ESERCIZIO S5 L4

SOCIAL ENGINEERING

Il **social engineering**, o ingegneria sociale, è una tecnica usata dagli attaccanti per manipolare psicologicamente le persone e indurle a compiere azioni che compromettano la sicurezza di un sistema, come rivelare informazioni sensibili, cliccare su link pericolosi o scaricare software malevolo. A differenza degli attacchi informatici puramente tecnici, il social engineering sfrutta la fiducia, l'errore umano e la scarsa consapevolezza per aggirare le misure di sicurezza.

In altre parole, anziché forzare la serratura, l'attaccante convince qualcuno ad aprire la porta.

Phishing

Una delle tecniche più diffuse e conosciute è il **phishing**. L'attaccante si finge un'entità affidabile — come una banca, un servizio online, un collega — e invia un'email o un messaggio contenente un link o un allegato. Il contenuto è costruito in modo da creare urgenza o preoccupazione: ad esempio, "Il tuo conto è stato bloccato, clicca qui per riattivarlo".

Un esempio pratico può essere un'email apparentemente proveniente da PayPal che invita l'utente a confermare le sue credenziali. Il link porta a un sito fasullo, graficamente identico a quello ufficiale, ma controllato dall'attaccante. Una volta inseriti i dati, l'utente li ha in realtà consegnati all'aggressore.

Il phishing è efficace perché fa leva su emozioni forti: paura, ansia, senso di urgenza. In situazioni di stress, le persone agiscono d'istinto, senza riflettere con attenzione.

Pretexting (o pretesto)

Il **pretexting** è una tecnica in cui l'attaccante costruisce una storia credibile — un pretesto — per ottenere informazioni. Qui l'inganno è più elaborato: non si tratta solo di un messaggio truffaldino, ma di una vera e propria messinscena. L'attaccante può fingere di essere un tecnico IT, un responsabile delle risorse umane o un fornitore, contattando la vittima via telefono o di persona.

Un esempio tipico è un finto addetto al supporto tecnico che chiama un dipendente e dice di dover effettuare un aggiornamento al sistema. Per farlo, ha bisogno della password dell'utente. Se il tono è professionale e il contesto è credibile, molte persone tendono a collaborare senza sospettare.

Il pretexting funziona perché gioca sulla fiducia e sul rispetto dell'autorità percepita. Inoltre, chi riceve la richiesta non vuole sembrare sgarbato o incompetente, e tende quindi a collaborare.

Baiting

Il **baiting**, ovvero "abboccare all'esca", sfrutta l'avidità o la curiosità della vittima. In genere l'attaccante offre qualcosa di attraente (un regalo, un accesso gratuito, file esclusivi), ma il contenuto è malevolo.

Un classico esempio è una chiavetta USB lasciata in un luogo pubblico — magari etichettata con qualcosa di stuzzicante come "stipendi 2025" o "foto personali" — che la vittima raccoglie e inserisce nel proprio computer. All'interno, naturalmente, si trova un malware pronto ad attivarsi.

Questo tipo di attacco è efficace perché sfrutta una debolezza psicologica molto comune: la tentazione di ottenere qualcosa gratuitamente o in anteprima. La trappola è tanto più efficace quanto più l'esca è su misura per il contesto.

Tailgating (o piggybacking)

Il **tailgating** è una tecnica fisica più che digitale, ma estremamente efficace. Consiste nel seguire una persona autorizzata per accedere a un'area riservata. Immagina un attaccante vestito da corriere o da tecnico che aspetta davanti alla porta di un ufficio con badge elettronico. Quando un impiegato apre la porta, l'attaccante si accoda, magari tenendo in mano un pacco per sembrare legittimo.

Nessun malware, nessun computer: solo psicologia e cortesia. Molte persone non vogliono sembrare maleducate o sospettose e tendono a lasciar passare chi sembra avere un motivo valido.

Questa tecnica è efficace perché sfrutta la naturale inclinazione alla collaborazione e la riluttanza a mettere in discussione la legittimità altrui in ambienti sociali.

Quid pro quo

Molto simile al baiting, il **quid pro quo** implica uno scambio apparente: "ti offro qualcosa, ma in cambio voglio qualcosa da te". Ad esempio, un attaccante può fingersi

parte di un help desk e chiamare casualmente numeri interni a un'organizzazione, offrendo supporto tecnico. Quando trova qualcuno che ha effettivamente un problema al computer, si offre di risolverlo — ma nel farlo chiede accesso remoto o le credenziali.

