Social Engineering

Il social engineering è una tecnica di manipolazione psicologica utilizzata dagli attaccanti per ingannare le persone e convincerle a rivelare informazioni sensibili, come password, dettagli finanziari o accessi a sistemi.

Invece di sfruttare vulnerabilità tecniche, gli attaccanti si concentrano sull’anello più debole della sicurezza: il comportamento umano.

Esempi di Social Engineering:

1. Phishing

Descrizione: Gli attaccanti inviano email, SMS o messaggi ingannevoli che imitano fonti affidabili (banche, colleghi, ecc.).

Come funziona:

L'utente riceve un messaggio con un link che lo reindirizza a una pagina falsa, simile a quella originale.

Una volta inserite le credenziali, queste vengono rubate.

Esempi reali:

Campagne di phishing contro PayPal o Amazon, in cui si richiedono dettagli di pagamento.

Messaggi di "aggiornamento password" da presunte piattaforme IT aziendali.

Difese:

Non cliccare su link sospetti e verificare sempre l'indirizzo del mittente.

Usare strumenti di sicurezza email avanzati come Mimecast.

Implementare l’autenticazione a due fattori (2FA).

2. Tailgating

Descrizione: Un attaccante segue una persona autorizzata per accedere a una zona protetta.

Come funziona:

L'attaccante si presenta come un dipendente o visitatore, approfittando della cortesia della vittima (es. una porta tenuta aperta).

Esempi reali:

In un'azienda, un intruso accede all'area server seguendo un tecnico IT.

Difese:

Implementare badge elettronici o sistemi biometrici.

Sensibilizzare i dipendenti a non aprire porte ad estranei e a chiedere conferma dell'identità.

3. Pretexting

Descrizione: L’attaccante crea una falsa identità per guadagnare la fiducia della vittima e ottenere informazioni sensibili.

Come funziona:

Un attaccante si finge un tecnico IT, un rappresentante del governo o un collega che necessita di dati per risolvere un "problema urgente".

Esempi reali:

Un falso tecnico IT chiama un dipendente chiedendo le credenziali per "risolvere un problema".

Difese:

Verificare sempre l'identità dell'interlocutore.

Adottare policy aziendali che vietano la condivisione di informazioni sensibili via telefono o email.

4. Baiting

Descrizione: Utilizzare un’esca per indurre la vittima a compiere un’azione pericolosa, come collegare un dispositivo infetto.

Come funziona:

Un attaccante lascia una chiavetta USB "sparita" in un luogo pubblico con un’etichetta accattivante (es. "Confidenziale").

La vittima collega la chiavetta, installando involontariamente un malware.

Esempi reali:

Chiavette infette distribuite nei parcheggi di aziende per accedere ai sistemi aziendali.

Difese:

Non collegare dispositivi sconosciuti ai propri computer.

Utilizzare soluzioni di endpoint protection per bloccare l'esecuzione di software non autorizzati.

5. Dumpster Diving

Descrizione: Cercare informazioni sensibili tra i rifiuti o tra dispositivi abbandonati.

Come funziona:

Gli attaccanti cercano documenti cartacei, vecchi computer, hard disk o badge aziendali smaltiti in modo non sicuro.

Esempi reali:

Raccolta di password o numeri di telefono aziendali da documenti gettati nei cassonetti.

Difese:

Distruggere i documenti sensibili con trituratori prima di smaltirli.

Utilizzare software di cancellazione sicura dei dati prima di smaltire dispositivi elettronici.

6. Quid Pro Quo

Descrizione: Gli attaccanti offrono un vantaggio (es. supporto tecnico) in cambio di informazioni sensibili o accesso ai sistemi.

Come funziona:

Un attaccante si finge un tecnico IT e offre un aggiornamento software in cambio di accesso al dispositivo della vittima.

Esempi reali:

Offerte di "regali" o "voucher" in cambio di credenziali.

Difese:

Non condividere informazioni personali o lavorative con estranei.

Verificare sempre l’autenticità delle offerte o richieste ricevute.

Alcune App utilizzate dagli attaccanti:

1. Phishing Toolkit

Descrizione: Strumenti progettati per creare e gestire campagne di phishing, che includono la simulazione di email ingannevoli e la costruzione di siti web falsi.

Esempi di Software:

Social-Engineer Toolkit (SET)

Utilizzato per simulare email e pagine web fraudolente.

Gophish

Open-source, permette la creazione di campagne di phishing mirate e la raccolta dei dati inseriti dalle vittime.

Phishing-as-a-Service (PhaaS)

Servizi online che forniscono kit preconfezionati per lanciare campagne di phishing con poca esperienza tecnica.

Come Proteggersi:

Formazione e Consapevolezza: Organizzare corsi regolari per insegnare a riconoscere email sospette.

