocentrico di turno, dal probo eroe; costruendo un alias appartenente alla stessa categoria sociale della vittima affinché quest'ultima possa facilmente immedesimarsi nelle problematiche eccepite dall'ingegnere sociale; proponendo un bellissimo regalo-premio come ad esempio un viaggio con tutte le spese già pagate; ecc.. Infine basta tempestare la vittima di domande, celando le richieste chiave tra quelle inutili al vostro scopo, misurandone il quantitativo o l'oggetto ad istinto. E la vittima improvvisamente si trasformerà nel vostro "aggancio" (in gergo criminale) contro il vostro vero obiettivo e le informazioni carpite, persino quelle ritenute inutili, saranno la moneta di scambio per ottenerne la fiducia o ricattarlo.

Nel primo dei tre esempi di questo capitolo viene citato il CREDITCHEX che in Italia corrisponde al CRIF - Registro cattivi pagatori della Centrale Rischi Finanziari S.p.A.
Nel secondo esempio viene citata la "mail drop" che è una casella postale utilizzata dagli ingegneri sociali per ricevere informazioni cartacee dalle vittime, da non confondersi con il servizio "mail drop" per gli allegati mail troppo pesanti per le comuni mail e che vengono condivisi sottoforma di link in quest'ultime.
Nel terzo esempio viene citato il "Social Security Number" o SSN che corrisponde in Italia al codice fiscale.

**cap. 3 L'attacco deve essere necessariamente complesso? No, basta il gaslighting.**

Il gaslighting è una componente fondamentale per un ingegnere sociale nella sua tattica ed è una forma di violenza psicologica. Si tratta di una tecnica utilizzata non solo da persone notoriamente criminali, ma soprattutto da insospettabili individui con un'intensa attività sociale, molto abili nei rapporti umani e ben affermati nel contesto professionale-lavorativo come servizi segreti, militari, agenti di polizia, politici, giornalisti, informatici, medici, giudici, avvocati, insegnanti, criminologi, ingegneri, psichiatri, psicologi, impiegati di enti pubblici, ecc.., che in realtà celano un indole "prevaricatoria" (la stessa indole che ha consentito loro di ottenere senza troppi scrupoli e probabilmente a discapito di terzi una delle summenzionate posizioni sociali) e poco propensi ad accettare un dialogo con il prossimo e soprattutto di confermare le sue scomode verità. Tale tecnica prevede che vengano presentate al bersaglio false informazioni o inscenati eventi bizzarri con l'intento di far dubitare lo stesso bersaglio della sua memoria e percezione (e di conseguenza disorientare la vittima ed allo stesso tempo negargli qualsiasi attendibilità). Viene notoriamente attuata nei confronti dei whistleblowers insieme con l'ostracismo e la macchina del fango.
Un esempio di gaslighting e di gang-stalking sono gli scherzi organizzati dal noto programma televisivo italiano "SCHERZI A PARTE" (per quanto di fatto possano concludersi con le risate e l'approvazione della stessa vittima).

Precisato ciò, nel capitolo sostanzialmente viene evidenziato come la conquista della **fiducia** della vittima da parte dell'ingegnere sociale sia essenziale affinché la sua tattica possa avere buon fine. La fiducia della vittima può

essere conquistata nel corso del tempo o istantaneamente dall'ingegnere sociale fingendosi un collega alla mano, un amico o un cliente entusiasta del servizio offerto dalla stessa vittima o dalla società della vittima. Inoltre il colloquio con la vittima, le domande dirette e gli argomenti affrontati dovranno essere espressi attraverso un linguaggio tecnico-aziendale familiare alla vittima per ottenere autorevolezza e ciò implica una conoscenza degli usi-abitudini della vittima in sé o della società per cui lavora, nonché dell'organigramma del personale della società (compreso il dislocamento delle sedi e dei reparti).

Negli esempi trattati da questo capitolo vengono citate le sottostanti nozioni:

**MLAC** Centro per l'assegnazione automatizzata delle linee (USA)
**NCIC** Centro Nazionale informazioni sul crimine (USA)
**loop-around** è un numero telefonico riservato impiegato dalle compagnie telefoniche per testare le linee telefoniche e presente negli elenchi di numeri di collaudo. Vengono utilizzati dai phreaks per chiamare o farsi chiamare gratis.
**SIFC** Sistema informazioni fatturazioni clienti (USA)

**cap. 4 Costruzione della fiducia**

<< L'ingegnere sociale anticipa sospetti e resistenze, ed è sempre pronto a ribaltare la sfiducia in fiducia. Se è in gamba programma l'attacco come se fosse una partita a scacchi, anticipando le domande che il bersaglio può porgli in modo da avere sempre la risposta pronta >> pag. 56

Ho volutamente modificato molti titoli dei capitoli concentrando in essi le argomentazioni essenziali degli aneddoti trattati dagli autori.
In questo capitolo l'ingegnere sociale procede per fasi per la conquista della fiducia della vittima e la programmazione di tali fasi avviene non come una partita a dama, bensì a scacchi dove è prevista una strategia che di fatto anticipi le mosse dell'avversario. Il gioco degli scacchi però è di derivazione militare e nelle operazioni militari niente va per il verso giusto. Pertanto l'ingegnere sociale dovrà adattarsi a qualsiasi esternalità imprevedibile seguendo solo il suo istinto.

**Improprio senso del dovere** L'ingegnere sociale agisce su incarico di terzi o su iniziativa personale e mai per eroismo o virtù. Per quanto l'ingegnere sociale giustifichi ai terzi le sue azioni quasi fosse il perseguimento di una causa nobile, non lo è mai. La vera ragione di tale mistificazione è lo sminuire le implicazioni morali o legali della sua condotta ed ingiuriare il bersaglio in modo che venga "stigmatizzato" e non riceva aiuto sostanzialmente da nessuno. Ciò che spinge davvero un ingegnere sociale a muoversi contro il bersaglio è un interesse personale di natura economica o una gratifica correlata alla sua posizione sociale (che sostanzialmente la consolidi). Ovviamente l'ingegnere sociale proprio per la sua abilità nei rapporti umani cela ai terzi il suo improprio senso del dovere (o genericamente "intento") palesandosi come un eroe e magari manipolando la sua vittima a provare un immotivato senso di colpa. [La versione di Doyle Lonnegan - pag. 58]
**Cooperazione - Gang-Stalking** L'ingegnere sociale potrebbe avvalersi della cooperazione della malavita organizzata o di individui equivoci per danneggiare o ingiuriare il bersaglio in modo che venga stigmatizzato e non possa difendersi adeguatamente dal suo attacco, neppure con l'aiuto dei suoi stessi congiunti. Così facendo gli giudici straordinari di turno saranno sempre pronti a linciare il bersaglio. [La versione di Doyle Lonnegan - pag. 58]
**Empatia e fiducia mal riposta** L'ingegnere sociale è un abile stratega. Pianifica per tempo ogni sua azione improvvisando solo per mantenere la sua "posizione" nei confronti del bersaglio quando richiede delle informazioni non previste. Il bersaglio viene avvicinato dall'ingegnere sociale sin dal primo approccio

