Cos'è il Social Engineering

Il social engineering è una forma di attacco che sfrutta le debolezze umane anziché quelle tecnologiche per ottenere informazioni sensibili, accesso non autorizzato a sistemi o per indurre le persone a compiere determinate azioni. Gli attaccanti manipolano psicologicamente le vittime, facendo leva su fattori come la fiducia, la curiosità, la paura o l'autorità percepita, per raggiungere i loro obiettivi.

Tecniche più comuni utilizzate dagli attaccanti

1. **Phishing**

   Il phishing è una delle forme più diffuse di social engineering. Consiste nell'invio di comunicazioni fraudolente, spesso sotto forma di email, messaggi di testo o chiamate telefoniche, che sembrano provenire da fonti affidabili come banche, aziende o enti governativi. L'obiettivo è ingannare le vittime affinché forniscano informazioni personali come password, numeri di carte di credito o dati finanziari, o per indurle a cliccare su link malevoli che possono installare malware sui loro dispositivi.

2. **Tailgating (o Piggybacking)**

   Il tailgating è una tecnica che mira a ottenere accesso fisico non autorizzato a aree riservate o edifici. L'attaccante segue una persona autorizzata attraverso un punto di accesso controllato, come una porta con badge o un tornello, sfruttando la cortesia o la distrazione della vittima. Ad esempio, potrebbe fingere di aver dimenticato il proprio badge e chiedere di essere lasciato entrare, o semplicemente approfittare di una porta che rimane aperta per pochi secondi.

Altre tecniche comuni di social engineering

- **Pretexting**: L'attaccante crea un falso scenario (pretesto) per convincere la vittima a fornire informazioni o a compiere azioni specifiche. Potrebbe fingersi un collega, un tecnico dell'assistenza o un rappresentante dell'autorità.
- **Baiting**: Si offre una sorta di "esca" per attirare le vittime. Un esempio comune è lasciare una chiavetta USB infetta in un luogo pubblico, sperando che qualcuno la raccolga e la inserisca nel proprio computer.
- **Spear Phishing**: Simile al phishing, ma mirato a un individuo o un'organizzazione specifica. Gli attaccanti personalizzano le loro comunicazioni per renderle più credibili.
- **Vishing e Smishing**: Varianti del phishing che utilizzano rispettivamente le chiamate vocali (voice phishing) e i messaggi di testo (SMS phishing) per ingannare le vittime.

Come proteggersi dal social engineering

- **Educazione e consapevolezza**: Essere informati sulle varie tecniche di social engineering è il primo passo per difendersi.
- **Verifica delle richieste**: Non fornire informazioni sensibili o accesso a meno che non si sia certi dell'identità della persona che lo richiede.
- **Politiche di sicurezza**: Seguire le linee guida e le procedure stabilite dall'organizzazione per la sicurezza delle informazioni e l'accesso fisico.
- **Cautela nelle comunicazioni**: Diffidare di email, messaggi o chiamate sospette, soprattutto se richiedono azioni immediate o informazioni personali.
- **Utilizzo di strumenti di sicurezza**: Installare software antivirus e firewall, mantenere aggiornati i sistemi operativi e le applicazioni, e utilizzare l'autenticazione a più fattori quando possibile.

Il social engineering sfrutta elementi fondamentali del comportamento umano, rendendo difficile la protezione esclusivamente attraverso misure tecniche. Pertanto, combinare la formazione con pratiche di sicurezza solide è essenziale per mitigare i rischi associati a queste minacce.

