Contents

[1.3] Suscettibilità all'impersonificazione della figura di autorità

1. Definizione operativa: La probabilità misurabile che un dipendente si conformerà a una richiesta di sicurezza (ad es., condivisione di credenziali, bypass di un controllo) da un individuo che percepisce come una figura di autorità, senza eseguire una verifica adeguata.

2. Metrica principale e algoritmo:

- **Metrica:** Tasso di successo dell'impersonificazione (ISR). Formula: `ISR = N_impersonificazioni_riuscit / N_tentativi_di_impersonificazione`.
- **Pseudocodice:**

  python

  ```
  def calculate_isr(security_events, start_date, end_date):
      # Interrogare dati di phishing/pen-test simulati per campagne basate su autorità
      impersonation_attempts = query_security_events(
          source='phishing_simulator',
          event_type='authority_impersonation',
          date_range=(start_date, end_date)
      )
      successful_attempts = [e for e in impersonation_attempts if e.status == 'clicked' or e

      total_attempts = len(impersonation_attempts)
      successful_count = len(successful_attempts)

      ISR = successful_count / total_attempts if total_attempts > 0 else 0
      return ISR
  ```

- **Soglia di avviso:** `ISR > 0.15` (ad es., più del 15% dei tentativi hanno successo).

3. Fonti di dati digitali (input dell'algoritmo):

- **API della piattaforma di simulazione del phishing** (ad es., KnowBe4, Cofense): Risultati della campagna filtrati per tema del modello (ad es., "CEO Fraud", "IT Helpdesk").
- **Log del gateway di sicurezza della posta** (ad es., Mimecast, Proofpoint): Log di email con intestazioni spoofed da domini di autorità interna che sono stati consegnati alla posta in arrivo.
- **Log di audit EDR/Identity** (ad es., CrowdStrike, Azure AD): Eventi in cui un utente ha eseguito un'azione ad alto rischio (ad es., cambio password, reset MFA) immediatamente dopo aver ricevuto un'email da un indirizzo esterno sospetto.

4. Protocollo di audit da umano a umano: Condurre una simulazione controllata e debrief. Dopo un test di phishing pianificato, intervistare un campione di dipendenti che si sono conformati. Chiedi: "Cosa di questo messaggio lo ha reso sembra legittimo? Cosa, se non altro, hai fatto per verificare l'identità del mittente prima di intraprendere un'azione?" Cercare modelli nella mancanza di passaggi di verifica.

5. Azioni di mitigazione consigliate:

- **Mitigazione tecnica/digitale:** Implementare politiche rigorose di DMARC, DKIM e SPF per ridurre lo spoofing di posta. Distribuire strumenti di verifica dell'identità che forniscono indicatori visivi per le email interne.
- **Mitigazione umana/organizzativa:** Condurre una formazione mirata su tattiche di impersonificazione di autorità, enfatizzando un protocollo di verifica obbligatorio e facile da usare (ad es., "Chiama la persona utilizzando un numero noto dalla directory aziendale").
- **Mitigazione dei processi:** Istituire un processo formale e non punitivo per segnalare i sospetti tentativi di impersonificazione al fine di rafforzare il comportamento desiderato.