affinché provi empatia e fiducia. La pietà, l'appartenenza alla stessa categoria sociale, gli elogi, ecc. sono un'ottima leva per manipolare il bersaglio. [La versione di Doyle Lonnegan - pag. 58]
**Incauto senso di invulnerabilità** Un potenziale bersaglio non deve sostanzialmente mai cullarsi per il progredire tecnologico dei sistemi sicurezza (hardware ed addestramento del personale) in quanto niente è esente da rischi. I databases interni delle società e la raccolta dati sono il primo tallone di Achille di qualsiasi sistema di sicurezza in particolare delle carte di credito. Pertanto meglio utilizzare carte prepagate per gli acquisti (anche non online) piuttosto che carte di credito direttamente collegate ai conti corrente [Papà sorpresa - pag. 59]
**Logica del grado ed ingenua condivisione delle procedure interne** I databases delle forze dell'ordine e degli addetti alla sicurezza sono una ghiotta fonte di informazione per gli ingegneri sociali che sostanzialmente si palesano come superiori di rango per non ricevere troppe eccezioni dalla vittima di turno. Quest'ultima difatti per deformazione professionale (e per l'addestramento ricevuto) tende a non porre troppe domande ai suoi superiori onde evitare ripercussioni disciplinari. Gli ingegneri sociali, per acquisire la proprietà di linguaggio dell'ente bersaglio, inoltre sfruttano i manuali dei protocolli interni o d'uso dei database riservati solo agli appartenenti dell'ente bersaglio (e condivisi pubblicamente via internet per addestrare il personale dislocato in diverse sedi, città o paesi). [Hacking ai federali - pag. 64]

**cap. 5 Un nuovo amico o una nuova amica del cuore, il ragazzo o la ragazza della porta accanto oppure il dolce angelo dalla voce suadente; l'avvocato irreprensibile che si promuove come un procacciatore d'affari; il soldato senza macchia pronto a vendere chiunque per un gallone in più; l'insegnante probo amante dello scambio di favori al limite della mafia; ecc. ... Indovina un po'? Tutti pronti a risolvere i vostri guai!**

<< Siamo tutti molto grati quando siamo assillati da un problema e una persona competente, abile e disponibile si offre di darci una mano. L'ingegnere sociale lo sa, e sa anche come approfittarsene.
Sa anche come causare quel vostro problema ... poi ottenere la vostra gratitudine appena ve lo risolve... e alla fine giocare sulla gratitudine per estrarre informazioni e ottenere un piccolo favore da voi, lasciando la vostra azienda (oppure voi individualmente) in condizioni ben peggiori rispetto a prima dell'incontro. E forse non saprete nemmeno di aver perso qualcosa di prezioso. >> pag. 68

L'attaccante agisce negli esempi descritti in questo capitolo secondo uno schema prefissato che adatta di volta in volta in base al contesto o alla situazioni in generale.

Genericamente riassumibile in:

1) Individuazione finalità missione
2) fase ex ante - asimmetria informativa
   A) Utilizzo o acquisto a basso costo di tecnologie che non consentano di essere rintracciati - L'attaccante non andrà mai sul posto di persona per l'acquisizione di documentazione "dal vivo" (live drop) ed userà fax, dead drop (ftp), dead letter box (mail e cassette postali), ecc.
   B) raccolta informazioni (organigramma personale ente, ubicazioni sedi ente, dati personali impiegati - nonché se possibile credenziali autenticazione eventualmente ottenuti attraverso un attacco a dizionario) - in gergo questa fase viene definita *foot print*
   C) individuazione del bersaglio
   D) individuazione degli agganci (terze parti)

3) Attuazione social engineering, reverse social engineering (ovvero il “controfavore” dal bersaglio o dall’aggancio)

**La tela del ragno - il reverse social engineering**

<< L’attaccante tesse una tela per convincere il bersaglio di avere un problema che in realtà non esiste, o in questo caso un problema che non si è ancora verificato ma l’attaccante sa che si presenterà perché sarà lui a provocarlo, per farsi poi vivo come la persona in possesso della soluzione. >> pag. 72

<< Se un estraneo vi fa un favore e poi vi chiede un controfavore non ricambiate senza aver riflettuto attentamente su cosa vi sta domandando. >> pag. 72

**Bersagli e agganci (terze parti vere o interpretate dall’ingegnere sociale) negli esempi:**

<< La priorità di chiunque in un’impresa è completare il proprio lavoro in tempo. Quando si è sottoposti a questa pressione spesso le procedure di sicurezza passano in secondo piano e sono trascurate ed ignorate >> pag. 82

<< Di solito, il personale ricopre ruoli e responsabilità diversi e ogni posizione ha una determinata vulnerabilità >> pag. 84

1) neoassunti (in quanto non conoscono procedure ed il personale - sono altamente collaborativi con l’attaccante)
2) assistenza (ruolo interpretato spesso dall’attaccante)
3) contabilità (per acquisizione dati personali)
4) IT (per disattivazione connessione di rete dei nodi attraverso il port number - simulazione guasti)
5) addetto corriere spedizioni (ruolo interpretato dall’attaccante per ottenere indirizzi abitativi e numeri telefonici personali)

**Protocolli basilari di sicurezza:**

Informazioni riservate
1) Nessuna collaborazione con estranei
2) Identificazione “sorgente” richieste - L’attacco può provenire dall’interno (come una richiesta verso/per un dipartimento interno)

**cap. 6 Fingersi in difficoltà o debole per ricevere aiuto dal bersaglio**

L’attaccante può essere potenzialmente interno e/o esterno all’ente o all’attività del bersaglio.

<< Un’altra tattica classica sceglie la procedura inversa: l’ingegnere sociale manovra la vittima fingendo di avere bisogno che l’altro gli dia una mano >> pag. 86

I cases proposti come esempi in questo capitolo sfruttano lo svantaggio delle sovradimensioni dell’ente bersaglio che generalmente posseggono una wide area network con una sicurezza piuttosto liquida e non solida denominata affettuosamente “candy security”.

Lo “speakeasy” è una tecnica di sicurezza di alcune società che si inspira sostanzialmente alla sicurezza dei locali dove si vendevano alcolici durante l’epoca del proibizionismo, dove il matching fra “una parola d’ordine” (lo speakeasy) e la conoscenza dell’esatta posizione del locale (abilmente celato agli occhi dei non consociati) consentiva l’accesso ai servizi. Il matching fra queste due variabili viene denominato “security through obscurity”.

Quindi nel caso di una società si presume che solo gli impiegati autorizzati conoscano il gergo e la posizione da dove richiedere il servizio senza necessità di autenticazione attraverso un nome utente ed una password. (L'ho visto al cinema - pag. 89)
Da qui la necessità di sistemi sempre più complessi per la crittografia delle comunicazioni come gli scrambler (Sintonizzarsi  pag. 91).

L'ANI (Automatic Number Identification) è un programma per gli istituti di credito per confrontare il numero del chiamante con l'elenco dei numeri associati agli account-utente dei servizi dell'istituto di credito.

