Tecniche comuni di social engineering:

Phishing: Il phishing è una delle forme più diffuse di social engineering e consiste nell'invio di messaggi fraudolenti, come e-mail o SMS, che sembrano provenire da fonti legittime (banca, servizi online, ecc.). L'obiettivo è ingannare la vittima per farle inserire credenziali di accesso o informazioni personali su siti web falsi o in risposta a messaggi fasulli.

Spear Phishing: Simile al phishing, lo spear phishing è più mirato. L'attaccante personalizza il messaggio utilizzando informazioni specifiche sulla vittima, rendendo l'e-mail o il messaggio più credibile.

Tailgating: Tailgating, o "piggybacking", è una tecnica in cui un attaccante entra in un'area protetta seguendo una persona autorizzata. Questo può avvenire quando qualcuno apre una porta con un badge, e l'attaccante si infila subito dopo, approfittando della distrazione o del fatto che la porta rimane aperta.

Pretexting: Nel pretexting, l'attaccante crea una storia (pretesto) per ottenere informazioni sensibili. Finge di essere una figura di autorità o un collega e convince la vittima a fornire dati o eseguire azioni che comprometteranno la sicurezza.

Baiting: Con il baiting, l'attaccante utilizza un'esca per indurre la vittima a compiere un'azione rischiosa, come scaricare un malware o fornire informazioni. Le esche possono essere fisiche (ad esempio, una chiavetta USB infetta lasciata in un posto pubblico) o digitali (ad esempio, un download gratuito di software compromesso).

Vishing: Vishing è il phishing via telefono. Gli attaccanti chiamano le vittime, spesso fingendosi rappresentanti di aziende affidabili, per convincerle a fornire informazioni sensibili o trasferire denaro.

Smishing: Smishing è il phishing via SMS, in cui l'attaccante invia messaggi di testo che invitano la vittima a cliccare su link dannosi o a fornire informazioni personali.

Per difendersi dagli attacchi di social engineering è fondamentale adottare un insieme di strategie che coprano sia aspetti tecnici sia quelli comportamentali. Di seguito, ecco alcune strategie efficaci, collegate alle tecniche di attacco elencate in precedenza:

1. Formazione e sensibilizzazione del personale

Una delle difese più efficaci contro il social engineering è la formazione continua dei dipendenti e degli utenti. Le persone devono essere consapevoli delle minacce e sapere come riconoscerle.

Training regolari: Organizzare corsi di formazione che includano simulazioni di attacchi di phishing, vishing e altre tecniche di social engineering.

Consapevolezza delle tecniche di attacco: Informare regolarmente il personale sui nuovi metodi di attacco in circolazione e sugli indicatori di truffe, come link sospetti o richieste insolite via e-mail o telefono.

Segnalazione immediata: Incoraggiare i dipendenti a segnalare subito e-mail o chiamate sospette ai team di sicurezza IT, senza timore di ritorsioni.

2. Autenticazione Multi-Fattore (MFA)

L'uso dell'autenticazione multi-fattore aggiunge un livello di sicurezza aggiuntivo anche se le credenziali vengono compromesse in un attacco di phishing o pretexting.

Implementazione obbligatoria: Applicare l'MFA per l'accesso a sistemi critici e dati sensibili, richiedendo sia una password che un secondo fattore come un codice SMS, una notifica su un'app o una chiave fisica.

MFA in tutti gli account: Utilizzare l'MFA anche su account di posta elettronica e social media per proteggersi da attacchi mirati (spear phishing) che potrebbero compromettere dati personali.

3. Politiche di sicurezza rigorose e applicate

Implementare e far rispettare politiche aziendali che regolino l'accesso ai dati e ai sistemi, riducendo il rischio di social engineering.

Accesso basato sui privilegi minimi: Garantire che i dipendenti abbiano accesso solo ai dati e ai sistemi strettamente necessari per svolgere il proprio lavoro, limitando le opportunità di abuso in caso di attacco.

Controlli di identità rigorosi: Non dare mai per scontato che un e-mail o una telefonata siano autentici solo perché sembrano provenire da una fonte affidabile. Verificare sempre l'identità dell'interlocutore utilizzando canali di comunicazione separati, ad esempio richiamando un numero ufficiale.

4. Verifica delle richieste sospette

Per contrastare attacchi come pretexting o spear phishing, è fondamentale avere processi per la verifica delle richieste che sembrano sospette o urgenti.

