S5L4

Il Social Engineering

Il **social engineering** è un metodo di attacco psicologico in cui un aggressore manipola o inganna una persona per ottenere informazioni sensibili, accesso a sistemi, risorse o per compiere azioni che danneggiano un'organizzazione o un individuo. A differenza di altri tipi di attacco, come quelli informatici diretti (hacking), il social engineering sfrutta la fiducia, le emozioni o l'ignoranza umana per raggiungere l'obiettivo.

Gli attaccanti spesso si concentrano sugli esseri umani piuttosto che sulle vulnerabilità tecniche dei sistemi. Questo tipo di attacco può essere particolarmente pericoloso poiché si basa sulla psicologia umana, che è più difficile da proteggere rispetto alle tecnologie.

Tecniche Preferite dagli Attaccanti e Perché

Il **phishing** è una delle tecniche di social engineering più comuni. In pratica, l'attaccante invia un messaggio che sembra provenire da una fonte affidabile, come una banca, un'azienda, o addirittura un collega. Solitamente questo messaggio è un'email o un SMS che contiene un link che porta a un sito web falso, progettato per rubare credenziali o dati personali. I messaggi di phishing cercano spesso di creare un senso di urgenza o paura, come ad esempio avvisarti che il tuo account è stato compromesso e che devi "verificare subito" i tuoi dati per evitare danni. Un esempio classico è un'email che sembra provenire da PayPal, in cui ti si avverte di un'attività sospetta sul tuo account e ti viene chiesto di cliccare su un link per "aggiornare le tue informazioni".

Il **spear phishing**, invece, è una forma più mirata di phishing. Mentre nel phishing tradizionale l'attaccante invia messaggi a molte persone, nel spear phishing l'aggressore si concentra su una persona o un piccolo

gruppo di persone specifiche. In questo caso, l'attaccante raccoglie informazioni personali o aziendali per rendere l'attacco più credibile e su misura. A differenza del phishing generico, lo spear phishing può sembrare più autentico, magari simulando una comunicazione da un collega o da un superiore. Per esempio, l'attaccante potrebbe inviare un'email che sembra provenire da un tuo collega e chiederti di aprire un file allegato che, in realtà, contiene malware.

Un'altra variante del phishing è il **vishing**, o voice phishing, che avviene tramite telefonate. Qui l'attaccante si finge una persona di fiducia, come un dipendente di una banca o di una compagnia telefonica, e cerca di indurre la vittima a fornire informazioni sensibili, come numeri di conto o codici PIN. A volte l'attaccante crea una situazione di emergenza per fare in modo che la vittima reagisca impulsivamente e riveli dati che normalmente non condividerebbe. Per esempio, l'attaccante potrebbe telefonarti fingendosi un operatore di una compagnia telefonica e chiederti di verificare i tuoi dati per evitare una sospensione del servizio.

Il **tailgating**, o piggybacking, è un attacco fisico in cui l'aggressore sfrutta l'opportunità di seguire una persona autorizzata per entrare in un edificio o in un'area sicura senza che questa lo noti. Gli attaccanti spesso approfittano della cortesia delle persone: per esempio, quando qualcuno tiene la porta aperta per un collega senza chiedere un'identificazione. L'aggressore potrebbe approfittare di un momento in cui una persona entra in una zona protetta, come un ufficio, e seguirla senza destare sospetti. In questo modo, riesce ad accedere a un'area che sarebbe normalmente vietata senza che nessuno lo fermi.

Il **pretexting**, invece, si basa sulla creazione di una falsa identità o di uno scenario inventato per raccogliere informazioni da una persona. L'attaccante può fingere di essere un'autorità o qualcuno che ha bisogno di informazioni per una causa legittima. Questo tipo di attacco viene pianificato con molta attenzione e spesso

cerca di far leva sulla fiducia della vittima. L'obiettivo è indurre la persona a rivelare dettagli sensibili che normalmente non condivideresti. Un esempio classico è quando un attaccante si finge un investigatore o un tecnico, chiedendo informazioni riservate per "verificare la sicurezza" o "risolvere un problema", convincendo la vittima a cooperare senza sospettare nulla.

Le tecniche preferite dagli attaccanti spesso sono quelle che si basano sulla psicologia della vittima. In particolare:

- **Phishing e Spear Phishing**: Queste sono le tecniche più comuni perché gli attaccanti possono inviare messaggi a un gran numero di persone, sperando che almeno una persona cada nel tranello. La personalizzazione dello spear phishing lo rende ancora più efficace, soprattutto se le informazioni utilizzate sono ben ricercate.
- **Tailgating**: Pur essendo un attacco fisico, è molto efficace in contesti aziendali in cui le persone sono abituate ad essere cortesi o distratte. Inoltre, non richiede sofisticate competenze tecnologiche da parte dell'attaccante.

Queste tecniche sono spesso preferite perché sono relativamente facili da eseguire e non richiedono conoscenze avanzate di hacking. Gli attaccanti sfruttano la vulnerabilità umana, che è molto più prevedibile delle difese informatiche.