Filtri Antispam: Utilizzare software come Mimecast o Microsoft Defender per bloccare email fraudolente.

Autenticazione Multi-Fattore (MFA): Riduce i rischi associati al furto di credenziali.

2. Keylogger

Descrizione: Software o hardware che registrano ogni tasto premuto, permettendo agli attaccanti di rubare password, dati personali e informazioni sensibili.

Esempi di Software:

Spyrix Keylogger

Monitora tastiera, schermate e attività online.

Ardamax Keylogger

Progettato per catturare input della tastiera e inviare report agli attaccanti.

Hardware Keylogger

Piccoli dispositivi fisici che si collegano tra tastiera e computer.

Come Proteggersi:

Anti-Malware e Anti-Keylogger: Soluzioni come Malwarebytes o Zemana AntiLogger rilevano e rimuovono i keylogger.

Tastiere Virtuali: Utilizzare tastiere software per inserire informazioni sensibili.

Monitoraggio Hardware: Controllare regolarmente la connessione delle periferiche.

3. Remote Access Trojans (RATs)

Descrizione: Malware che consente agli attaccanti di ottenere accesso remoto ai dispositivi infetti.

Esempi di Software:

njRAT

Consente di controllare in remoto il sistema della vittima, rubare file e attivare webcam.

DarkComet

Molto popolare per la sua facilità d’uso e la vasta gamma di funzionalità (spionaggio, keylogging, ecc.).

Quasar RAT

Open-source, utilizzato principalmente per spionaggio industriale.

Come Proteggersi:

Firewall e IDS/IPS: Implementare soluzioni come Snort o Suricata per monitorare e bloccare traffico sospetto.

Endpoint Protection: Utilizzare software EDR (Endpoint Detection and Response) come CrowdStrike Falcon per rilevare comportamenti anomali.

Patch di Sicurezza: Mantenere aggiornati i sistemi operativi e le applicazioni per evitare vulnerabilità sfruttabili.

4. Malware su USB (es. Rubber Ducky)

Descrizione: Strumenti che sembrano normali dispositivi USB ma eseguono script malevoli quando collegati a un computer.

Esempi di Software e Hardware:

Rubber Ducky

Un dispositivo USB programmabile che esegue script malevoli per rubare dati o installare malware.

Bash Bunny

Dispositivo avanzato che automatizza attacchi su larga scala contro dispositivi USB.

Come Proteggersi:

Bloccare USB Sconosciute: Configurare policy di sicurezza che vietino l'uso di dispositivi USB non autorizzati.

Soluzioni Endpoint: Implementare software come Microsoft Defender o Symantec Endpoint Protection per rilevare script non autorizzati.

Sensibilizzazione: Formare i dipendenti a non collegare dispositivi sconosciuti.

5. OSINT Tools (Open Source Intelligence)

Descrizione: Strumenti utilizzati per raccogliere informazioni pubbliche su persone o aziende, sfruttando dati disponibili online.

Esempi di Software:

Maltego

Consente di visualizzare relazioni tra email, domini, nomi e account social.

Recon-ng

Framework avanzato per l'automazione di ricerche OSINT.

Shodan

Motore di ricerca per dispositivi connessi a Internet, come webcam e server.

Come Proteggersi:

OSINT inverso: Utilizzare strumenti come SpiderFoot per identificare e limitare le proprie informazioni pubbliche.

Protezione Privacy: Configurare i profili social con impostazioni di privacy restrittive.

Anonimizzazione dei Dati: Rimuovere riferimenti personali da database pubblici, ove possibile.

6. Password Cracking Tools

Descrizione: Strumenti progettati per violare password tramite attacchi di forza bruta, dizionario o ingegneria inversa su hash crittografici.

Esempi di Software:

Hashcat

Uno dei più potenti strumenti per il cracking di hash di password.

John the Ripper

Ideale per violare password semplici su diversi formati di hash.

Hydra

Utile per attacchi su protocolli di rete come SSH, FTP e HTTP.

Come Proteggersi:

Password Sicure: Utilizzare password lunghe e complesse, generate da strumenti come LastPass o Bitwarden.

Hashing Robusto: Conservare le password con algoritmi di hashing sicuri come bcrypt o Argon2.

Blocchi su Tentativi Falliti: Implementare limiti sui tentativi di accesso.

Strategie Generali di Protezione

- Monitoraggio Costante
- Utilizzare soluzioni di monitoraggio avanzate come Splunk o Elastic Stack per rilevare comportamenti sospetti.
- Aggiornamenti Software
- Patchare regolarmente sistemi e applicazioni per ridurre la superficie di attacco.
- Autenticazione Multi-Fattore (MFA)
- Riduce l’efficacia di molti attacchi basati su credenziali rubate.
- Formazione Regolare
- Educare i dipendenti e gli utenti finali a riconoscere tecniche di attacco.