Il secure-id o "time-based token" è un ulteriore mezzo-strumento (grande come una carta di credito o una penna usb) per convalidare l'username di un utente, attraverso un pin segreto che varia nel corso nel tempo. Purtroppo ha le sue falle dovute al fattore umano (Danny l'intercettatore - pag. 91)

**Controffensiva:**

1) Verificare il numero interno del chiamante (confrontandosi con la voce registrata in segreteria);
2) Conservare meticolosamente i numeri di matricola degli impiegati;
3) Non convalidare l'identità di un impiegato attraverso sistemi speakeasy;
4) I managers devono rispettare gli stessi protocolli di sicurezza degli impiegati;
5) Non condividere il secure-id o altri sistemi a tempo con altri impiegati.

**cap. 7 "Nessuno regala niente a questo mondo" oppure "quando è troppo bello non è vero"**

<< Però il trucco di offrire qualcosa gratis è ancora una grossa esca sia per gli affari legittimi ("Aspetti, non è finita! Se chiama subito aggiungiamo un set di coltelli e la macchina per fare i popcorn!") e meno legittimi ("Se compra un ettaro di palude in Florida gliene diamo un secondo gratis!") >> pag. 100

Il bersaglio/aggancio viene attirato attraverso "vantaggi" di qualsiasi natura, che poi si rilevano "fittizi" (viaggi premio, offerte black friday, massaggi terapeutici in centri spa, ecc.) o "effimeri" (pornografia; software, giochi, film, musica, immagini distribuiti legalmente o illegalmente; seduzione-relazioni romantiche; ecc.), ma soprattutto altamente lesivi per lo stesso bersaglio.

L'attacco viene implementato sia attraverso ingegneria sociale (anche tramite agganci inconsapevoli o consapevoli), sia tramite mezzi tecnologici come:
- posta elettronica (allegati);
- siti civetta (siti clone).

L'attaccante può agire in live drop fingendo sostanzialmente di aiutare il bersaglio/aggancio o chiedendo aiuto al bersaglio/aggancio attraverso: software in regalo; consulenza o perizia informatica; film, musica, immagini, documenti; ecc.

Il bersaglio/aggancio sostanzialmente:
- concede i propri dati sensibili direttamente attraverso i siti civetta (compresi i dati sensibili di carte di credito) oppure indirettamente tramite virus;
- infetta solo la propria home directory (se non usa un account con titolarità dei diritti dell'amministratore) o l'intera macchina (se usa un account con titolarità dei diritti dell'amministratore);

- installa inconsapevolmente worms, rootkits (una collezione di malware), backdoors, ecc.;

L'attaccante potrà quindi potenzialmente disporre:
- dei dati personali del bersaglio/aggancio (compresi i dati sensibili delle carte di credito);
- del controllo in remoto delle macchine/dispositivi del bersaglio/aggancio (ovvero potrà anche intercettare illegalmente il bersaglio/aggancio tramite webcams e microfoni installati sulle macchine/dispositivi in remoto);
- chiavi di criptazione e passwords in generale del bersaglio/aggancio.

**Controffensiva:**

- Valutare la sorgente di qualsiasi tipo di file a prescindere dal mezzo di acquisizione (usb, mail, browser, riga di comando, ecc.) o dal proprietario/ autore;
- Utilizzare i files altrui attraverso: macchine virtuali; account senza titolarità di diritti di amministrazione; firewalls e software antivirus;
- Per ragioni di privacy usufruire di monitor o laptop privi di webcam o microfono o quantomeno che possano isolare le suddette componenti elettricamente.

**cap. 8 Autorevolezza, simpatia, senso di colpa, intimidazione ... Come gli ingegneri sociali (truffatori, delinquenti, avvocati, periti di parte, investigatori privati, insegnanti universitari, forze dell'ordine, servizi segreti, mafiosi, brokers di informazioni, ecc. insomma "chiunque") si approfittano delle vostre "reazioni automatiche" per danneggiarvi o distruggervi**

<< I più abili sono molto bravi a impostare un raggiro che susciti emozioni tipo paura, eccitazione o senso di colpa, e ci riescono facendo scattare dei pulsanti psicologici, dei meccanismi automatici che inducono le persone a rispondere alle richieste senza fare un'analisi approfondita di tutte le informazioni disponibili >> pag. 111

Nei cases presi ad esempio in questo capitolo persino il personale esperto di tribunali, forze dell'ordine o università non è esente da attacchi, specialmente se l'attaccante conosce l'organigramma dell'ente bersaglio.

Il "name dropping" ovvero il citare il nome di un interno dell'ente o genericamente di una persona nota è un'ottima arma per accattivarsi la simpatia dal bersaglio/aggancio o suscitare in generale in lui/lei emozioni in reazione automatica.

<< Signora Wang sono Arthur Arondale dell'Ispettorato generale. Possiamo darci del tu, May? >> (La telefonata a May Linn pag. 118)

Gli autori inoltre precisano:

**<< Non tutti coloro che usano le tecniche di ingegneria sociale sono ingegneri sociali. Chiunque conosca i segreti di una data azienda può diventare pericoloso. >> pag. 114**

Ovvero anche ex impiegati che ritengono disconosciuto o non apprezzato il loro operato dal datore di lavoro o dai colleghi in generale.

<< L'intimidazione può creare la paura della punizione, costringendo la gente a collaborare. Inoltre, può anche far nascere la paura dell'imbarazzo o di essere esclusi dalla prossima promozione >> pag. 117

Solitamente avviene quando il truffatore si palesa come un superiore o un appartenente alle forze dell'ordine. Le frasi solite sono "Lei è consapevole ..."; "Lei rischia ..."; "Ha le prove ..."; "Confessi ..."; "Deve essere processato ...".

Ricordatevi in questi casi che se qualcuno vi interpella riguardo ad un atto o un fatto voi non dovrete MAI dimostrare nulla al riguardo (neppure la vostra innocenza) a meno che la suddetta richiesta sia a seguito di un atto di un giudice. Fate inoltre attenzione a non concedere documentazione in generale o dispositivi a pseudo "cavalieri mascherati". L'intimidazione difatti può essere giustificata e minimizzata dagli attaccanti per ottemperare ad uno "scopo superiore" (ad esempio "diritti civili", "diritti ambientali", "sicurezza nazionale"; ecc.) o con la scusa di far valere un vostro diritto. Nella maggior parte dei casi però si tratta di un acquisizione di informazioni su un bersaglio/aggancio (ossia "un povero cristo ingenuo ed innocente") con una buona dose di discredito e stigmatizzazione.

In "La versione di Peter" pag. 123 l'attaccante usa come:
- "Distrazione" - la paura dell'aggancio/bersaglio del computer guasto;
- "Diversivo" - l'apertura del bersaglio/aggancio di applicazioni innocue mentre l'attaccante da remoto "assiste" seguendo passo dopo passo la vittima per conquistarne la fiducia (con una buona dose di gaslighting);
- "Divisione" - l'attaccante pur essendo vicino alla vittima opera di fatto da remoto, celando così "visivamente" anche la sua effettiva attività in corso al bersaglio/aggancio quindi:
  - dapprima l'attaccante ottiene il cambio "innocuo della password" di Windows dal bersaglio/aggancio con la scusa di un test
  - poi l'attaccante installa da remoto un'applicazione sul computer del bersaglio/aggancio, eleva i suoi "privilegi di sistema" e cancella il registro dei logs con un'applicazione "clearlogs" (per nascondere l'attacco).

