Relazione Discorsiva: Introduzione al Social Engineering

Introduzione

Il **social engineering** rappresenta una delle minacce più insidiose nel panorama della cybersecurity moderna. Si tratta di tecniche che sfruttano la psicologia umana per indurre le persone a rivelare informazioni sensibili o a compiere azioni dannose, come cliccare su link malevoli o fornire credenziali di accesso. A differenza di altre forme di attacco, il social engineering punta sull'elemento umano, spesso considerato l'anello debole della sicurezza informatica.

Tecniche Comuni di Social Engineering

1. **Phishing**
    - Consiste nell'invio di email, messaggi o chiamate fraudolente progettate per sembrare provenienti da fonti affidabili.
    - **Esempio**: Un'email che simula una banca e chiede di confermare le credenziali tramite un link.
    - **Impatto**: Furto di identità, accesso non autorizzato ad account bancari o aziendali.
2. **Tailgating**
    - Avviene quando un attaccante accede a una zona protetta seguendo una persona autorizzata, sfruttando spesso la cortesia o la distrazione.
    - **Esempio**: Fingere di aver dimenticato il badge per farsi aprire una porta sicura.
3. **Pretexting**
    - Si basa sull'invenzione di un pretesto convincente per ottenere informazioni sensibili.
    - **Esempio**: Una telefonata fingendosi un tecnico IT che richiede la password per risolvere un problema.
4. **Baiting**
    - Prevede l'uso di esche, come dispositivi USB infetti, per invogliare la vittima a interagire con l'elemento compromesso.

Strategie di Difesa

Per proteggersi dagli attacchi di social engineering, è fondamentale adottare strategie preventive:

1. **Educazione e Consapevolezza**
    - Formare gli utenti a riconoscere i segnali di phishing e altre tattiche.
    - Organizzare workshop o simulazioni di attacchi per migliorare la prontezza.
2. **Implementazione di Tecnologie di Sicurezza**
    - Utilizzare l'autenticazione a più fattori (MFA) per proteggere gli account.

    - Adottare software di rilevamento delle minacce per bloccare email fraudolente.
3. **Procedure di Verifica**
    - Instaurare protocolli per verificare richieste insolite, come chiamate per reset delle password.
4. **Controlli Fisici**
    - Installare sistemi di accesso sicuri e scoraggiare il tailgating tramite educazione e tecnologie come badge elettronici.

CVE e Vulnerabilità su Windows 11 Home

Gli attacchi di social engineering possono sfruttare vulnerabilità note, come quelle su Windows 11 Home:

1. **CVE-2024-21351**
    - Permette il bypass di funzionalità di sicurezza, mettendo a rischio dati sensibili.
    - **Soluzione**: Installare immediatamente le patch rilasciate da Microsoft.
2. **CVE-2023-21768**
    - Una vulnerabilità del driver di rete WinSock che consente di ottenere privilegi elevati.
    - **Prevenzione**: Monitorare le connessioni e aggiornare regolarmente il sistema.
3. **CVE-2023-21765**
    - Colpisce il servizio di spooler di stampa di Windows, consentendo attacchi di tipo "elevazione di privilegi".
    - **Mitigazione**: Disabilitare il servizio se non necessario e applicare le patch più recenti.

Conclusione

Il social engineering rappresenta una minaccia concreta e in evoluzione. Per difendersi è necessario non solo implementare strumenti tecnologici, ma soprattutto educare gli utenti e promuovere una cultura della sicurezza. Allo stesso tempo, è fondamentale mantenere aggiornati i sistemi per mitigare i rischi derivanti dalle vulnerabilità conosciute.