Contents

[3.1] Sfruttamento della Reciprocità

1. Definizione Operativa: La vulnerabilità del personale agli attacchi di social engineering che sfruttano il principio psicologico della reciprocità, in cui un piccolo favore o gesto da parte di un attaccante crea un obbligo inconscio di conformarsi a una richiesta malevola successiva.

2. Metrica Principale e Algoritmo:

- **Metrica:** Tasso di Accettazione delle Richieste di Reciprocità (RRAR). Formula: `RRAR = (Numero di richieste accettate precedute da un "favore") / (Numero totale di richieste precedute da un "favore")`.
- **Pseudocodice:**

  python

  ```
  def calculate_rrar(email_logs, im_logs, access_logs, start_date, end_date):
      """
      email_logs, im_logs: Dati di comunicazione
      access_logs: Per verificare se una richiesta è stata eseguita
      """
      # 1. Identifica i thread di comunicazione contenenti un "favore" (ad esempio, "Ti ho a
      threads_with_favors = find_threads_with_favor_keywords(email_logs, im_logs, start_date

      # 2. Estrai la richiesta successiva dallo stesso thread
      requests_after_favor = extract_subsequent_requests(threads_with_favors)

      # 3. Incrocia i dati con access/logs per vedere se la richiesta è stata soddisfatta
      accepted_requests = 0
      for req in requests_after_favor:
          if was_request_granted(req, access_logs):
              accepted_requests += 1

      # 4. Calcola RRAR
      total_requests = len(requests_after_favor)
      RRAR = accepted_requests / total_requests if total_requests > 0 else 0
      return RRAR
  ```

- **Soglia di Allerta:** `RRAR > 0.1` (Oltre il 10% delle richieste seguenti a un favore percepito sono concesse)

3. Fonti di Dati Digitali (Input dell'Algoritmo):

- **API Email/Instant Messaging (MS Graph, Slack):** Per scansionare le parole chiave relative ai favori e alle richieste (`"Ti ho inviato"`, `"puoi aiutarmi"`, `"come ringraziamento"`, `"per favore potresti"`).
- **Log IAM/Accesso e Sistemi di Ticketing:** Per determinare se una richiesta menzionata nella comunicazione è stata effettivamente eseguita.

4. Protocollo di Audit Umano-Umano: Integra scenari nella formazione di consapevolezza sulla sicurezza che testano il bias di reciprocità. Ad esempio, in un esercizio di phishing simulato, fornisci prima un'informazione genuina utile o un "aiuto" al target, quindi segui con una richiesta malevola. Misura il tasso di click-through/conformità rispetto a un gruppo di controllo che non ha ricevuto il favore iniziale.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Distribuisci gateway di sicurezza email configurati con regole avanzate di protezione dalle minacce per contrassegnare email esterne che contengono sia linguaggio relativo ai favori che richieste di azione successive.
- **Mitigazione Umana/Organizzativa:** Forma il personale per riconoscere esplicitamente il principio di reciprocità. Insegna loro a separare il favore dalla richiesta: "Grazie per l'informazione. Elaborerò la tua richiesta attraverso il sistema di ticketing ufficiale per la convalida".
- **Mitigazione del Processo:** Applica rigorosamente un processo che richiede che tutte le richieste di accesso, soprattutto quelle provenienti da canali informali, siano convalidate attraverso il sistema di ticketing ufficiale, indipendentemente dalla relazione o dal contesto.