Controlli aggiuntivi: Prima di eseguire richieste finanziarie o divulgare informazioni sensibili, verificare tramite una doppia conferma, ad esempio contattando il presunto richiedente tramite un numero di telefono ufficiale o parlando direttamente con il responsabile.

Diffidare dalle urgenze: Gli attacchi di social engineering spesso creano un senso di urgenza per ridurre la capacità critica della vittima. In questi casi, è utile fermarsi, valutare la situazione e cercare una conferma aggiuntiva.

5. Filtri anti-phishing e sicurezza e-mail

Implementare soluzioni tecniche per proteggere la posta elettronica e prevenire attacchi di phishing e spear phishing.

Filtri e-mail avanzati: Utilizzare filtri anti-phishing e anti-spam che analizzano automaticamente le e-mail alla ricerca di modelli sospetti, link dannosi o allegati pericolosi.

Segnalazione delle e-mail sospette: Abilitare un'opzione semplice per segnalare le e-mail sospette, così che possano essere analizzate e, se necessario, bloccate prima che arrivino a tutti gli utenti.

6. Controllo fisico degli accessi

Per prevenire attacchi come tailgating, è importante implementare misure di sicurezza fisica per limitare l'accesso agli edifici o alle aree riservate.

Badge di sicurezza e serrature elettroniche: Utilizzare badge identificativi che permettono l'accesso solo a chi è autorizzato, e assicurarsi che le porte si chiudano automaticamente dopo l'ingresso.

Politiche anti-tailgating: I dipendenti devono essere formati per non consentire a estranei o non autorizzati di accedere agli edifici seguendoli. Ciò può includere misure come richiedere a chiunque di mostrare il badge o segnalare persone non identificate.

Sorveglianza video e guardie di sicurezza: Implementare la sorveglianza nelle aree più sensibili per monitorare e registrare accessi non autorizzati.

7. Protezione delle informazioni personali

Evitare di divulgare troppe informazioni personali sui social media o in altre piattaforme pubbliche, poiché gli attaccanti possono utilizzarle per personalizzare attacchi di spear phishing o pretexting.

Limitare la visibilità dei profili social: Impostare le opzioni di privacy in modo che solo contatti fidati possano vedere informazioni sensibili, come il luogo di lavoro o la posizione attuale.

Non condividere dati aziendali: Evitare di discutere apertamente dettagli sui ruoli aziendali, piani futuri o dettagli di sicurezza sui social network, poiché queste informazioni possono essere sfruttate dagli attaccanti.

8. Simulazioni di attacchi

Le simulazioni di attacchi di social engineering, come phishing o tailgating, possono aiutare a preparare i dipendenti a riconoscere e reagire correttamente a tentativi di attacco reali.

Test periodici di phishing: Inviare e-mail di phishing simulate per misurare come i dipendenti reagiscono e fornire formazione aggiuntiva se necessario.

Controlli di sicurezza fisica simulati: Effettuare simulazioni di tailgating o altre violazioni fisiche per vedere se i dipendenti sono in grado di riconoscere e segnalare situazioni potenzialmente pericolose.

9. Politiche di segnalazione di incidenti

Creare e diffondere chiare politiche aziendali che incoraggino i dipendenti a segnalare immediatamente qualsiasi comportamento sospetto o tentativi di attacco di social engineering.

Canali di segnalazione sicuri e anonimi: Fornire canali facili e riservati per segnalare incidenti di sicurezza, come attacchi di phishing, tailgating o tentativi di pretexting.

Risposta rapida agli incidenti: Assicurarsi che ci sia un team pronto a rispondere a segnalazioni di attacchi, per evitare che situazioni sospette si trasformino in veri e propri attacchi.

10. Utilizzare strumenti di sicurezza avanzati

L'adozione di strumenti tecnologici di sicurezza avanzati può aiutare a prevenire gli attacchi di social engineering prima che raggiungano gli utenti.

Software anti-malware e firewall: Proteggere i dispositivi aziendali con software che rileva e blocca automaticamente link pericolosi e allegati sospetti.

Browser sicuri e autenticazione crittografica: Utilizzare browser che avvertono gli utenti di siti potenzialmente dannosi e implementare sistemi di crittografia che proteggono le comunicazioni interne.