DIGITAL RISK MANAGER - ALEX FIORILLO

RISK MANAGEMENT
PROCESSI E RISCHI

INTRODUZIONE

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

Esempio delle sole attività:
1. Valutare la necessità dell'aggiornamento
2. Effettuare Backup completo del server web
3. Scegliere Metodo Di aggiornamento
4. Scaricare L'aggiornamento
5...

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

PROCESSO DI AGGIORNAMENTO DEL SERVER WEB

APPROFONDIMENTO

Processo: un insieme di attività correlate o interagenti che trasformano gli input in output. Un processo prende uno o più input definiti e li trasforma in output definiti. I processi definiscono la sequenza delle azioni e le loro dipendenze.

Attività: unità di lavoro elementare all'interno di un processo.

Procedura: modo documentato per svolgere un'attività o un processo.

1. **Valutazione delle necessità di aggiornamento:**
   - Attività: Verificare la disponibilità di nuove versioni di Apache e gli aggiornamenti di sicurezza.
   - Procedura: Monitorare i canali ufficiali di Apache per notizie sugli aggiornamenti e le patch di sicurezza.

2. **Backup completo del server:**
   - Attività: Effettuare una copia di backup di tutti i file e dei database critici del server.
   - Procedura: Utilizzare strumenti di backup automatizzati per garantire una copia completa e aggiornata dei dati.

3. **Scegliere il metodo di aggiornamento:**
   - Attività: Determinare se eseguire l'aggiornamento manualmente o utilizzare strumenti automatizzati.
   - **Procedura:** Valutare i rischi e i benefici di ogni approccio e scegliere quello più adatto alla situazione.

4. **Scaricare l'aggiornamento:**
   - Attività: Acquisire e verificare la correttezza dell'aggiornamento scaricato.
   - Procedura: Scaricare l'aggiornamento dal sito ufficiale di Apache o da fonti attendibili e verificare l'integrità del file checksum.

   Quindi continuiamo da qui quelli che secondo noi dovrebbero essere gli step successivi nel processo di aggiornamento di un server web.

5. **Installare l'aggiornamento:**
   - Attività: Applicare l'aggiornamento al server web.
   - Procedura: Seguire le istruzioni fornite con l'aggiornamento per installarlo correttamente sul server.

6. **Verifica e test:**
   - Attività: Verificare che l'aggiornamento sia stato installato correttamente e testare

il funzionamento del server.

- Procedura: Eseguire test di funzionalità, sicurezza e prestazioni per assicurarsi che il server sia stabile e sicuro.

CATENE DI RISCHIO

Prendiamo in considerazione i primi tre passi del processo preso in esame, quindi valutazione delle necessità di aggiornamento, backup completo del server e scelta del metodo di aggiornamento per andare a identificare e descrivere tre catene del rischio.

1. **Valutazione delle necessità di aggiornamento**

   - Threat agent: Hacker malintenzionati.

   - **Threat:** Attacco tramite vulnerabilità conosciute non corrette dall'aggiornamento.

   - Vulnerability: Mancanza di aggiornamento tempestivo del server.

   - Impact: Possibile compromissione della sicurezza dei dati immagazzinati nel server.

   - Risk: Rischio elevato di attacchi e perdita di dati sensibili.

2. **Backup completo del server**

   - Threat agent: Errore umano o guasto hardware.

   - Threat: Perdita di dati durante il backup.

   - Vulnerability: Mancanza di procedure di backup robuste o mancata verifica dei dati durante l'aggiornamento.

   - Impact: Perdita permanente dati critici.

   - Risk: Rischio medio di perdita di dati a causa di errori umani o guasti hardware.

3. **Scelta metodo di aggiornamento**

   - Threat agent: Interferenze esterne, guasti del sistema.

   - Threat: Interruzione durante l'aggiornamento.

   - Vulnerability: Scelta di un metodo di aggiornamento non adeguato o non testato.

   - Impact: Downtime del server, indisponibilità dei servizi.

   - Risk: Rischio moderato di interruzioni dei servizi critici durante l'aggiornamento.