Strategie più efficaci per difendersi dagli attacchi di Social Engineering

Il social engineering sfrutta le vulnerabilità umane, pertanto la difesa più efficace combina misure tecniche con la formazione e la consapevolezza delle persone. Ecco le strategie chiave per proteggersi da questi attacchi:

1. **Formazione e Consapevolezza del Personale**
    - **Programmi di formazione regolari**: Organizzare sessioni di formazione periodiche per educare il personale sui vari tipi di attacchi di social engineering, come riconoscerli e come reagire.
    - **Simulazioni di attacco**: Eseguire test di phishing simulati e altre esercitazioni per valutare la prontezza dei dipendenti e rinforzare le buone pratiche.
    - **Aggiornamenti sulle minacce attuali**: Informare costantemente il personale sulle nuove tecniche utilizzate dagli attaccanti.
2. **Procedure di Verifica dell'Identità**
    - **Autenticazione a più fattori (MFA)**: Implementare sistemi di autenticazione che richiedono più di un metodo di verifica per accedere a sistemi e dati sensibili.
    - **Verifica delle richieste**: Stabilire protocolli chiari per confermare l'identità di chi richiede informazioni o accesso, specialmente se le richieste arrivano tramite email o telefono.
3. **Politiche di Sicurezza Aziendali**
    - **Linee guida chiare**: Definire politiche aziendali riguardanti l'uso delle email, l'accesso ai dati e la condivisione di informazioni sensibili.
    - **Accesso basato sui ruoli**: Limitare l'accesso ai dati e ai sistemi solo a coloro che ne hanno effettivamente bisogno per il loro lavoro.

- **Segnalazione di incidenti**: Implementare un processo semplice e anonimo per segnalare potenziali attacchi o comportamenti sospetti.

4. **Sicurezza Fisica**

- **Controlli di accesso fisici**: Utilizzare badge, sistemi biometrici o codici per controllare l'accesso agli edifici e alle aree riservate.
- **Sorveglianza e monitoraggio**: Installare telecamere di sicurezza e sistemi di monitoraggio per dissuadere e rilevare accessi non autorizzati.
- **Politica sui visitatori**: Stabilire procedure per l'accompagnamento dei visitatori e per l'identificazione di persone non autorizzate.

5. **Tecnologie di Sicurezza Informatica**

- **Software antivirus e antimalware aggiornati**: Assicurarsi che tutti i dispositivi siano protetti con software di sicurezza aggiornati.
- **Filtri anti-spam e anti-phishing**: Utilizzare sistemi che filtrano le email sospette e bloccano i contenuti malevoli.
- **Aggiornamenti e patch**: Mantenere tutti i sistemi operativi e le applicazioni aggiornati per proteggersi da vulnerabilità note.

6. **Consapevolezza delle Informazioni Personali**

- **Limitare la condivisione di informazioni**: Evitare di condividere dettagli personali o aziendali sui social media o in ambienti pubblici.
- **Verifica delle fonti**: Diffidare di richieste non sollecitate di informazioni personali o aziendali, sia online che offline.

7. **Gestione delle Password**

- **Password forti e uniche**: Utilizzare password complesse e diverse per ogni account o sistema.
- **Utilizzo di gestori di password**: Impiegare strumenti sicuri per gestire e memorizzare le password.
- **Cambi regolari delle password**: Aggiornare periodicamente le password e dopo qualsiasi sospetto di compromissione.

8. **Cultura della Sicurezza**

- **Promuovere una mentalità di sicurezza**: Incoraggiare tutti i membri dell'organizzazione a considerare la sicurezza come parte integrante del loro lavoro quotidiano.
- **Comunicazione aperta**: Favorire un ambiente in cui i dipendenti si sentano a proprio agio nel segnalare incidenti o sospetti senza timore di ripercussioni.
- **Responsabilità condivisa**: Far comprendere che la sicurezza è una responsabilità collettiva, non solo del dipartimento IT.

9. **Test e Audit di Sicurezza**

- **Valutazioni periodiche**: Condurre audit di sicurezza regolari per identificare e correggere vulnerabilità nei sistemi e nelle procedure.
- **Test di penetrazione**: Ingaggiare esperti per simulare attacchi e valutare l'efficacia delle misure di sicurezza in atto.

10. **Piani di Risposta agli Incidenti**

    - **Procedure di emergenza**: Stabilire un piano dettagliato per rispondere rapidamente ed efficacemente in caso di attacco.
    - **Team dedicato**: Formare un gruppo di risposta agli incidenti con ruoli e responsabilità chiari.
    - **Lezioni apprese**: Dopo un incidente, analizzare cosa è successo e aggiornare le procedure per prevenire future occorrenze.

