Social Engineering

Il social engineering è una tecnica di attacco informatico che sfrutta la manipolazione psicologica per ingannare le persone e ottenere informazioni riservate, accesso a sistemi o eseguire azioni che compromettono la sicurezza. Gli attaccanti fanno leva sulla fiducia, la disattenzione o la mancanza di conoscenza della vittima per raggiungere il loro scopo.

Tecniche più comuni di social engineering

1. **Phishing** – L'attaccante invia e-mail fraudolente che sembrano provenire da fonti legittime (banche, aziende, servizi online) per indurre la vittima a rivelare credenziali, scaricare malware o effettuare pagamenti. Varianti:
    - **Spear phishing**: Attacco mirato su una persona o azienda specifica.
    - **Whaling**: Presa di mira di figure di alto livello, come dirigenti aziendali.
    - **Smishing**: Phishing via SMS.
    - **Vishing**: Phishing vocale, spesso via telefono.
2. **Tailgating** (o **Piggybacking**) – L'attaccante si introduce fisicamente in un'area riservata seguendo una persona autorizzata, sfruttando la cortesia umana (es. chiedendo di tenere aperta la porta) o fingendo di essere un dipendente.
3. **Pretexting** – Creazione di un pretesto convincente per ottenere informazioni sensibili. L'attaccante può fingersi un tecnico IT, un agente di supporto o un dirigente aziendale per convincere la vittima a rivelare credenziali o dati riservati.
4. **Baiting** – L'attaccante offre un'esca, come una chiavetta USB infetta lasciata in un luogo pubblico o un link a un file apparentemente interessante, per indurre la vittima a eseguire un'azione dannosa.
5. **Quid pro quo** – Simile al baiting, ma l'attaccante offre un vantaggio in cambio di informazioni. Ad esempio, si finge un tecnico IT che offre assistenza gratuita, inducendo la vittima a fornire credenziali di accesso.
6. **Shoulder surfing** – Osservare qualcuno mentre digita password o dati sensibili, ad esempio guardando sopra la spalla della vittima in luoghi pubblici come aeroporti o caffè.
7. **Dumpster diving** – Ricerca di informazioni riservate nei rifiuti aziendali, come documenti con password, dati finanziari o altre informazioni sensibili.

Come difendersi dal social engineering

- Essere scettici e verificare sempre le richieste di informazioni.
- Non cliccare su link o aprire allegati sospetti nelle e-mail.
- Usare autenticazione a più fattori (MFA).
- Non rivelare informazioni sensibili via telefono o e-mail senza conferme ufficiali.
- Bloccare accessi fisici non autorizzati e non lasciare dispositivi incustoditi.
- Formare dipendenti e utenti sulla sicurezza informatica.

1. Difendersi dal Phishing (E-mail, SMS, Telefonico)

✅ **Verificare il mittente** – Controlla sempre l'indirizzo e-mail del mittente per assicurarti che provenga da una fonte legittima.
✅ **Non cliccare su link sospetti** – Passa il mouse sopra il link per vedere l'URL di destinazione prima di cliccare. Se sembra strano, non aprirlo.
✅ **Diffidare delle urgenze** – Le e-mail che ti spingono ad agire rapidamente (es. "Il tuo account verrà chiuso in 24 ore!") sono spesso truffe.
✅ **Chiamare direttamente la fonte** – Se ricevi una richiesta sospetta, contatta direttamente l'azienda o l'ente tramite il numero ufficiale.
✅ **Utilizzare un filtro anti-phishing** – Molti servizi di posta elettronica come Gmail o Outlook bloccano i tentativi di phishing.
✅ **Abilitare l'autenticazione a più fattori (MFA)** – Anche se un attaccante ruba le credenziali, senza il secondo fattore non potrà accedere al tuo account.

---

2. Difendersi dal Tailgating (Ingresso non autorizzato)

✅ **Non aprire la porta a sconosciuti** – Anche se sembrano legittimi, chiedi sempre un tesserino di identificazione o conferma con la reception.
✅ **Usare badge e controlli di accesso** – Le aziende dovrebbero implementare sistemi di badge o smart card per limitare l'accesso agli edifici.
✅ **Formare i dipendenti** – Il personale deve essere istruito a non far entrare persone senza autorizzazione, anche se sembrano cortesi o in difficoltà.
✅ **Videosorveglianza e sicurezza** – Telecamere e guardie di sicurezza possono aiutare a prevenire accessi non autorizzati.

