- ***Definire un processo(semplificato) di aggiornamento di un server web (es. Apache), includendo le procedure per ogni attività:***

1. Individuare la necessità dell'aggiornamento
2. Valutarne la necessità
3. Backup del server
4. Leggere note e specifiche dell'aggiornamento
5. Metodo: automatico o manuale
6. Installazione su ambiente di staging
7. Installazione dell'update
8. Verifica (Testing & Checking) delle impostazioni post-update

- ***Sul processo appena definito, identificare 3 "catene" del rischio in forma qualitativa e descrittiva: Threat agent → Threat → Vulnerability → Impact → Risk***

1. *Threat agent*: Attaccanti esterni

Threat: Rilevamento di una vulnerabilità nota nel server web non aggiornato.

Vulnerability: Presenza di bug o falle di sicurezza non corrette nell'attuale versione del server web.

Impact: Possibile compromissione dei dati, interruzione dei servizi o danni alla reputazione dell'azienda.

Risk: Alto rischio di violazione della sicurezza e conseguenti danni finanziari e reputazionali.

2. Threat agent: Errori umani

Threat: Fallimento nel completare il backup completo prima dell'aggiornamento.

Vulnerability: Mancanza di una procedura di backup adeguata o negligenza nell'esecuzione.

Impact: Perdita di dati critici in caso di fallimento dell'aggiornamento o necessità di ripristino.

Risk: Moderato rischio di perdita di dati e interruzione dei servizi.

3. *Threat agent*: Errori di configurazione

Threat: Configurazione errata durante l'installazione dell'aggiornamento.

Vulnerability: Possibili conflitti di versione o errori di configurazione durante l'installazione dell'aggiornamento.

Impact: Possibile interruzione dei servizi web o danni alla funzionalità del server.

Risk: Moderato rischio di interruzione delle attività e perdita di reputazione per l'azienda.