**Protocolli basilari di sicurezza (contro forze dell'ordine, militari, servizi segreti, avvocati, giudici, esperti di tribunale, ecc. in mala fede):**
1) Onde evitare conseguenze e ripercussioni dovrete conoscere il vostro nemico - Sappiate che gli appartenenti alle forze dell'ordine, militari, servizi segreti, avvocati, giudici, esperti di tribunale, medici, liberi professionisti, ecc. non amano particolarmente essere denunciati e sono spesso legati a pseudo gruppi politici/sociali che sono la facciata legale di malavita organizzata e populisti violenti (di destra e di sinistra) - gruppi che in fin dei conti hanno contribuito alla loro stessa scalata sociale tramite raccomandazioni e cooptazione. Potreste subire in gang-stalking come whistleblower: denunce a tappeto, macchina del fango, minacce e violenze fisiche, discredito e stigmatizzazione (in modo da precludervi qualsiasi entrata di natura economica ed annullarvi nel contesto sociale - fino a farvi passare per malati di mente).
2) Lupo non mangia Lupo - Non riceverete aiuto da nessuno a meno che non siate Russel Crowe e non stiate recitando con Al Pacino in "The Insider". Quindi tenete i vostri dispositivi e documenti al sicuro e non tentate nemmeno a dimostrare le violenze subite (non vi ascolterà nessuno).
3) Dal punto di vista legale limitatevi ad una strategia difensiva meno costosa possibile ed al massimo lasciate che altri parti interessate si confrontino duramente (in tribunale) un giorno al posto vostro. Ovvero tanto "la gatta va al lardo che ci lascia lo zampino". In sostanza, non esponetevi se non è necessario, mai!
4) La "prova" è sempre "diabolica", pertanto lasciate sempre agli altri l'onere di dimostrare qualunque cosa.

**Controffensiva:**
1) Addestrare il personale a non fidarsi di nessuno ed a non accettare bevande o alimenti o altro (penne usb, cd, ecc.) da nessuno (solo il paranoico sopravvive!);

2) Preparare una checklist di domande per identificare i privilegi e le autorizzazioni del personale interno e di terze parti;
3) I dipendenti (impiegati, managers) dovranno frequentare studi clinici-medici con avanzata sicurezza IT onde evitare che possa essere compromessa dolosamente la loro salute (o la loro capacità cognitiva) per estrometterli parzialmente o del tutto dalle loro mansioni oppure per sostituirli con agganci consapevoli (troverete su YouTube su questo argomento un video promosso da HP denominato "The Wolf - La Caccia Continua" con Christian Slater);
4) I rapporti interni fra superiori e semplici impiegati/manovalanza dovranno essere basati sul reciproco rispetto e sulla reciproca osservanza dei protocolli di sicurezza;
5) Si dovrà mettere in atto una "compartizione" dell'informazione. Difatti, organigramma a parte, l'informazione dovrà essere condivisa fra interni limitatamente alle loro mansioni;
6) MAI condividere i protocolli aziendali (e se possibile neppure l'organigramma onde evitare il "name dropping") via internet e MAI promuovere lo speakeasy.

**cap. 9 La stangata inversa**

<< Le truffe tradizionali, quale che sia il trucco specifico, seguono sempre uno schema. In certi casi, però, procedono in direzione opposta e allora sono chiamate "stangata inversa", un balletto intricato in cui l'attaccante dispone le cose in modo che sia la vittima a chiamare *lui* per chiedere aiuto, oppure racconta che ci sarebbe un collega che ha fatto una richiesta a cui lui deve rispondere. >> pag. 135

Fra i delitti di frode l'ordinamento italiano attraverso l'art. 640 del cp delinea la truffa in generale: << Chiunque, con artifizi o raggiri(1), inducendo taluno in errore(2), procura a sé o ad altri un ingiusto profitto con altrui danno(3), ...>>

Genericamente in tutto il mondo vengono identificate tre tipi di truffe:

- *Truffa assicurativa* (messa in scena o aggravamento delle conseguenze di un sinistro; falsificazione di documenti compresa la polizza del contratto di assicurazione)
- *Truffa aziendale* (attività inesistente - di facciata; prodotti-servizi esistenti ma non all'altezza della loro descrizione; attività basate su schemi piramidali)
- *Truffa informatica* (alterazione dei dati o dei programmi contenuti da un sistema informatico o telematico allo scopo di commettere delle frodi)

Ma l'ordinamento italiano è piuttosto peculiare riguardo ai delitti di frode dedicando loro degli articoli ad hoc nel codice penale:

Delitti di false informazioni al PM (articolo 371-bis cp)
Di falsa testimonianza (articolo 372 cp)
Di frode processuale (articolo 374 cp)
Depistaggio (articolo 375 cp)
Di favoreggiamento (articolo 378 cp)
Ecc.

Inoltre nonostante il noto vulnus del codice penale italiano riguardo al reato di plagio attraverso l'art. 643 cp viene delineata la circonvenzione di incapace, dove l'incapacità non necessariamente deve essere permanente ma meramente temporanea.

**Detto questo come viene messa in atto una truffa?**

L'attaccante prima di mettere in atto la truffa in sé procede con la raccolta illegale di informazioni personali (dati anagrafici, medicinali, abitudini quotidiane, età) sull'aggancio/bersaglio con gaslighting, telefonate, pedinamenti (anche in gang-stalking), interrogazione dei vicini di casa e screditamento della vittima impersonando pubblici ufficiali, amici, tecnici-riparatori, ecc. Dopodiché viene avvicinata la vittima e perpetrata la truffa. L'attaccante per rendere la vittima inoffensiva o non disponibile presso l'ente bersaglio potrebbe anche mettere in atto forme di violenza psicologica nei suoi confronti come avvertimenti, ricatti e minacce (tipiche dell'associazioni mafiose) o lesioni personali (attraverso aggressioni fisiche o somministrazioni di sostanze nocive-psicotrope contro la volontà della stessa vittima e senza che quest'ultima ne sia a conoscenza).

