Contents

[1.5] Conformità basata sulla paura senza verifica

1. Definizione operativa: Conformità a una direttiva di sicurezza o richiesta guidata principalmente dall'ansia o dalla paura di ritorsioni da parte di una figura di autorità, portando all'omissione dei passaggi di verifica standard o del pensiero critico.

2. Metrica principale e algoritmo:

- **Metrica:** Tasso di azione basato sulla paura (FAR). Formula: `FAR = N_azioni_paura / N_azioni_totali`.
- **Pseudocodice:**

  python

  ```
  # Questa metrica richiede la correlazione del comportamento con il tono della comunicazion
  def calculate_far(comms_data, action_logs, start_date, end_date):
      # 1. Identificare comandi ad alta pressione in comms (ad es., "FALO ORA O ALTRIMENTI",
      high_pressure_comms = analyze_sentiment_and_tone(comms_data, keywords=["urgent", "imme

      far_actions = 0
      # 2. Per ogni comunicazione ad alta pressione, trovare azioni sensibili alla sicurezza
      for comm in high_pressure_comms:
          user_actions = get_user_actions(user=comm.recipient, timeframe=comm.timestamp + ti
          # Cercare azioni atipiche per l'utente o che mancano di flag di verifica normali
          for action in user_actions:
              if action.sensitivity == 'high' and action.verification_level == 'low':
                  far_actions += 1

      total_high_risk_actions = count_high_risk_actions(action_logs)
      FAR = far_actions / total_high_risk_actions if total_high_risk_actions > 0 else 0
      return FAR
  ```

- **Soglia di avviso:** Una correlazione statisticamente significativa (`p-value < 0.05`) tra comunicazioni ad alta pressione e successive azioni basso-verifica ad alto rischio.

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

- **API delle piattaforme di comunicazione** (Slack, Teams): Per analizzare il tono e il contenuto delle direttive da manager/superiori.
- **Log SIEM/Applicazione:** Per acquisire azioni utente sensibili alla sicurezza successive (ad es., accesso ai dati, modifiche di sistema).
- **Log di gestione dell'identità e dell'accesso (IAM):** Per stabilire una baseline del comportamento utente normale.

4. Protocollo di audit da umano a umano: Durante i sondaggi sulla cultura della sicurezza, includere domande come: "Ho sentito la pressione di bypassare un passaggio di sicurezza per evitare di deludere il mio manager." Utilizzare una scala Likert. Condurre interviste confidenziali per esplorare le risposte positive in profondità.

5. Azioni di mitigazione consigliate:

- **Mitigazione tecnica/digitale:** Implementare "interruttori di circuito" tecnici obbligatori che forzano un ritardo e un controllo di verifica per le azioni critiche, anche in un contesto admin.
- **Mitigazione umana/organizzativa:** Favorire una cultura impeccabile focalizzata sulla sicurezza psicologica. La leadership deve esplicitamente premiare i dipendenti per aver messo in dubbio gli ordini e seguito le procedure sicure.
- **Mitigazione dei processi:** Istituire un canale formale e anonimo per segnalare la pressione a violare le politiche di sicurezza.