### **Il Social Engineering: Cos’è e Come Proteggersi**

Il **social engineering** è l’arte di manipolare psicologicamente le persone per ottenere informazioni riservate o accesso a sistemi. Questo tipo di attacco si basa sullo sfruttamento del fattore umano, spesso più vulnerabile rispetto alle tecnologie di sicurezza.

### 

### **Principali Tipologie di Attacchi**

1. **Phishing**
   * Invio di comunicazioni false (e-mail, SMS, chiamate) per ottenere dati sensibili o far cliccare su link dannosi.
   * **Varianti:** Spear phishing (mirato), whaling (dirigenti), smishing (via SMS), vishing (telefonate).
2. **Pretexting**
   * Creazione di un pretesto credibile per ottenere informazioni, come fingere di essere un tecnico IT.
3. **Baiting**
   * Promessa di qualcosa di allettante, come una chiavetta USB “abbandonata” contenente malware.
4. **Tailgating**
   * Accesso non autorizzato a un’area sicura seguendo una persona autorizzata.
5. **Quid Pro Quo**
   * Offerta di un servizio o un vantaggio in cambio di informazioni o accesso (es. falso supporto tecnico).
6. **Dumpster Diving**
   * Recupero di informazioni sensibili dai rifiuti aziendali (es. documenti stampati).
7. **Shoulder Surfing**
   * Spiare qualcuno mentre digita informazioni sensibili in pubblico.

### **Obiettivi degli Attacchi**

* **Raccolta di informazioni:** Password, dati personali, segreti aziendali.
* **Accesso non autorizzato:** Sistemi, database, reti.
* **Compromissione:** Installazione di malware o furto di proprietà intellettuali.

### **Come Difendersi**

1. **Educazione e Consapevolezza:**
   * Formare i dipendenti sui metodi di social engineering e condividere esempi reali.
2. **Verifica delle Richieste:**
   * Controllare sempre l’identità di chi richiede dati sensibili.
3. **Politiche di Sicurezza:**
   * Implementare procedure come il badge per l’accesso fisico e l’autenticazione a due fattori (2FA).
4. **Segnalazione:**
   * Creare una cultura aziendale in cui ogni attività sospetta venga immediatamente riportata.

### **CVE RHEL**

### 

### **1. Vulnerabilità in OpenPrinting CUPS (CVE-2024-47076, CVE-2024-47175, CVE-2024-47176, CVE-2024-47177)**

* **Descrizione**: Queste vulnerabilità interessano i componenti OpenPrinting CUPS su tutte le versioni di Red Hat Enterprise Linux (RHEL). Sebbene non siano attive nelle configurazioni predefinite, possono essere sfruttate da un utente malintenzionato per compromettere il sistema.
* **Soluzioni**:
  + Red Hat ha rilasciato aggiornamenti di sicurezza per correggere queste vulnerabilità. Si consiglia di aggiornare il pacchetto **cups** e le sue dipendenze tramite il comando: yum update cups
  + È importante rivedere la configurazione di CUPS per limitare gli accessi non autorizzati

### **2. CVE-2024-45001 (RHEL CoreOS)**

* **Descrizione**: Questa vulnerabilità riguarda la gestione dei contenitori in RHEL CoreOS, utilizzato in ambienti containerizzati come OpenShift. Un attaccante potrebbe sfruttare un'inadeguata validazione degli input per eseguire codice arbitrario.
* **Soluzioni**:
  + Utilizzare l'ultimo aggiornamento RHEL CoreOS tramite i processi automatizzati di OpenShift Update Service (OSUS).
  + Verificare le versioni installate usando il comando: oc adm release info <version>
  + Sostituire <version> con la versione specifica del sistema

### **3. CVE-2024-48802 (Kernel RHEL)**

* **Descrizione**: Un difetto nel kernel Linux può causare un'errata gestione della memoria, consentendo a un attaccante locale di elevare i propri privilegi.
* **Soluzioni**:
  + Applicare immediatamente gli aggiornamenti al kernel disponibili tramite: yum update kernel
  + Assicurarsi che il sistema venga riavviato dopo l'aggiornamento per applicare le patch in modo completo​

### **4. Raccomandazioni Generali**

* **Automazione delle patch**: Configurare strumenti come **Red Hat Insights** per monitorare e gestire automaticamente le vulnerabilità sui sistemi Red Hat.
* **Best practice di sicurezza**:
  + Abilitare il SELinux in modalità enforcing.
  + Limitare gli accessi amministrativi attraverso configurazioni SSH sicure.
  + Eseguire regolarmente controlli di sicurezza sulle immagini container e sulle configurazioni del sistema.