[Un esempio di tali forme di violenza psicologica sono gli avvenimenti che hanno coinvolto anche illustri sconosciuti come: i dissidenti politici dell'Iran da parte della SAVAK durante il regno di Mohammad Reza Shah Pahlavi; i giornalisti che hanno osato fotografare nel luglio del 1981 a Castelgandolfo (Roma) papa Giovanni Paolo II in piscina; personaggi di rilievo nel contesto sociale come il noto virologo Matteo Bassetti (nel suo caso da parte di gruppi no-vax notoriamente legati a partiti populisti di estrema destra e sinistra, nonché di forze dell'ordine, servizi, medicina, politica, avvocatura, liberi professionisti, magistratura, ecc. - gruppi che paradossalmente inneggiano i diritti civili, ambientalisti, i diritti degli animali, ecc. e si dichiarano contro ogni forma di violenza). Nell'ultimo caso citato in sostanza il sopracitato virologo è stato "palesemente" ed "esasperatamente" inseguito, pedinato e fotografato-filmato attraverso dispositivi di registrazione occasionali come i cellulari. L'obiettivo di tale comportamento, volutamente reitero esasperato e non celato, è duplice: instillare nella vittima un timore nei confronti degli aggressori che lo attenzionano in modo che la vittima ritenga gli aggressori autorizzati (persino per i membri delle forze dell'ordine, e non semplici civili, il suddetto comportamento è comunque illegale con o senza un regolare atto di un giudice); allo stesso tempo rappresenta una dimostrazione palese di forza nei confronti della vittima (a modo di legione), che prevede anche il reclutamento temporaneo di individui vicini alla stessa vittima in cambio di utilità o benefici (anche non materiali) - dimostrazioni di forza tipiche delle associazioni mafiose o criminali. Tale collaborazione sempre "palese" ed "esasperata" verrà negata dai complici o dai membri del team qualora la vittima richieda a costoro di pronunciarsi formalmente riguardo a dei fatti accaduti allo scopo di sminuire l'attendibilità della vittima. Gli attaccanti potranno così poi spingersi oltre (minacciando, provocando, tacitando, aggredendo, ingiuriando e screditando oppure mettendo in atto il gaslighting ovvero inscenando degli eventi inverosimili in modo che se raccontanti o denunciati dall'individuo che li subisce possano inficiarne ulteriormente l'attendibilità) sino a rendere la vittima dei loro "giochi" de facto "inerme" ed "isolata" sia per il trauma subito ("annullandola"), sia per lo screditamento nel contesto sociale ("stigma"). La gravità di circostanze simili è che la denuncia del noto virologo ha avuto efficacia solo perché si tratta di una persona di spicco sia nel suo ambito lavorativo, sia nel contesto sociale-politico. Ossia se fosse stato un mero dipendente di una società IT bersaglio o una persona qualunque rea di aver pestato i calli dell'individuo sbagliato (tipico per i whistleblowers) non avrebbe avuto scampo. Anzi è molto probabile che i legali o i consulenti di parte a cui si sarebbe rivolto avrebbero agito contro di lui per danneggiarlo ulteriormente. Da notare che tali organizzazioni con finti scopi altruistici o politici pur essendo civili (del resto persino gli stessi servizi segreti italiani sono "teoricamente" composti da civili) seguono un protocollo paramilitare per attuare le loro violenze (hacking compreso), agiscono quasi sempre in team e trovano molto spesso supporto (logistico e non) da pubblici ufficiali infedeli (che ne fanno parte a

volte di fatto e non di diritto, qualora la forza armata di appartenenza non lo consenta) o da civili semplicemente desiderosi di scaricare le loro frustrazioni sul capro espiatorio di turno. Difatti i servizi, i militari o gli appartenenti alle forze dell'ordine si servono di tali gruppi per consolidare la loro posizione sociale e per rafforzare le loro attività illegali nei confronti del whistleblower di turno. Lo screditamento-stigma inoltre provoca nei confronti della vittima un effetto onda per cui gli attaccanti-stalkers potrebbero non essere più infine dei membri del team originario, ma semplici colleghi o vicini di casa sino a creare un inarrestabile circolo vizioso per la vittima.]

**Ma la *stangata inversa*?**

Nella stangata inversa proposta in questo capitolo invece l'attaccante, oltre a mettere in atto quanto sopra espresso, crea una strategia in modo che siano gli agganci/bersagli a contattarlo (al bisogno anche attraverso hacking - vedi "POLIZIOTTI COME POLLI" a pag. 142) oppure ad interrogarli sulle credenziali personali o delle transazioni fra uffici o dipartimenti, ecc. (vedi "La telefonata a Louis" pag. 136).

Inoltre gli autori precisano che l'attaccante: non deve essere necessariamente un hacker, ma è molto probabile; è un esperto "dell'arte della persuasione amichevole" ossia un individuo non necessariamente cupo o non alla moda, bensì con un'intensa attività sociale.

**La prevenzione dalle frodi**

Donald R. Creseey ed Edwin Sutherland hanno individuato tre elementi essenziali nelle frodi, che di fatto sono stati evidenziati in tutti i cases esposti in questi capitoli. Steve Albrecht ha successivamente definito tali elementi come il *triangolo della frode*.

*Causa-Motivi* -> Il fattore scatenante che induce l'attaccante a commettere la frode

*Logica dell'attaccante* -> Le giustificazioni dell'attaccante nonostante sia consapevole di commettere un reato (dall'improprio senso del dovere al desiderio di ricchezze e denaro)

*Opportunità* -> Le condizioni favorevoli per commettere una frode (ad esempio dovute a delle vulnerabilità dei protocolli o dei meccanismi del sistema di sicurezza)

L'obiettivo del testo preso in esame, come del resto di qualsiasi strategia di sicurezza implementata in base al triangolo della frode, è eliminare il terzo ed ultimo elemento ovvero l'*opportunità*.

**Terza Parte Infiltrazione, furto e cyberterrorismo - minacce interne ed esterne**

**cap. 10 Infiltrazione**

<< Perché è tanto facile per un estraneo assumere l'identità del dipendente di un'azienda e recitare in maniera molto convincente da ingannare persino le persone più pignole? >> pag. 151

In questo capitolo vengono evidenziate attraverso i cases le tecniche per acquisire informazioni dal bersaglio, opportunamente creare un falso profilo con credenziali esistenti ossia quelle di un reale impiegato e poi approfittarsene. Inoltre viene ribadito che persino una pattumiera o un dipendente scontento possono costituire una minaccia.

1) *Celare SEMPRE le proprie competenze di ingegneria sociale o di hacking con TUTTI.* Non dovrà mai importarvi come vi considerano le persone, perché gli individui giudicano gli altri individui in base alle azioni che quest'ultimi sono in grado di compiere (o almeno in base a quelle che ritengano abbiano compiuto o che siano in grado di compiere). << È preferibile che la gente ti sottovaluti, non che ti consideri una minaccia >> pag. 167
2) *Killer Instinct* - L'ingegnere sociale deve essere in grado di "deviare" a suo vantaggio qualsiasi tentativo da parte del bersaglio/aggancio di riappropriarsi della sua percezione della realtà. La realtà che il bersaglio/aggancio deve percepire è soltanto quella imposta dall'ingegnere sociale. In "la versione del custode" a pag. 151 Joe Harper ruba l'identità di un dipendente (Tom Stilton) e poi, per acquisire autorevolezza con il suo interlocutore (Leroy Greene, un guardiano notturno), usa come name dropping il nome del capo squadra del suo alias (Judy Underwood). Quando "Judy" viene chiamata telefonicamente da "Leroy" per confermare la versione di Joe/Tom, quest'ultimo se la fa passare alla cornetta inscenando una discussione inesistente (gaslighting) per far sentire al guardiano notturno quello che desidera, chiudendo poi la cornetta in modo da non far conversare direttamente "Judy" con "Leroy". Il reato di furto d'identità in Italia viene disciplinato dall'art. 494 c.p. (reato di sostituzione di persona).
3) *Dumpster diving* - L'informazione può essere estratta dai cassonetti dell'immondizia (anche dalla documentazione cartacea in brandelli), dal cestino della cartella "home" del bersaglio o dai supporti di memoria. In "cash in cambio di trash" a pag. 159 l'obiettivo (fallito) è lo spionaggio industriale. In Italia il reato di rivelazione di segreti industriali corrisponde all'art. 623 c.p.
4) *Minaccia interna* - In "il capo ufficio umiliato" a pag. 160 un impiegato (Harlan) viene riassegnato con un incarico dequalificante (la pulizia dei servizi igienici) da George, il suo capoufficio. Quindi Harlan sostituisce una presentazione in power point con una modificata con immagini estratte da Playboy per umiliare George durante un meeting aziendale. Il reato di ingiuria è punito dall'art. 594 del c.p.