Conclusione

Difendersi dagli attacchi di social engineering richiede un approccio olistico che combina tecnologia, processi e, soprattutto, persone. Investire nella formazione e nella creazione di una cultura aziendale orientata alla sicurezza è fondamentale per ridurre il rischio e proteggere le informazioni sensibili sia a livello personale che organizzativo.

Lista dei CVE relativi a Windows 11

Windows 11, come qualsiasi altro sistema operativo, è soggetto a vulnerabilità di sicurezza che vengono identificate e catalogate attraverso il sistema CVE (Common Vulnerabilities and Exposures). Di seguito è riportata una lista di alcune vulnerabilità note relative a Windows 11, con dettagli su alcune di esse e le soluzioni consigliate.

Elenco di alcune vulnerabilità (CVE):

1. **CVE-2022-21907** - Vulnerabilità di esecuzione di codice remoto nello stack del protocollo HTTP di Windows.
2. **CVE-2022-30190** - Vulnerabilità di esecuzione di codice remoto in Microsoft Support Diagnostic Tool (conosciuta come "Follina").
3. **CVE-2022-26925** - Vulnerabilità di spoofing in Windows LSA (Local Security Authority).
4. **CVE-2022-22047** - Vulnerabilità di elevazione dei privilegi nel Client/Server Runtime Subsystem (CSRSS).
5. **CVE-2022-24521** - Vulnerabilità di elevazione dei privilegi nel driver del sistema di file di registro comune di Windows.
6. **CVE-2023-23397** - Vulnerabilità di esecuzione di codice remoto in Microsoft Outlook.
7. **CVE-2023-28252** - Vulnerabilità di elevazione dei privilegi nel driver del sistema operativo Windows.
8. **CVE-2023-21674** - Vulnerabilità di elevazione dei privilegi nel kernel di Windows.

Dettagli su alcune vulnerabilità:

1. CVE-2022-21907 - Vulnerabilità di esecuzione di codice remoto nello stack del protocollo HTTP di Windows

Dettagli della vulnerabilità:

Questa vulnerabilità riguarda lo stack del protocollo HTTP (http.sys) di Windows. Un attaccante remoto non autenticato potrebbe sfruttare questa vulnerabilità inviando una richiesta HTTP appositamente predisposta al server target, causando l'esecuzione di codice arbitrario.

Impatto potenziale:

- **Esecuzione di codice remoto**: L'attaccante potrebbe eseguire codice con privilegi di sistema.
- **Compromissione completa del sistema**: Possibilità di installare programmi, visualizzare, modificare o eliminare dati, o creare nuovi account con pieni diritti utente.

Soluzioni consigliate:

- **Aggiornamento di sicurezza**: Applicare immediatamente la patch fornita da Microsoft tramite Windows Update.
- **Mitigazioni temporanee**: Se non è possibile applicare la patch immediatamente, disabilitare temporaneamente l'HTTP Trailer Support modificando il registro di sistema.

---

2. CVE-2022-30190 - Vulnerabilità di esecuzione di codice remoto in Microsoft Support Diagnostic Tool (MSDT) ("Follina")

Dettagli della vulnerabilità:

Conosciuta come "Follina", questa vulnerabilità permette a un attaccante di eseguire codice arbitrario tramite Microsoft Word. L'attacco sfrutta la possibilità di chiamare MSDT tramite un protocollo URL appositamente formato quando un documento di Office viene aperto.

Impatto potenziale:

- **Esecuzione di codice remoto**: L'attaccante può eseguire comandi con i privilegi dell'utente vittima.
- **Compromissione dei dati**: Possibilità di accedere, modificare o eliminare informazioni sensibili.

Soluzioni consigliate:

- **Aggiornamento di sicurezza**: Installare le patch rilasciate da Microsoft per correggere la vulnerabilità.
- **Disabilitare il protocollo MSDT URL**: Come mitigazione temporanea, è possibile disabilitare l'associazione del protocollo MSDT URL nel registro di sistema.