---

3. Difendersi dal Pretexting (Manipolazione per ottenere informazioni)

✅ **Verifica sempre l'identità** – Non fornire mai informazioni sensibili a qualcuno che si spaccia per un tecnico o un collega senza verificare la loro identità con un responsabile.
✅ **Non condividere dati personali o aziendali al telefono** – Le aziende serie non ti chiederanno mai password o dati bancari al telefono.
✅ **Usare domande di sicurezza difficili da indovinare** – Evita domande con risposte facilmente reperibili sui social media (es. "Qual è il nome del tuo animale domestico?").

---

4. Difendersi dal Baiting (Esche dannose)

✅ **Non inserire USB sconosciute nel computer –** Se trovi una chiavetta USB per strada o in ufficio, non collegarla! Potrebbe contenere malware.
✅ **Scaricare software solo da fonti ufficiali** – Evita di scaricare programmi da siti non verificati che potrebbero nascondere virus o ransomware.
✅ **Usare software di protezione** – Antivirus e firewall aggiornati possono aiutare a bloccare file dannosi.

---

5. Difendersi dal Quid Pro Quo (False offerte di aiuto)

✅ **Diffidare di offerte "troppo belle per essere vere"** – Se qualcuno ti promette un premio, un servizio gratuito o assistenza tecnica senza motivo, probabilmente è una truffa.
✅ **Verifica l'identità prima di fornire informazioni** – Se qualcuno si finge un tecnico IT o un supporto clienti, verifica il suo nome e il suo ruolo nell'azienda.
✅ **Bloccare numeri sospetti** – Se ricevi chiamate ripetitive da qualcuno che chiede informazioni sensibili, segnala e blocca il numero.

---

6. Difendersi dallo Shoulder Surfing (Spiare informazioni visivamente)

✅ **Usare protezioni per schermo –** Le pellicole privacy impediscono a chi ti sta accanto di leggere lo schermo del tuo laptop o smartphone.
✅ **Digitare password con discrezione –** Copri la tastiera mentre inserisci le credenziali in luoghi pubblici.
✅ **Evitare di lavorare su dati sensibili in luoghi affollati** – Se possibile, lavora su documenti riservati solo in ambienti sicuri.

---

7. Difendersi dal Dumpster Diving (Ricerca di informazioni nei rifiuti)

✅ **Distruggere documenti sensibili –** Usa un distruggidocumenti per eliminare fogli con informazioni aziendali, dati personali o password scritte.
✅ **Non lasciare documenti riservati incustoditi** – Anche nei bidoni della spazzatura aziendali, assicurati che i dati sensibili siano distrutti.
✅ **Usare la crittografia per documenti digitali** – Non lasciare informazioni importanti in chiaro nei computer o su dispositivi di archiviazione.

💡 **Best Practices Generali**

🔹 **Formazione e sensibilizzazione** – La miglior difesa è la consapevolezza: organizza sessioni di formazione periodiche sulla sicurezza.
🔹 **Politiche aziendali di sicurezza** – Implementa regole chiare su come gestire e proteggere le informazioni.
🔹 **Monitoraggio e logging** – Tieni traccia degli accessi ai sistemi e ai locali aziendali per individuare attività sospette.
🔹 **Segnalazione di sospetti attacchi** – Se pensi di essere stato bersaglio di un tentativo di social engineering, avvisa subito il reparto IT o la sicurezza.

Relazione sulle Vulnerabilità di Windows 10 Home

Introduzione

Windows 10 Home, come tutte le versioni di Windows, è soggetto a vulnerabilità di sicurezza che possono compromettere l'integrità, la disponibilità e la riservatezza dei dati degli utenti. Queste vulnerabilità sono identificate attraverso il sistema CVE (Common Vulnerabilities and Exposures), un database globale che raccoglie informazioni sulle falle di sicurezza.

In questa relazione verranno analizzate alcune delle più recenti e significative vulnerabilità di Windows 10 Home, fornendo dettagli sulle cause, i potenziali rischi e le soluzioni consigliate per mitigare le minacce.