**Controffensiva:**

1) Distruzione completa dei documenti cartacei o dei manuali cartacei non più utili in modo che gli attaccanti non possano giocare con dei nastri adesivi a modo di puzzle;
2) Rimozione sicura dei files (formattazione sicura del disco o della partizione) e pulizia cache ram, buffer e swap;
3) Distruzione fisica di qualsiasi supporto di memoria inutilizzabile o obsoleto in modo da rendere impossibile il recupero dei files da parte di terzi;
4) Cessazione del rapporto con immediata rimozione dei privilegi (informatici e non) concessi in correlazione all'incarico;
5) Controllo accessi accurato onde evitare "il rimorchio" ossia l'ingresso di persone non autorizzate che semplicemente si sono aggregate a gruppi di dipendenti all'ingresso;
6) Limitare l'accesso internet ad alcuni ambienti interni per impiegati interni alla sede;
7) Impedire agli impiegati di entrare o uscire con supporti di memoria e se non è necessario neppure con tablet/laptop. Il cellulare degli impiegati dovrà utilizzare solo l'accesso alla rete dati della propria sim e non la rete aziendale.

## cap. 11 Si vis pacem, para bellum - Se vuoi la pace prepara la guerra.

È una locuzione latina attribuita a Vegezio a cui vengono associati svariati significati tra cui:

1) Coloro che imparano a combattere apprezzano la pace;
2) Il miglior modo per governare un popolo è creare “un nemico”, approfittando del *metus hostilis* ossia la *paura del nemico*.
3) Il significato invece più immediato “preparare la guerra” o “preparare la difesa in anticipo” è strategicamente errato.

Il concetto di *metus hostilis* è stato evidenziato in tutti i capitoli precedenti ed è alla base di un attacco per la conquista della fiducia di un bersaglio.

<< Un ingegnere sociale sfrutta la propria capacità di manipolare le persone in modo che lo aiutino ad arrivare al suo scopo, ma spesso per il successo pieno ha bisogno di una notevole competenza tecnica e di tanta abilità con i sistemi informatici e i sistemi telefonici >> pag. 173

In questo capitolo senza entrare nel dettaglio vengono puntualizzate alcune qualità negative che deve avere l’ingegnere sociale. Allo stesso tempo viene evidenziata l’illusione di invulnerabilità del bersaglio, spesso dovuta al fatto che questi appartiene a categorie professionali “intoccabili” o ad enti che di fatto esercitano in via diretta il monopolio della forza di uno stato.

Nel sopracitato caso non dovrete mai correggere un nemico tronfio e sicuro di essere invulnerabile.

<< Non interrompere mai il tuo nemico mentre sta facendo un errore >> Napoleone Bonaparte
<< La Bibbia ci dice di amare il nostro prossimo, e anche di amare i nostri nemici; probabilmente perché di solito si tratta delle stesse persone >> GK Chesterton

“Hacking dietro le sbarre” pag. 173 -> speech tech
“Lo scaricamento veloce” pag. 179 -> autorevolezza ed un supporto di memorizzazione digitale
“Soldi facili” pag. 180 -> distrazione e scasso
“L’attacco alle password” pag. 185 -> metodo a forza bruta ed attacco a dizionario

A pag. 184 viene citato il termine “dual-homed host” che genericamente indica un firewall, un proxy o un gateway a supporto delle applicazioni che necessitano di connettersi ad una rete non sicura (come Internet).

***Contromisure*:**

<< Ogni organizzazione deve trovare quel difficile equilibrio tra una forte sicurezza e la produttività del personale, una situazione che porta alcuni dipendenti a ignorare le contromisure, a non capire quanto siano essenziali queste contromisure a salvaguardia dell’integrità di preziose informazioni aziendali >> pag. 191

**cap. 12 Pianificazione Down Top - dal basso verso l’alto**

<< Come dimostrano le tante storie qui contenute, l’ingegnere sociale in gamba prende di mira di solito i lavoratori al livello inferiore della gerarchia. Può essere facile manipolare queste persone in modo che svelino informazioni apparentemente innocue che l’attaccante userà per fare un passo avanti verso il raggiungimento di informazioni più sensibili. >> pag. 193

In questo capitolo viene ribadito il concetto di “anello debole” ed evidenziato il rischio alla sicurezza aziendale dovuto al fattore umano, in particolare a

causa della disinformazione del personale appena assunto e non successivamente addestrato per appianare apparentemente i costi, che invece si trasformano in costi dovuti agli “attacchi” in pieno “paradosso del risparmio”.

Gli autori precisano a pag. 193 (in “L’amichevole custode”) la differenza sostanziale fra i “truffatori” e gli “ingegneri sociali”, non per difendere moralmente i secondi, ma per distinguere “l‘esca” utilizzata per avvicinare i bersagli:
<< I truffatori sperano di trovare sempre persone avide perché più passibili di cascare in un raggiro. Gli ingegneri sociali, quando prendono di mira un addetto alle pulizie o una guardia giurata, sperano di trovare una persona amichevole, paciosa e che si fida degli altri. >>

Sempre nel paragrafo sopracitato, degno di nota è il tipo di attacco informatico al sistema UNIX-like non protetto, che di fatto si tratta di un vero e proprio “attacco fisico”. In pratica la macchina in questione è stata avvicinata dall’attaccante tramite un aggancio non consapevole. Dopodiché la macchina è stata semplicemente riavviata dall’ibernazione dall’aggancio con un paio di click su invio. Con grande sorpresa per l’attaccante la macchina apre l’applicazione “riga di comando” da account di “root”(#). L’attaccante non si fa sfuggire l’occasione per creare un account di nome “fix”, con una password nulla, quindi fa battere all’aggancio i seguenti comandi:

```
# echo ‘fix:x:0:0::/:/bin/sh’ >> /etc/passwd
# echo ‘fix::10300:0:0’ >> /etc/shadow
```

Il comando “echo” molto genericamente serve per trasmettere come suo output una stringa che di fatto è anche il suo “argomento”. Il carattere ‘ in questo caso serve per individuare la stringa che dovrà gestire il comando “echo”. I caratteri “>” e “>>” servono rispettivamente per soprascrivere o aggiungere una stringa ad un file e sono seguiti dal “path” o percorso di un file.

Il file passwd con path /etc/passwd contiene gli accounts, le password ed altre informazioni come ad esempio:
clark:x:1001:1001:clark,,,:/home/mark:/bin/bash

ossia:
**Account:** clark
**Password:** x (configurazione di default - la password criptata ormai nei nuovi sistemi UNIX si trova in /etc/shadow)
**UID (codice id utente):** 1001
**GID (codice id del gruppo di appartenenza dell’utente):** 1001
**GECOS (informazioni sull’utente):** mark,,,
**Home directory:** /home/mark
**Login shell:** /bin/bash

Il numero UID e GID dipende dalla titolarità di diritti da assegnare al nuovo utente e dalla distro Linux o UNIX-like.

