Contents

[3.5] Decisioni Guidate dalla Scarsità

1. Definizione Operativa: Il bias cognitivo in cui la scarsità percepita (ad esempio, di tempo, opportunità o risorse) scatena il processo decisionale impulsivo, portando gli individui ad aggirare i controlli di sicurezza per evitare di perdere un'opportunità.

2. Metrica Principale e Algoritmo:

- **Metrica: Frequenza di Bypass per Urgenza (UBF)**. Formula: `UBF = Conteggio delle azioni di sicurezza eseguite entro un breve tempo (T) da una comunicazione a tema scarsità.`
- **Pseudocodice:**

  python

```
def calculate_ubf(access_logs, chat_logs, email_logs, time_window_minutes=30):
    """
    Traccia le azioni di sicurezza precedute da segnali di urgenza.
    """
    # 1. Scansiona le comunicazioni per parole chiave di scarsità/urgenza
    urgency_comms = query_comms(
        [chat_logs, email_logs],
        keywords=["urgente", "ASAP", "ultima chance", "time-sensitive", "deadline", "solo
        period='14d'
    )

    bypass_actions = []
    # 2. Per ogni comunicazione urgente, verifica le azioni di sicurezza successive
    for comm in urgency_comms:
        user = comm.user
        start_time = comm.timestamp
        end_time = start_time + timedelta(minutes=time_window_minutes)

        # Cerca azioni di sicurezza da questo utente subito dopo il messaggio
        actions = get_actions(access_logs, user, start_time, end_time)
        for action in actions:
            if is_security_bypass(action): # ad esempio, aggira un blocco, disabilita un c
                bypass_actions.append(action)

    # 3. Restituisci la frequenza di tali eventi
    UBF = len(bypass_actions)
    return UBF
```

- **Soglia di Allerta:** `UBF > 5` per team per settimana.

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

- **Log Email Server (ad esempio, Microsoft Graph API):** Per scansionare le parole chiave di urgenza nelle righe di oggetto e nei corpi. Campi: `sender`, `recipients`, `subject`, `body_preview`, `timestamp`.
- **API Piattaforma di Comunicazione (Slack/Teams):** Come sopra.
- **Log Controlli di Sicurezza (ad esempio, VPN, EDR, Cloud Security):** Per rilevare le azioni di override. Campi: `user`, `event_name` (ad esempio, `OverrideBlock`, `BypassWarning`), `timestamp`.

4. Protocollo di Audit Umano-Umano: Dopo un incidente di sicurezza che coinvolge un'azione affrettata, condurre un post-mortem senza colpevolizzare. Chiedi: "Quale era la conseguenza percepita del ritardo? Cosa ha reso la situazione così urgente? Esistevano percorsi sicuri alternativi che avrebbero potuto rispettare la scadenza?".

5. Azioni di Mitigazione Consigliate:

- **Mitigazione Tecnica/Digitale:** Implementa "interruttori di protezione" tecnici che impongono un periodo di raffreddamento obbligatorio breve per determinate azioni ad alto rischio, visualizzando un avviso sulla tattica della scarsità.
- **Mitigazione Umana/Organizzativa:** Forma i dipendenti per riconoscere i modelli linguistici di scarsità artificiale utilizzati nel social engineering e per convalidare le richieste urgenti attraverso un canale secondario offline.
- **Mitigazione del Processo:** Pre-autorizza e documenta procedure fast-track per scenari veramente critici dal punto di vista aziendale, in modo che il personale non sia costretto a scegliere tra la sicurezza e il mancato rispetto di una vera scadenza.