Obiettivo del Progetto:

L'obiettivo è migliorare la resilienza dell'organizzazione agli attacchi ransomware attraverso una simulazione pratica di attacco che permette di identificare, testare e rafforzare le misure di sicurezza esistenti.

Descrizione della Simulazione di Attacco:

1. **Creazione dello Scenario di Attacco**:
    - Definire un caso realistico di attacco ransomware, che rispecchi le minacce attuali del settore.
    - Determinare i principali punti di ingresso del malware (ad esempio phishing, vulnerabilità nei software, accesso remoto).
    - Stabilire una sequenza di attacco simulata, includendo infezione iniziale, diffusione laterale e attivazione della crittografia.
2. **Obiettivi della Simulazione**:
    - Valutare la velocità e l'efficacia dei sistemi di rilevamento e risposta.
    - Verificare la capacità di contenimento dell'infezione in una sezione limitata della rete aziendale.
    - Testare la prontezza del personale nel riconoscere e rispondere a un attacco.
3. **Team Coinvolti**:
    - **IT Security Team**: Pianificazione e monitoraggio dell'attacco simulato.
    - **Personale IT Operativo**: Gestione e risposta tecnica.
    - **HR e Ufficio Legale**: Revisione delle politiche interne e delle pratiche di risposta.
    - **Management**: Revisione delle decisioni strategiche di sicurezza.

Fasi dell'Implementazione:

1. **Pre-Simulazione**:
    - Condurre una valutazione preliminare dei sistemi di sicurezza attuali.
    - Configurare un ambiente di test isolato per ridurre i rischi durante la simulazione.
    - Addestrare il personale su pratiche di riconoscimento delle email di phishing e sulle risposte immediate a comportamenti sospetti.
2. **Simulazione dell'Attacco**:
    - Lanciare il ransomware simulato nel punto di ingresso definito.
    - Monitorare il comportamento della rete e degli endpoint, rilevando i tentativi di accesso ai dati.
    - Eseguire test sulle capacità di isolamento e sulla prontezza nella disconnessione di sistemi compromessi.
3. **Post-Simulazione**:
    - Analizzare i risultati della simulazione, includendo il tempo di rilevamento, contenimento e recupero.
    - Identificare le aree di miglioramento sia nei processi tecnici che nelle pratiche del personale.

    - Aggiornare le policy di sicurezza, introducendo procedure migliorate di backup, segmentazione della rete e di gestione degli accessi.

Misure di Sicurezza Derivate:

- **Implementare Segmentazione della Rete**: Creare segmenti isolati per limitare la diffusione laterale.
- **Rafforzare i Sistemi di Backup**: Assicurarsi che i backup siano separati e verificati.
- **Formazione Continua del Personale**: Condurre sessioni periodiche di formazione sulla sicurezza informatica.
- **Valutazione Periodica della Sicurezza**: Programmare simulazioni regolari per adattare le misure di difesa alle nuove minacce.

Monitoraggio e Revisione:

Stabilire un piano di monitoraggio continuo dei sistemi di sicurezza per rilevare tempestivamente potenziali minacce e assicurare che i miglioramenti implementati abbiano un impatto tangibile sulla sicurezza aziendale.