Il file shadow con path /etc/shadow contiene gli accounts, le password criptate ed altre informazioni come ad esempio:
clark:$6$.n.:17736:0:99999:7:::

ossia:
**Username:** clark
**Metodo di criptazione della password, salt e password criptata:** In questo caso $6$. Solitamente si trova la seguente stringa $metodo_hash$salt$password_in_hash Il “salt” è di fatto una seconda password causale assegnata automaticamente dal sistema, utilizzata per criptare in hash la prima password dell’utente in modo

che se due utenti utilizzano la stessa password, la password risultante in hash non sia la stessa. I metodi di criptazione sono i seguenti:
$1$ - MD5
$2a$ - Blowfish
$2y$ - Eksblowfish
$5$ - SHA-256
$6$ - SHA-512

Se il campo della password contiene un asterisco * o un punto esclamativo ! l'utente non potrà loggarsi nel sistema.
**La data espressa in giorni a partire dal 1 Gennaio 1970 in cui l'utente ha cambiato l'ultima volta la password:** 17736
**Il numero minimo di giorni che deve durare una password:** 0 - è una configurazione di default
**Il numero massimo di giorni che deve durare una password:** 99999 - è una configurazione di default
**Il numero di giorni entro cui l'utente deve cambiare password dopo la sua scadenza altrimenti il suo account diverrà inattivo:** 7 - generalmente questo campo viene lasciato vuoto
**La data in cui l'account è stato disabilitato -**
**L'ultimo campo per quanto esistente non viene ancora utilizzato nei sistemi Unix**

Un altro aneddoto tecnico citato dagli autori è lo spyware (pag. 200 in "La telefonata ad Anna") che viene inoculato dall'attaccante al bersaglio tramite ingegneria sociale, dettandogli semplicemente le istruzioni come nel caso precedente.

Quindi d'ora in poi non eseguite le istruzioni di nessuno, tutto qui!

**cap. 13 Non è sempre vero quel che appare - DEPISTAGGIO**

Il depistaggio purtroppo è una variabile che deve essere tenuta in considerazione durante una ricostruzione dei fatti o quando si vuole attuare un protocollo di sicurezza offensiva.
L'arma utilizzata per realizzare il depistaggio è il gaslighting anche attraverso attrezzature altamente tecnologiche; la falsificazione degli elementi essenziali per la percezione della realtà che circonda il bersaglio è ineluttabile in un attacco programmato e l'incauto senso di invulnerabilità non dovrà mai influenzare il vostro giudizio.

Poniamo un esempio:
un rapinatore ha il viso coperto, ma indossa una canottiera con le braccia esposte in bella vista ed il suo corpo è ricoperto da tatuaggi. Non notate un controsenso? Perché coprire soltanto il viso con il rischio di essere identificati? Semplicemente perché i tatuaggi potrebbero essere falsi, temporanei e non permanenti.

Ne "La fuorviante identificazione di chiamata" a pag. 207 l'attaccante semina "*un'orgia di prove*" contro la sua vittima, ovvero ricostruisce dolosamente degli elementi che potrebbero essere erroneamente utilizzati dagli inquirenti per risalire alla sua identità, elementi che ovviamente non potranno mai essere utili per risalire alla sua vera identità bensì per depistare le indagini e per scaricare le sue responsabilità su un capro espiatorio. Tale metodo viene purtroppo comunemente utilizzato non solo da associazioni notoriamente criminali, ma anche da chi dispone, non per meritocrazia, di incarichi con poteri decisionali con effetti diretti o indiretti sulle vite di terzi. Un esempio pratico di tale metodo è lo scandalo del 2015 che ha coinvolto il cerchio magico (composto da giudici, avvocati, ingegneri, insegnanti universitari, alti dirigenti delle forze dell'ordine, ecc.) dell'antimafia di

Palermo con la condanna con sentenza di primo grado nel 2021 persino dell'ex presidente della sezione misure di prevenzione del Tribunale di Palermo Silvana Saguto.
Ritornando invece all'aneddoto "La fuorviante identificazione di chiamata" a pag. 207, l'incauto senso di invulnerabilità del bersaglio è dovuto al dispositivo di identificazione della chiamata in entrata dello stesso bersaglio. L'attaccante ha sfruttando un servizio a pagamento degli operatori telefonici il cui protocollo di trasporto è denominato T1 ISDN (in Nord America) o E1 ISDN (in Europa) che di fatto è un collegamento in fibra ottica o in rame che concede all'azienda controparte del contratto telefonico b2b n canali dedicati al traffico portante (in ingl. *bearer*) ed n canali dedicati al traffico delle segnalazioni (*signaling traffic* in ingl.). I canali dedicati al traffico delle segnalazioni sono utilizzati per trasmettere il numero della chiamata in uscita. Quindi l'attaccante ha programmato il PBX (acronimo di *private branch exchange*), ossia un centralino telefonico ISDN, con un numero identificativo della chiamata in uscita ad hoc per il suo depistaggio. In "Variazione sul tema: c'è al telefono il presidente degli Stati Uniti" a pag. 210 gli autori si sono sbilanciati indicando anche il marchio del pbx utilizzato per il depistaggio-scherzo al conduttore radiofonico bersaglio, un Meridian.

A differenza dei privati le aziende possono difendersi dalle frodi acquistando dei pacchetti dai providers che prevedono la concessione di numeri verdi (a condizione di pagare anche per le chiamate in entrata). Allo stesso tempo alle aziende viene offerto un servizio di identificazione del chiamante reale ed esente dagli attacchi attraverso un pbx connesso ad una rete isdn terza.

Per il mail drop gli autori sottolineano che gli attaccanti solitamente utilizzano delle caselle email di provider-società con sede legale presso nazioni notoriamente poco accondiscendenti ai mandati di atti persecutori emessi dai tribunali statunitensi.

In realtà anche le vittime di whistle-bowling potrebbero fare riferimento per le loro comunicazioni a servizi di paesi terzi. Tra questi servizi occorre citare quelli di messaggistica denominati "*warrant canary*" dei providers di caselle email nei confronti dei loro utenti. Tali providers sfruttano essenzialmente un noto cavillo giuridico per rendere inefficaci potenziali atti persecutori da parte delle autorità statunitensi. Difatti per quanto legalmente non possano dichiarare all'utente bersaglio di aver ricevuto un atto ufficiale di un tribunale che li obbliga alla consegna del traffico dati, si limitano di fatto a comunicare periodicamente all'utente un messaggio in cui lo informano di non aver ricevuto atti giuridici che lo riguardano. Quindi quando l'utente non riceverà più periodicamente il messaggio *warrant canary* potrà facilmente "intuire" di essere stato messo sotto controllo. Inoltre è possibile criptare le proprie email, in modo da "rallentare" ulteriormente forme di controllo illegali.

Una tecnica da non sottovalutare per carpire password o dati sensibili altrui (per quanto possa sembrare banale o scontata) viene citata a pagina 218 nel case denominato "Ritorsione". Tale tecnica viene definita dagli autori "*shoulder surfing*" e consiste nell'osservare il bersaglio mentre digita su una tastiera o scrive su un foglio di carta informazioni essenziali o dati sensibili come il nome di un account e la password correlata.

