Contents

[4.5] Occultamento della Sicurezza Basato sulla Vergogna

1. Definizione Operativa: La tendenza a nascondere errori di sicurezza, sfioramento o mancanza di conoscenza a causa della paura dell'imbarazzo o della punizione, impedendo l'apprendimento organizzativo e creando vulnerabilità invisibili.

2. Metrica Principale e Algoritmo:

- **Metrica:** Near-Miss Reporting Rate (NMRR). Formula: `NMRR = N_sfioramenti_segnalati / E_sfioramenti_stimati`. *Poiché il numero vero è sconosciuto, lo stimiamo (E) tramite altri proxy.*
- **Pseudocodice:**

  python

  ```
  def estimate_nmrr(ticketing_system, chat_logs, keywords):
      """
      Stima NMRR confrontando i rapporti ufficiali con le discussioni nei canali informali.
      """
      # 1. Ottenere i rapporti di NEAR-MISS UFFICIALI dal sistema di ticketing (es. etichett
      official_reports = query_jira('project = SOC AND labels = near-miss')

      # 2. Cercare nei canali PRIVATI discussioni che indicano che un sfioramento è stato so
      private_messages = query_slack_dms(keywords) # keywords: ["oops", "almost", "close cal
      # Usare NLP/topic modeling per raggruppare messaggi che suggeriscono un evento di sfio
      inferred_near_misses = topic_cluster(private_messages)

      # NMRR è il rapporto tra rapporti ufficiali e eventi totali dedotti
      nmrr = len(official_reports) / (len(official_reports) + len(inferred_near_misses)) if
      return nmrr
  ```

- **Soglia di Allarme:** `NMRR < 0.5` (Meno della metà degli sfioramenti dedotti sono ufficialmente segnalati).

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

- **Sistema di Ticketing (Jira):** API per cercare i ticket con un tag `near-miss`.
- **Piattaforma di Comunicazione (Slack/Teams):** Accesso API *anonimizzato* per cercare le parole chiave nei canali privati/DM. **CRITICO: Questo deve essere fatto con piena supervisione etica, usando solo dati aggregati e anonimizzati.**

4. Protocollo di Audit Umano-su-Umano: Istituire un processo di post-mortem senza colpa e tracciare la partecipazione. Condurre sondaggi anonimi chiedendo: "Negli ultimi 6 mesi, hai commesso un errore di sicurezza che non hai segnalato? Perché?" Assicurare la sicurezza psicologica nel processo di risposta.

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Creare un canale di segnalazione anonimo integrato con il sistema di ticketing.
- **Mitigazione Umana/Organizzativa:** La leadership deve modellare pubblicamente la vulnerabilità discutendo i propri errori. Formalizzare e promuovere una cultura di post-mortem senza colpa.
- **Mitigazione del Processo:** Implementare un programma "Good Catch" che premia e celebra la segnalazione degli sfioramenti, disaccoppiandola dai risultati punitivi.