Contents

[1.7] Deferenza ai reclami di autorità tecnica

1. Definizione operativa: L'accettazione automatica di istruzioni o richieste da individui che utilizzano gergo tecnico o affermano competenze specializzate, senza mettere in dubbio la legittimità o le implicazioni di sicurezza della richiesta.

2. Metrica principale e algoritmo:

- **Metrica:** Tasso di conformità indotto dal gergo (JICR). Formula: `JICR = N_successioni_gergo / N_tentativi_gergo`.
- **Pseudocodice:**

  python

  ```
  # Meglio misurato tramite simulazioni di phishing mirate.
  def calculate_jicr(simulated_attack_data, start_date, end_date):
      # Interrogare i risultati della simulazione per campagne che utilizzano pretesti tecni
      tech_pretext_campaigns = query_simulations(
          theme=['it_support', 'system_upgrade', 'security_patch'],
          date_range=(start_date, end_date)
      )

      total_attempts = tech_pretext_campaigns.total_recipients
      success_count = tech_pretext_campaigns.clicked_count + tech_pretext_campaigns.complied

      JICR = success_count / total_attempts if total_attempts > 0 else 0
      return JICR
  ```

- **Soglia di avviso:** `JICR > 0.1` (ad es., tasso di successo superiore al 10% per attacchi di pretesto tecnico).

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

- **API della piattaforma di simulazione del phishing:** Dati da campagne in cui l'esca coinvolge l'autorità tecnica (ad es., "IT Helpdesk ha bisogno che tu esegua questo script", "Cloud Team richiede la verifica della password").
- **Log del gateway di posta/proxy:** Per rilevare attacchi nel mondo reale con esche simili che non sono state catturate dai filtri.

4. Protocollo di audit da umano a umano: Nelle sessioni di formazione, presentare uno scenario: "Ricevi una chiamata da 'Mike da IT' che dice che il tuo PC è infetto e che hai bisogno di andare su un sito web. Cosa fai?" Recita la conversazione per vedere se il dipendente chiede la verifica (ad es., numero di ticket, richiamata alla linea di helpdesk ufficiale).

5. Azioni di mitigazione consigliate:

- **Mitigazione tecnica/digitale:** Implementare un portale IT centralizzato in cui tutte le richieste legittime vengono registrate e possono essere verificate dai dipendenti. Utilizzare firme digitali per gli script ufficiali.

- **Mitigazione umana/organizzativa:** Formare i dipendenti su un semplice protocollo di verifica: “Stacca, trova il numero ufficiale da solo e richiama per verificare.” Addestrarli a riconoscere le tattiche di social engineering che utilizzano il gergo per creare confusione e urgenza.
- **Mitigazione dei processi:** Stabilire un processo chiaro e ben pubblicizzato per come IT comunicherà e non comunicherà con i dipendenti, impostando le aspettative per le interazioni legittime.