---

3. CVE-2023-23397 - Vulnerabilità di esecuzione di codice remoto in Microsoft Outlook

Dettagli della vulnerabilità:

Questa vulnerabilità consente a un attaccante di ottenere l'hash NTLM dell'utente inviando un messaggio email appositamente creato, che verrà elaborato da Outlook senza necessità di interazione dell'utente.

Impatto potenziale:

- **Furto di credenziali**: L'attaccante può autenticarsi come l'utente vittima in altri servizi che accettano l'autenticazione NTLM.
- **Accesso non autorizzato**: Possibilità di accedere a risorse di rete protette.

Soluzioni consigliate:

- **Aggiornamento di sicurezza**: Applicare le patch fornite da Microsoft per Microsoft Outlook.

- **Bloccare le connessioni SMB in uscita**: Configurare il firewall per bloccare le connessioni in uscita sulle porte 445/TCP.

---

4. CVE-2022-24521 - Vulnerabilità di elevazione dei privilegi nel driver del sistema di file di registro comune di Windows

Dettagli della vulnerabilità:

Un attaccante locale potrebbe sfruttare questa vulnerabilità per eseguire codice con privilegi elevati a causa di una gestione impropria degli oggetti in memoria da parte del driver del sistema di file di registro comune.

Impatto potenziale:

- **Elevazione dei privilegi**: L'attaccante può ottenere privilegi di amministratore sul sistema.
- **Compromissione del sistema**: Possibilità di eseguire qualsiasi operazione sul sistema target.

Soluzioni consigliate:

- **Aggiornamento di sicurezza**: Installare gli aggiornamenti disponibili tramite Windows Update.
- **Limitare l'accesso fisico**: Assicurarsi che solo utenti fidati abbiano accesso fisico al dispositivo.

Consigli generali per la protezione dalle vulnerabilità:

1. **Mantenere il sistema aggiornato:**
    - **Aggiornamenti automatici**: Abilitare gli aggiornamenti automatici per ricevere le ultime patch di sicurezza.
    - **Verifiche periodiche**: Controllare regolarmente la disponibilità di aggiornamenti per il sistema operativo e le applicazioni installate.
2. **Utilizzare soluzioni di sicurezza affidabili:**
    - **Software antivirus e antimalware**: Installare e mantenere aggiornati programmi di sicurezza per rilevare e prevenire minacce.
    - **Firewall**: Assicurarsi che il firewall di Windows sia attivo o utilizzare un firewall di terze parti.
3. **Formazione e consapevolezza:**
    - **Email sospette**: Non aprire allegati o cliccare su link in email non richieste o sospette.
    - **Download da fonti affidabili**: Scaricare software solo da siti ufficiali o riconosciuti.
4. **Gestione delle password:**
    - **Password forti**: Utilizzare password complesse e uniche per ogni account.
    - **Autenticazione a più fattori (MFA)**: Abilitare l'MFA dove possibile per aggiungere un ulteriore livello di sicurezza.
5. **Backup regolari:**

- **Backup dei dati**: Eseguire regolarmente backup dei dati importanti su dispositivi esterni o servizi cloud sicuri.
- **Verifica dei backup**: Testare i backup per assicurarsi che i dati possano essere ripristinati correttamente.

6. **Configurazioni di sicurezza avanzate:**

- **Controllo degli accessi**: Limitare i privilegi utente al minimo necessario.
- **Politiche di gruppo**: Utilizzare le politiche di gruppo per implementare configurazioni di sicurezza coerenti in ambienti aziendali.

Conclusione

La sicurezza informatica è un processo continuo che richiede attenzione costante. Rimanere informati sulle ultime vulnerabilità e applicare tempestivamente le soluzioni consigliate è fondamentale per proteggere i propri sistemi e dati. Adottando pratiche di sicurezza proattive e mantenendo una postura di difesa multilivello, è possibile mitigare efficacemente i rischi associati alle vulnerabilità di Windows 11.