Il social engineering è una tecnica utilizzata dagli attaccanti per manipolare le persone e indurle a fornire informazioni riservate, effettuare azioni che compromettono la sicurezza di un sistema o rivelare dettagli che possono essere sfruttati per un attacco informatico. Piuttosto che tentare di violare direttamente un sistema, gli attaccanti sfruttano la psicologia umana, come fiducia, paura o urgenza.

Tecniche più comuni di social engineering

Phishing

Il phishing è una tecnica in cui un attaccante invia comunicazioni (email, messaggi o link) apparentemente legittime per indurre la vittima a:

Inserire credenziali (username e password) su un sito falso.

Scaricare malware.

Fornire informazioni sensibili (es. numeri di carte di credito).

Varianti del phishing:

Spear phishing: Messaggi personalizzati, mirati a una specifica persona o organizzazione.

Whaling: Bersaglia alti dirigenti di un'azienda, cercando informazioni particolarmente sensibili.

Smishing: Phishing attraverso SMS o app di messaggistica.

Vishing: Phishing tramite chiamate vocali.

Tailgating (o Piggybacking)

Con il tailgating, un attaccante accede a un'area protetta seguendo una persona autorizzata, sfruttando la cortesia comune (es. chiedendo di tenere aperta la porta) o la distrazione. Questa tecnica è tipica per accedere a edifici, data center o uffici.

Esempio: Un attaccante si avvicina a un dipendente con le mani occupate e chiede gentilmente di aprire una porta, fingendo di essere un collega o un addetto alla consegna.

Pretexting

L'attaccante crea un falso pretesto per ottenere informazioni. Potrebbe fingere di essere un tecnico IT, un dirigente, un fornitore o persino un amico della vittima per guadagnare fiducia e accedere a informazioni sensibili.

Esempio: Un falso "addetto al supporto tecnico" chiama un dipendente chiedendo la password per risolvere un problema urgente.

Baiting

Con il baiting, l'attaccante offre un'esca per attirare la vittima. Questo può includere dispositivi infetti come chiavette USB lasciate in luoghi pubblici o promesse di contenuti allettanti come file gratuiti (musica, film, software).

Esempio: Un dipendente trova una chiavetta USB etichettata "Salari 2024" nel parcheggio aziendale e la inserisce nel proprio computer.

Quid Pro Quo

Questa tecnica consiste nell'offrire qualcosa in cambio di informazioni o accesso. Spesso si basa sulla promessa di un vantaggio, come supporto tecnico o un omaggio.

Esempio: Un falso tecnico IT chiama un dipendente offrendo assistenza per un problema inesistente in cambio delle sue credenziali.

Dumpster Diving

L'attaccante ricerca informazioni sensibili scartate nei rifiuti, come documenti, appunti, o hardware inutilizzati.

Esempio: Estrarre da un cestino note con password scritte o documenti con informazioni riservate.

Prevenzione e difesa

Per mitigare i rischi del social engineering, è fondamentale:

Formare i dipendenti a riconoscere tentativi di manipolazione.

Implementare procedure rigorose, come la verifica dell'identità per richieste di informazioni.

Utilizzare misure fisiche di sicurezza, come badge elettronici e videosorveglianza.

Seguire la regola del "zero trust", verificando sempre l'identità di chiunque richieda accesso o informazioni.

Difendersi dagli attacchi di social engineering richiede un mix di consapevolezza, formazione e implementazione di misure di sicurezza sia tecniche che comportamentali. Ecco alcune strategie efficaci:

1. Formazione e Consapevolezza

Training regolare del personale: Organizzare corsi periodici per insegnare ai dipendenti a riconoscere tentativi di social engineering, come phishing, pretexting e baiting.

Simulazioni di attacchi: Condurre test di phishing o altre simulazioni per valutare e migliorare le competenze di riconoscimento delle minacce.

Creare una cultura della sicurezza: Incoraggiare i dipendenti a segnalare attività sospette senza timore di ripercussioni.

2. Autenticazione e Verifica

Politica del doppio controllo: Verificare sempre richieste insolite di informazioni o accesso, ad esempio, contattando direttamente il richiedente tramite un canale ufficiale.

Autenticazione multifattoriale (MFA): Aggiungere un livello di sicurezza richiedendo più fattori per accedere a sistemi o dati (es. password + codice SMS o biometria).

Verifica identità per accesso fisico: Implementare badge di accesso, codici PIN o riconoscimento biometrico per evitare che sconosciuti accedano fisicamente a luoghi riservati.

3. Gestione delle Informazioni

Limitare l’accesso ai dati: Applicare il principio del "least privilege", fornendo accesso solo alle informazioni e ai sistemi necessari per svolgere il proprio lavoro.