La forza di questo metodo sta nella reciprocità: l'utente riceve un servizio e si sente in dovere di collaborare. La disponibilità dell'attaccante lo rende più credibile.

Perché il social engineering funziona?

Il social engineering funziona perché non attacca le macchine, ma le persone. E le persone, a differenza dei sistemi informatici, non seguono sempre regole rigide. Possono essere distratte, stanche, curiose o troppo fiduciose. Gli attaccanti conoscono bene questi punti deboli e li sfruttano con astuzia, spesso studiando l'ambiente, i ruoli aziendali e le abitudini della vittima.

Funziona perché fa leva su comportamenti umani naturali, come la fiducia negli altri, la disponibilità ad aiutare, il rispetto per l'autorità e l'abitudine a eseguire istruzioni in ambienti lavorativi. A differenza di un attacco informatico che richiede competenze tecniche, il social engineering può essere messo in pratica da chiunque abbia una buona capacità di comunicazione e una strategia convincente.

Le contromisure più efficaci per proteggersi dal social engineering

Per proteggersi dagli attacchi di **social engineering**, la tecnologia da sola non basta: serve anche un approccio consapevole, critico e costante da parte degli utenti. Gli attaccanti puntano sulle debolezze umane, quindi la difesa più solida parte proprio dalla **formazione**, dalla **vigilanza** e da una **cultura della sicurezza** condivisa.

1. Educazione e formazione continua

La prima e più importante misura di difesa è l'**educazione** degli utenti. Non è sufficiente un corso una tantum: la formazione deve essere continua, aggiornata e coinvolgente. Le persone devono imparare a **riconoscere i segnali d'allarme**: email sospette, richieste urgenti, errori grammaticali, link strani o incongruenze nei messaggi.

Un esempio concreto: in molte aziende si organizzano **simulazioni di phishing**, inviate dai team di sicurezza per testare l'attenzione dei dipendenti. Chi clicca sul link viene reindirizzato a una pagina che spiega l'errore e rafforza la consapevolezza. Questo metodo è efficace perché allena il personale a individuare i segnali anche in situazioni reali.

2. Verifica dell'identità

Una delle contromisure più utili è **non fidarsi mai ciecamente** di una richiesta, soprattutto se proviene da email, telefonate o messaggi. Ogni informazione sensibile (password, accessi, dati personali) deve essere **verificata attraverso canali ufficiali**.

Immagina di ricevere una telefonata da qualcuno che si presenta come tecnico IT e ti chiede le credenziali per "verificare un errore sul tuo account". Una buona prassi è **interrompere la conversazione con cortesia** e contattare direttamente il supporto interno all'azienda per verificare l'identità del chiamante.

Questo approccio è efficace perché interrompe la dinamica psicologica su cui fa leva il social engineer: l'urgenza e la fiducia forzata.

3. Uso del principio del "dubbio utile"

In molte situazioni, soprattutto nel pretexting o nel quid pro quo, il truffatore si presenta in modo professionale, gentile, disponibile. Qui entra in gioco il principio del **dubbio utile**: ogni richiesta anomala, anche se ben confezionata, va trattata con attenzione. Non significa diventare paranoici, ma **applicare una sana diffidenza**.

Per esempio, se un collega ti chiede via email un file riservato, ma tu non sei sicuro che ne abbia davvero bisogno, **non c'è nulla di male a chiedere conferma a voce o via chat interna**. Questo semplice gesto può evitare danni gravi.

È efficace perché spezza l'automatismo del "fidarsi per cortesia" e spinge le persone a riflettere prima di agire.

4. Bloccare l’accesso fisico non autorizzato

Per contrastare il tailgating, è importante applicare regole semplici ma ferme. Una buona pratica è **non far entrare sconosciuti negli spazi aziendali riservati**, anche se sembrano legittimi. Il classico esempio del “corriere con un pacco” o del “tecnico col tesserino” deve essere sempre verificato.

Molte aziende installano **tornelli, badge elettronici e videocamere**, ma la misura più efficace è la **vigilanza collettiva**. Se ognuno si sente responsabile, il livello di sicurezza aumenta in modo esponenziale. È utile anche insegnare a dire **"Mi scusi, può attendere mentre chiedo conferma?"** in modo fermo ma cortese.