---

1. CVE-2024-43491

Descrizione:

Questa vulnerabilità riguarda lo **Stack di Servizio** di Windows 10 versione 1507. Un difetto nello stack ha causato il rollback delle correzioni per alcune vulnerabilità che interessano componenti opzionali, esponendo il sistema a potenziali attacchi.

Sistemi Affetti:

- Windows 10 versione 1507
- Windows 10 Enterprise 2015 LTSB
- Windows 10 IoT Enterprise 2015 LTSB

Soluzione Consigliata:

- Aggiornare il sistema operativo a una versione più recente di Windows 10.
- Microsoft ha interrotto il supporto per la versione 1507, quindi l'aggiornamento a una versione supportata garantirà la protezione da questa e altre vulnerabilità.

---

2. CVE-2025-21275

Descrizione:

Questa vulnerabilità riguarda una possibile elevazione dei privilegi tramite l'**App Installer** di Windows. Un utente malintenzionato potrebbe sfruttare questa falla per ottenere privilegi elevati sul sistema.

Sistemi Affetti:

- Tutte le versioni supportate di Windows 10.

Soluzione Consigliata:

- Applicare le patch di sicurezza rilasciate da Microsoft nel gennaio 2025.
- Mantenere il sistema aggiornato con gli ultimi aggiornamenti di sicurezza.

---

3. CVE-2024-21412

Descrizione:

Questa vulnerabilità è stata sfruttata in campagne di furto di informazioni, permettendo agli attaccanti di eseguire codice arbitrario sul sistema della vittima.

Sistemi Affetti:

- Versioni di Windows 10 precedenti all'aggiornamento KB5040525.

Soluzione Consigliata:

- Installare l'aggiornamento cumulativo KB5040525 rilasciato da Microsoft.

---

4. CVE-2021-36934 (HiveNightmare o SeriousSAM)

Descrizione:

Questa vulnerabilità consente a un utente senza privilegi amministrativi di accedere ai file di registro di sistema, esponendo le password di amministrazione e altre informazioni sensibili.

Sistemi Affetti:

- Tutte le versioni di Windows 10 fino a luglio 2021.

Soluzione Consigliata:

- Microsoft ha rilasciato una procedura per mitigare il problema, che include la restrizione degli accessi ai file di sistema sensibili e l'implementazione di aggiornamenti di sicurezza.

---

5. CVE-2021-26419

Descrizione:

Una vulnerabilità di esecuzione di codice remoto (RCE) che interessa Microsoft Internet Explorer 11 e 9 su diverse versioni di Windows 10. Un attaccante potrebbe creare un sito web appositamente progettato per sfruttare questa vulnerabilità quando visualizzato con Internet Explorer.

Sistemi Affetti:

- Versioni di Windows 10 con Internet Explorer 11 e 9.

Soluzione Consigliata:

- Applicare le patch di sicurezza rilasciate da Microsoft.
- Utilizzare browser più moderni e sicuri come Microsoft Edge, Google Chrome o Mozilla Firefox.

Best Practices per la Sicurezza

Per proteggersi da queste e altre vulnerabilità, si consiglia di adottare le seguenti misure di sicurezza:

Aggiornamenti Regolari:

- Mantenere sempre il sistema operativo e le applicazioni aggiornate con le ultime patch di sicurezza rilasciate da Microsoft.

Backup Periodici:

- Eseguire backup regolari dei dati importanti per prevenire perdite in caso di attacco o guasti del sistema.

Utilizzo di Software Antivirus:

- Installare e mantenere aggiornato un software antivirus affidabile per proteggere il sistema da malware e altre minacce.

Formazione sulla Sicurezza:

- Educare gli utenti sulle pratiche di sicurezza informatica, come il riconoscimento di e-mail di phishing e l'evitamento di download da fonti non attendibili.

Conclusione

Le vulnerabilità di Windows 10 Home rappresentano una minaccia significativa per gli utenti e le aziende, ma possono essere mitigate attraverso aggiornamenti tempestivi, una corretta configurazione della sicurezza e l'adozione di buone pratiche operative.

Rimanere informati sulle ultime minacce e adottare misure preventive è essenziale per garantire la sicurezza dei propri dati e del proprio sistema. Per ulteriori dettagli, si consiglia di consultare le fonti ufficiali di Microsoft e il National Vulnerability Database (NVD).