Strategie e buone abitudini per difendersi dagli attacchi di Social Engineering

Per contrastare efficacemente queste minacce, è indispensabile adottare un approccio multidisciplinare che combini formazione, procedure e strumenti tecnologici.

Educazione e Consapevolezza: La formazione dei dipendenti e degli utenti è la prima linea di difesa. Devono essere consapevoli delle tecniche comuni di social engineering e sapere come identificarle.

Best practice: Non aprire link o allegati sospetti provenienti da mittenti sconosciuti o inaspettati. Non fornire mai informazioni personali o aziendali sensibili (es. password, dettagli bancari, dati aziendali riservati) a meno che non si sia assolutamente certi della legittimità della fonte e della necessità della richiesta.

Autenticazione a Due Fattori (2FA): Implementare l'autenticazione a due fattori (o multi-fattore, MFA) riduce drasticamente il rischio di accesso non autorizzato agli account, anche nel caso in cui le credenziali (ad esempio, username e password) siano state compromesse tramite phishing.

Best practice: Abilitare e utilizzare sempre l'autenticazione a due fattori su tutti gli account sensibili, sia aziendali che personali, preferendo app di autenticazione dedicate rispetto agli SMS, dove possibile.

Verifica delle Comunicazioni: Quando si ricevono richieste di informazioni sensibili, azioni urgenti o pagamenti via email, telefono o messaggi, è sempre una buona pratica verificare la veridicità della comunicazione tramite un canale indipendente e affidabile.

Best practice: Evitare di rispondere direttamente a richieste non sollecitate. In caso di dubbio, contattare l'interessato o l'organizzazione tramite i canali ufficiali (numeri di telefono presenti sul sito web aziendale, indirizzi email ufficiali), senza utilizzare i contatti forniti nella comunicazione sospetta.

Controllo degli Accessi Fisici Il social engineering non è solo digitale. Limitare l'accesso fisico a zone sensibili e monitorare attentamente gli accessi agli edifici è cruciale per prevenire attacchi "pretexting" o "tailgating" che sfruttano la fiducia o l'inganno in ambiente fisico.

Best practice: Utilizzare sempre badge identificativi. Implementare politiche rigorose per garantire che solo le persone autorizzate possano entrare in aree protette e non permettere a persone sconosciute di seguirvi attraverso varchi di sicurezza senza identificazione.

Simulazioni di Phishing e Test di Consapevolezza: Eseguire periodicamente attacchi di phishing simulati all'interno dell'organizzazione è uno strumento efficace per testare la preparazione dei dipendenti e sensibilizzarli ulteriormente in un ambiente controllato.

Best practice: Creare campagne di sensibilizzazione e formazione basate sui risultati delle simulazioni, evidenziando i pericoli legati alla disattenzione e fornendo linee guida chiare su come reagire e a chi segnalare i tentativi sospetti.

Rilevamento di Malware e Protezione End-point Implementare software antivirus aggiornato, sistemi di rilevamento delle intrusioni (IDS/IPS) e soluzioni di protezione degli end-point è fondamentale per identificare e neutralizzare malware o attività sospette, soprattutto in caso di phishing con allegati malevoli.

Best practice: Mantenere tutti i sistemi operativi e i software applicativi costantemente aggiornati, in quanto gli aggiornamenti spesso includono patch di sicurezza per vulnerabilità conosciute. Effettuare scansioni regolari e utilizzare firewall.

Il social engineering è una minaccia persistente e in continua evoluzione, che si adatta abilmente alle emozioni e alla psicologia umana, rendendola particolarmente difficile da rilevare con i soli mezzi tecnologici. Proteggere la nostra azienda da queste minacce non richiede solo l'adozione di misure tecniche avanzate, ma anche e soprattutto la promozione di una cultura aziendale radicata nella consapevolezza, nella prudenza e nella responsabilità individuale. La chiave per difendersi dal social engineering è diventare consapevoli di questi meccanismi psicologici. Formare il personale ad **identificare segnali di inganno** e a **essere scettici** rispetto a richieste insolite o urgenti è fondamentale. La consapevolezza e l'educazione continua sui rischi psicologici legati a questi attacchi possono ridurre notevolmente le possibilità di successo degli aggressori.

In sostanza, la psicologia umana è il "veicolo" attraverso cui gli attaccanti conducono i loro attacchi di social engineering. Comprendere questi principi psicologici non solo aiuta a prevenire questi attacchi, ma anche a costruire difese più efficaci contro di essi.

La formazione continua del personale, l'uso sistematico di tecnologie di sicurezza come l'autenticazione a due fattori, la verifica scrupolosa di ogni comunicazione sospetta e la rigorosa applicazione delle politiche di sicurezza sono le chiavi per mitigare efficacemente il rischio di attacchi basati sul social engineering. Investire nella consapevolezza dei nostri dipendenti è l'investimento più efficace per costruire una barriera robusta contro queste minacce. Invitiamo tutti i membri del personale a prendere sul serio queste linee guida e a segnalare immediatamente qualsiasi attività sospetta al team di sicurezza IT.