Questo è efficace perché crea una barriera culturale all’ingresso, non solo fisica.

5. Uso dell’autenticazione a più fattori (MFA)

Un’altra difesa tecnica ma fondamentale è l’**autenticazione a più fattori**. Anche se un attaccante riesce a carpire la password tramite phishing o pretexting, il secondo fattore (un codice temporaneo inviato al cellulare o generato da un’app) può bloccare l’accesso.

Ad esempio, se ricevi una notifica MFA su un accesso che non hai richiesto, ti accorgi subito che qualcuno ha la tua password. Questo ti dà il tempo di intervenire e cambiare le credenziali.

È una misura efficace perché **introduce una barriera in più**, e costringe l’attaccante a superare due livelli di sicurezza.

6. Policy chiare e linee guida comportamentali

Un’azienda o un’organizzazione deve **definire regole chiare**, che tutti conoscano: ad esempio, “mai inviare password via email”, “mai aprire allegati da mittenti sconosciuti”, “mai fornire informazioni sensibili per telefono senza verifica”.Queste policy vanno **comunicate con esempi pratici** e ricordate periodicamente, magari con poster, newsletter o micro-video.

Per esempio: se un dipendente riceve una richiesta per trasferire fondi da parte di un “direttore” via email, sa che deve seguire una procedura di doppia conferma, magari attraverso un secondo canale. Questo evita truffe note come **Business Email Compromise (BEC)**.

Queste regole sono efficaci perché tolgono ambiguità e danno ai dipendenti una chiara “mappa” da seguire nei momenti critici.

7. Controllo dei dispositivi esterni

Nel caso del **baiting**, è fondamentale **non inserire mai dispositivi USB sconosciuti** nei propri computer. I sistemi aziendali dovrebbero disattivare automaticamente l’autoplay delle periferiche e, se possibile, **impedire l’uso di supporti non autorizzati**.

Un esempio pratico: in molte aziende, le porte USB sono disattivate per default, oppure ogni periferica dev’essere prima scansionata e autorizzata dal team IT.

Questo è efficace perché elimina una delle vie più semplici di compromissione fisica dei sistemi.

8. Monitoraggio dei comportamenti anomali

Infine, un sistema di difesa efficace deve includere **strumenti di monitoraggio** per rilevare comportamenti insoliti: accessi fuori orario, trasferimenti di file anomali, tentativi multipli di login falliti. Anche se l’inganno ha avuto successo, **una risposta tempestiva può contenere i danni**.

Per esempio: se un utente cade in un attacco phishing e inserisce le sue credenziali in un sito falso, ma il sistema rileva che poi c’è un accesso da un IP inusuale (es. Russia o India), può bloccare automaticamente l’account e inviare un alert.

Questa contromisura è efficace perché **funziona anche dopo che l’errore umano è già stato commesso**.

Conclusione

Il **social engineering** è una delle minacce più insidiose della sicurezza informatica moderna, non perché sfrutti vulnerabilità nei sistemi, ma perché sfrutta le persone. È un tipo di attacco che non agisce solo sul fronte tecnologico, ma si insinua nella psicologia, nella fiducia, nella disattenzione e nella routine. Per questo motivo non può essere contrastato soltanto con software o firewall: serve un approccio umano, culturale, quotidiano.

La cultura della sicurezza deve diventare parte integrante del lavoro di ogni individuo, in ogni ruolo e in ogni settore. Non è più sufficiente che solo il reparto IT sia responsabile della protezione dei dati: ogni dipendente, collaboratore, studente o cittadino digitale è un potenziale bersaglio — e dunque anche una linea di difesa.

Chi utilizza dispositivi connessi, email, social network o servizi online ha la responsabilità di **formarsi**, mantenersi aggiornato, e agire con lucidità. Questo vale sia in ambito aziendale sia nella vita privata. I truffatori non colpiscono solo le grandi aziende: **anche un singolo account personale compromesso può essere l'inizio di una catena di attacchi**.

Inoltre, è importante comprendere che **l'attacco più riuscito è quello che non viene nemmeno riconosciuto come tale**. Se una persona viene manipolata senza rendersene conto, l'attaccante ha vinto in silenzio. Per questo motivo, la prevenzione è l'unica vera arma: diffondere consapevolezza, condividere esperienze, imparare dagli errori propri e altrui.