ESERCIZIO

S5_L4_SOCIAL_ENGENEERING

Consegna:

- *Dovrete scrivere un prompt per ChatGPT che vi permetta di ottenere informazioni dettagliate sulle tecniche di social engineering.*

- *Analizzate gli esempi forniti e sviluppate una serie di raccomandazioni per prevenire tali attacchi. Infine, create una presentazione o un documento che riassuma le vostre scoperte e raccomandazioni.*

Introduzione al Social Engineering

Il social engineering (ingegneria sociale) è un insieme di tecniche psicologiche finalizzate a manipolare comportamenti umani per ottenere informazioni sensibili, accessi non autorizzati o influenzare decisioni.
A differenza delle minacce tecniche, questa forma di attacco sfrutta principalmente le debolezze umane, come l'urgenza, la fiducia e la mancanza di consapevolezza.
È frequentemente utilizzata come vettore iniziale per attacchi più complessi, come infezioni ransomware, compromissioni di sistemi o esfiltrazione di dati. La sua efficacia deriva dalla capacità di bypassare controlli tecnici mediante l'inganno umano.

PHISHING

Definizione:

Tecnica che prevede l'invio massivo di comunicazioni (email, SMS, messaggi) apparentemente legittime, con l'obiettivo di indurre l'utente a cliccare su link dannosi o a fornire informazioni riservate (es. credenziali).

Obiettivi comuni:

- Acquisizione di credenziali
- Installazione di malware
- Raccolta di dati personali o finanziari

Esempio:

Email fittizia da parte di un istituto bancario che invita a "verificare" l'account tramite un link contraffatto.

Indicatori tipici:

- Tono allarmistico o senso di urgenza
- Errori ortografici o grammaticali
- Mittente con dominio sospetto
- Link che puntano a URL falsificati

Misure preventive:

- Utilizzo di filtri antiphishing e sandboxing
- Implementazione di autenticazione multifattore (MFA)
- Formazione periodica per il riconoscimento delle truffe

SPEAR PHISHING

Definizione:

Attacco mirato basato su phishing, altamente personalizzato in base al ruolo e al contesto della vittima.

Obiettivi comuni:

- Compromissione di utenti ad alto privilegio
- Infiltrazione iniziale per attacchi avanzati (APT)

Esempio:

Email indirizzata al responsabile finanziario con dettagli reali su fornitori o progetti, contenente una richiesta fraudolenta di pagamento.

Indicatori tipici:

- Contenuti personalizzati e contestualizzati
- Presenza di nomi o riferimenti interni
- Indirizzi email simili ma non ufficiali

Misure preventive:

- Applicazione di policy di doppia verifica per richieste finanziarie
- Formazione specifica per personale ad alto rischio (es. HR, finance, C-level)
- Configurazione corretta di SPF, DKIM e DMARC

PRETEXTING

Definizione:

Tecnica basata sulla creazione di un pretesto credibile con cui l'attaccante finge di essere una figura autorizzata, al fine di ottenere informazioni riservate.

Obiettivi comuni:

- Accesso a sistemi interni
- Raccolta di dati utili per attacchi futuri

Esempio:

Chiamata da parte di un falso tecnico IT che richiede le credenziali per "risolvere un malfunzionamento urgente".

Indicatori tipici:

- Mancanza di verifica dell'identità del richiedente
- Richieste fuori procedura
- Comunicazioni troppo insistenti o vaghe

Misure preventive:

- Politiche interne di verifica identità
- Proibizione della condivisione di credenziali via telefono o email
- Procedure di escalation e conferma tramite canali ufficiali

---

BAITING

Definizione:

Attacco che fa leva sulla curiosità o sull'avidità della vittima, mediante la distribuzione di "esche" contenenti malware o link compromessi.

Obiettivi comuni:

- Installazione di software malevolo
- Accesso non autorizzato a reti o dispositivi

Esempio:

Una chiavetta USB infetta etichettata "Riservato – Buste paga" viene lasciata in un luogo pubblico con l'intento che qualcuno la colleghi a un computer aziendale.

Indicatori tipici:

- Presenza di dispositivi o file sconosciuti
- Offerte o risorse gratuite inattese
- Download da fonti non verificate

Misure preventive:

- Disabilitazione dell'autoplay per dispositivi USB
- Educazione alla gestione sicura dei dispositivi rimovibili
- Software antivirus e antimalware aggiornati

TAILGATING

Definizione:

Tecnica di intrusione fisica in cui un attaccante ottiene accesso a un'area protetta seguendo un dipendente autorizzato, spesso approfittando della cortesia altrui.

Obiettivi comuni:

- Accesso diretto a postazioni di lavoro o infrastrutture
- Installazione fisica di malware o hardware malevolo (es. keylogger)

Esempio:

Un individuo si presenta all'ingresso aziendale fingendo di aver dimenticato il badge e chiede di essere accompagnato dentro.

Indicatori tipici:

- Presenza di soggetti non identificati in aree riservate
- Badge non visibili o assenti
- Comportamento evasivo o sospetto

Misure preventive:

- Implementazione di sistemi di accesso controllato (tornelli, badge elettronici)
- Formazione sulla sicurezza fisica
- Politiche di "no tailgating" chiare e condivise

QUID PRO QUO

Definizione:

Attacco in cui viene offerto un vantaggio o servizio in cambio di informazioni o accessi.

Obiettivi comuni:

- Ottenimento di accesso remoto
- Esecuzione di azioni dannose da parte dell'utente

Esempio:

Un finto operatore di supporto tecnico offre un "aggiornamento urgente" in cambio delle credenziali o dell'accesso remoto.

Indicatori tipici:

- Offerte inattese o troppo vantaggiose
- Pressioni a compiere azioni tecniche senza verifica
- Uso eccessivo di linguaggio tecnico per impressionare

Misure preventive:

- Policy chiare per la gestione del supporto tecnico
- Verifica dell'identità degli operatori IT
- Divieto di concedere accessi non autorizzati

Best Practices contro il Social Engineering

Per ridurre il rischio di compromissione tramite social engineering, si raccomandano le seguenti pratiche:

- **Verificare sempre l'identità** di chi richiede informazioni o accessi.
- **Non cliccare link o aprire allegati sospetti.**
- **Utilizzare l'autenticazione multifattore (MFA)** ove possibile.
- **Formare periodicamente il personale** su minacce e tecniche di attacco.
- **Segnalare immediatamente comportamenti sospetti** o attività anomale.
- **Implementare strumenti tecnici di protezione**, come filtri email, antivirus aggiornati e DLP.
- **Promuovere una cultura aziendale della sicurezza**, inclusa la sicurezza fisica.