**cap. 14 - Effetti diretti ed indiretti, colposi o dolosi, materiali e non materiali, del controllo e dell'acquisizione delle informazioni da parte di terzi illegalmente**

<< Tanti uomini d'affari leggono questi articoli credendo che alla loro azienda non potrebbe mai accadere >> pag.232

Il vero titolo di questo capitolo è “Spionaggio industriale”, ma credo sia riduttivo in quanto il bersaglio potrebbe in apparenza non essere plausibilmente oggetto di attenzioni illegali o quantomeno di spionaggio industriale.
Gli autori attraverso gli aneddoti inquadrano indirettamente i mandanti tipo o gli istigatori-ingaggiatori degli ingegneri sociali o quantomeno la loro categoria professionale di appartenenza. Tenendo in considerazione il già citato “triangolo della frode” nel dettaglio, incontriamo nei seguenti cases come mandanti:

Causa collettiva - pag. 222 -> un avvocato-studio legale (movente “improprio senso del dovere”);
Il nuovo partner commerciale - pag. 225 -> una società terza rivale (movente “avidità”);
La versione di Sammy Sanford -> un ex appartenente dei servizi segreti pag. 228 (alleanza opportunistica con microcriminalità, movente “opportunità”);
Giocare alla cavallina -> due studenti universitari che si ingaggiano a vicenda pag. 232 (movente “odio ed invidia”).

La massima da imparare da questo capitolo è:

<< Le attenzioni da parte di qualsiasi ente, gruppo o individuo non sono mai esenti da pregiudizio o attuate secondo equità e cagionano sempre un danno materiale per l’individuo che le riceve (altrimenti Edward Snowden oggi non vivrebbe in Russia). >>

**Controffensiva:**

- Crittografia dei dati ed opportuna conservazione delle chiavi onde evitare eventi accidentali o atti colposi-dolosi contro cose e persone (compresi lesioni personali e omicidio);
- Addestramento del personale contro il depistaggio. Nella cultura anglosassone il depistaggio viene definito anche *red herring* (“aringa rossa”) per quanto il suo significato estensivo indichi direttamente una tecnica usata nell’oratoria, nella retorica-politica e nella letteratura che consiste nel distrarre, fuorviare o confondere intenzionalmente rispettivamente l’interlocutore, il pubblico o il lettore al fine che essi giungano a delle conclusioni false o sbagliate. Il termine fu coniato nel 1807 da William Cobbett il quale sosteneva di aver sviato intenzionalmente dalla traccia della preda (per l’esattezza un coniglio) i cani di un cacciatore rivale durante una battuta di caccia attraverso i fumi di un’aringa rossa salata ed affumicata.

**Quarta Parte Addestramento alla sicurezza Cap. 15 e Vademecum**
**Sicurezza in breve Checklist**

<< Un ingegnere sociale è stato incaricato di rubarvi i piani del vostro nuovo prodotto innovativo che deve uscire tra due mesi.
Che cosa può fermarlo?
Il vostro firewall? No.
Forti strumenti di autenticazione? No.
Sistemi di rilevamento delle intrusioni? No.
La cifratura? No.
Un accesso limitato ai numeri di telefono per gli accessi modem su linea commutata? No.
I nomi in codice ai server che rendono difficile a un esterno capire quale di loro ospita i progetti del prodotto? No.
La verità è che non esiste tecnologia al mondo che possa prevenire un attacco portato da un ingegnere sociale. >> pag. 241

Fattore umano, Social Engineering ed Hacking: ecco cosa aspettarsi nella giungla odierna di tutti i giorni, dove tutti credono di poter far tutto in totale disprezzo dei sacrifici e delle vite altrui.

I capitoli finali di questo libro hanno principalmente due obiettivi:
1) Awareness, ossia la presa di coscienza dei rischi, nonché dei limiti dell'efficacia dei protocolli di sicurezza e degli effetti delle violazioni leggere o gravi, colpose o dolose, del personale.
2) Un quadro dettagliato per i responsabili della sicurezza IT e non, in modo che possano stilare con gli amministratori un total cost of ownership dell'hardware adeguato e programmare i costi per l'addestramento del personale in base alle mansioni svolte o agli incarichi assegnati, alla quantità nominale del personale ed alla loro dislocazione nelle varie sedi.

<< Data la natura umana, ogni tanto il personale ignorerà o aggirerà i provvedimenti che gli sembrano ingiustificati o troppo laboriosi. È responsabilità della direzione verificare che il personale comprenda l'importanza di questa politica e sia motivato a rispettarla piuttosto che trattarla come una serie di ostacoli da aggirare >> pag. 257

Viene suggerito al riguardo di attuare una politica che premi la perseveranza del rispetto dei protocolli di sicurezza e che "pubblicizzi" le violazioni o gli attacchi in generale.
A mio modesto parere tale politica nella realtà non è attuabile in quanto nei confronti del dipendente solerte restituisce degli effetti indesiderati dovuti a corporativismo, invidia, prevaricazione, ostracismo fino al suo licenziamento o alla sua lettera di dimissioni. Per di più le norme di qualsiasi tipo di ordinamento, persino quello interno ad un'azienda, non devono essere applicate con troppo zelo onde evitare di sfociare nella mera applicazione della regola ad libitum (exceptio doli) da parte di sedicenti, saccenti ed idioti giudici straordinari.
Lo stesso testo puntualizza che persino il personale dirigenziale deve ottemperare alle richieste dei subordinati, ma nella maggior parte dei casi la natura narcisistica dei managers prende il sopravvento a discapito della stessa azienda. E se il comportamento sconsiderato del dirigente di turno determina il successo di un attacco o un evento spiacevole, lo stesso dirigente viene protetto dalla sua stessa categoria di appartenenza (in quanto ne fa parte, nella maggior parte dei casi, non per meritocrazia ma per cooptazione e corruzione o quanto meno per scambio di favori). Non è un caso che i figli degli avvocati fanno gli avvocati, i figli dei medici fanno i medici, ecc.. E non è un caso che la nostra vita di tutti i giorni, priva di dialogo fra le parti, sia resa meno piacevole da palesi episodi di corruzione, violenza, malasanità, ecc..
Gli autori inoltre citano gli studi del sociologo Robert B. Cialdini, riconosciuti e sintetizzati nel numero di febbraio del 2001 di "Scientific American". Per Cialdini le sei tendenze della natura umana che determinano il successo di un attacco di ingegneria sociale sono le seguenti:
- *Autorevolezza*;
- *Simpatia*;
- *Ricambiare* (ossia lo "scambio di favori" o il "mantenere la parola data");
- *Coerenza* (dove si intende elasticamente il "presupposto ideologico" o lo "sposare una causa");
- *Convalida Sociale* ("senso di appartenenza ad una data categoria o contesto sociale");
- *Scarsità* (ovvero "l'opportunità di poter acquisire o usufruire di un bene o un servizio riservato a pochi").

Si ribadisce che il testo del Vademecum e della Checklist è rivolto al dirigente incaricato di stilare i protocolli di sicurezza ed essendo di per sé schematico e sintetico non può essere riassunto in questi appunti, ma deve essere analizzato direttamente nel testo originale.