Protezione delle informazioni sensibili:

Distruggere documenti cartacei sensibili (es. mediante trituratori).

Configurare policy per l'eliminazione sicura di file digitali.

Evitare condivisioni non necessarie: Non rivelare informazioni sensibili (password, dettagli aziendali) attraverso canali insicuri o non richiesti.

4. Protezione Contro il Phishing

Filtri anti-phishing: Utilizzare software di sicurezza per bloccare email sospette.

Valutazione di email sospette:

Controllare l'indirizzo del mittente per individuare falsificazioni.

Diffidare di richieste urgenti o troppo allettanti.

Uso di password uniche: Evitare di riutilizzare password su più account e cambiarle regolarmente.

5. Sicurezza Fisica

Prevenzione del tailgating:

Implementare sistemi di controllo accessi, come tornelli o porte con badge.

Formare i dipendenti a non consentire l'accesso a sconosciuti, anche per cortesia.

Videosorveglianza: Monitorare ingressi e aree sensibili con telecamere di sicurezza.

6. Procedure Operative Standard

Linee guida per richieste sensibili: Stabilire processi chiari per richieste di modifiche ai pagamenti, accesso a dati o interventi tecnici, prevedendo sempre conferme multiple.

Accesso remoto sicuro: Garantire che i dipendenti accedano ai sistemi aziendali solo tramite connessioni VPN e dispositivi autorizzati.

7. Resilienza Tecnologica

Segmentazione della rete: Limitare i danni isolando parti della rete in caso di violazione.

Monitoraggio e audit regolari: Implementare sistemi di rilevamento delle intrusioni (IDS) e controlli per individuare attività insolite.

Aggiornamento regolare dei software: Assicurarsi che tutti i sistemi e i software siano aggiornati per evitare exploit di vulnerabilità conosciute.

8. Politiche di Segnalazione

Canali di segnalazione chiari: Creare un sistema semplice e anonimo per riportare attività sospette.

Risposta rapida agli incidenti: Avere un piano ben definito per gestire eventuali attacchi o compromissioni.

Il Common Vulnerabilities and Exposures (CVE) è un sistema standardizzato per identificare e catalogare le vulnerabilità di sicurezza informatica in software, hardware e firmware. Ogni CVE è associato a un identificativo univoco (es. CVE-2023-12345) che consente alle organizzazioni di condividere informazioni sulle vulnerabilità e di adottare misure correttive appropriate.

Red Hat

Per ottenere un elenco completo dei CVE relativi a uno specifico software o sistema operativo, è consigliabile consultare il sito ufficiale del programma CVE, che offre funzionalità di ricerca per prodotto, versione e altri criteri.

CVE

Di seguito, presento alcune vulnerabilità note relative a Microsoft Windows, con dettagli sulle vulnerabilità e le soluzioni consigliate:

1. CVE-2021-34527: PrintNightmare

Descrizione: Questa vulnerabilità nel servizio Print Spooler di Windows consente l'esecuzione di codice remoto, permettendo a un attaccante di installare programmi, visualizzare, modificare o cancellare dati, e creare nuovi account con pieni diritti utente.

Wikipedia

Soluzione: Microsoft ha rilasciato aggiornamenti di sicurezza per risolvere questa vulnerabilità. È fondamentale applicare immediatamente queste patch e, se il servizio

Print Spooler non è necessario, considerare la sua disabilitazione come misura preventiva.

2. CVE-2020-0796: SMBGhost

Descrizione: Una vulnerabilità nel protocollo Server Message Block 3.1.1 (SMBv3) di Windows 10 e Windows Server permette a un attaccante non autenticato di eseguire codice arbitrario sul sistema target, potenzialmente propagando malware simile a un worm.

Wikipedia

Soluzione: Microsoft ha distribuito patch di sicurezza per questa vulnerabilità. È essenziale aggiornare i sistemi interessati e, come misura aggiuntiva, bloccare la porta TCP 445 sul firewall per prevenire accessi non autorizzati.

3. CVE-2016-5195: Dirty COW

Descrizione: Una vulnerabilità nel kernel Linux che consente a un utente locale di ottenere privilegi elevati sfruttando una condizione di competizione nel meccanismo di copy-on-write.

Wikipedia

Soluzione: Le principali distribuzioni Linux hanno rilasciato aggiornamenti del kernel per correggere questa vulnerabilità. È cruciale applicare questi aggiornamenti e monitorare regolarmente le patch di sicurezza.

Nota: Le informazioni sulle vulnerabilità sono in continua evoluzione. È pertanto consigliabile consultare fonti ufficiali e aggiornate per ottenere dettagli specifici e le soluzioni più recenti.