Contents

[3.9] Minacce all'Identità Sociale

1. Definizione Operativa: La percezione che un protocollo di sicurezza o la sua applicazione minacci il senso di appartenenza, lo status o l'autostima di un individuo all'interno di un gruppo, portando a resistenza, non conformità o bypass covert.

2. Metrica Principale e Algoritmo:

- **Metrica: Punteggio Sentimentale di Percezione della Minaccia (TPSS)**. Questo richiede un'analisi NLP delle comunicazioni che seguono gli annunci relativi alla sicurezza o l'applicazione.
- **Pseudocodice:**

  python

  ```
  def calculate_tpss(chat_logs, comms_channel, time_after_event_hours=24):
      """
      Analizza il sentiment in un canale dopo un annuncio di aggiornamento di sicurezza.
      """
      # 1. Ottieni il timestamp dell'annuncio di sicurezza (ad esempio, "nuovo MFA richiesto
      announcement_time = get_announcement_time(comms_channel)

      # 2. Ottieni i messaggi nella finestra dopo l'annuncio
      start = announcement_time
      end = start + timedelta(hours=time_after_event_hours)
      messages = get_messages_in_window(chat_logs, comms_channel, start, end)

      # 3. Esegui l'analisi del sentiment su questi messaggi
      sentiment_scores = []
      for msg in messages:
          score = analyze_sentiment(msg.text) # Restituisce un punteggio tra -1 (negativo) e
          sentiment_scores.append(score)

      # 4. Calcola il sentiment medio. Un punteggio fortemente negativo indica un TPSS eleva
      TPSS = sum(sentiment_scores) / len(sentiment_scores) if sentiment_scores else 0
      return TPSS
  ```

- **Soglia di Allerta:** `TPSS < -0.3` (Sentiment significativamente negativo a seguito di un'iniziativa di sicurezza).

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

- **API Piattaforma di Comunicazione (Slack/Teams):** La fonte primaria per misurare la reazione agli annunci. Campi: `channel`, `text`, `reactions`, `timestamp`.
- **Piattaforme Email/Intranet:** Per ottenere il timestamp e il contenuto dell'annuncio di sicurezza originale.

4. Protocollo di Audit Umano-Umano: Conduci "pulse check" o sondaggi dopo il rollout di nuove misure di sicurezza. Fai domande come: "Pensi che questa nuova misura di sicurezza aiuti o ostacoli la capacità del tuo team di lavorare efficacemente?" "Capisci perché questo cambiamento è stato apportato per la nostra sicurezza?".

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Assicurati che l'esperienza utente dei strumenti di sicurezza sia il più fluida possibile per minimizzare l'attrito percepito e la minaccia all'efficienza.
- **Mitigazione Umana/Organizzativa:** Inquadra la sicurezza non come un set di regole restrittive, ma come un valore condiviso e una responsabilità collettiva che protegge l'intero gruppo ("noi contro gli attori di minaccia").
- **Mitigazione del Processo:** Coinvolgi i team presto nella fase di progettazione e test dei nuovi processi di sicurezza. Il loro feedback può aiutare a modellare il rollout in modo da minimizzare le minacce percepite all'identità e allo status.