



# Digital Risk Manager – S1/L1

## PROCESSI E RISCHI

### »» Phantom srl

#### Phantom Team:

Alessio D'Ottavio

Davide Di Turo

Francesco Pio Scopece

Giuseppe Pinatello

Luca Iannone

Manuel Di Gangi

Marco Fasani

Oliviero Camarota

# TABLE OF CONTENTS

**03** Traccia

**04-06** Introduzione e Procedure

**07-08** Catene di rischio

**09** Consigli e Conclusioni

# TRACCIA

Definire un processo (semplificato) di aggiornamento di un server web (es. Apache), includendole procedure per ogni attività. Esempio delle sole attività:

1. Valutare la necessità dell'aggiornamento
2. Effettuare backup complete 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

# RISK MANAGEMENT NELL'AGGIORNAMENTO DEL SERVER WEB APACHE

## Introduzione:

L'aggiornamento del server web Apache è una pratica fondamentale per mantenere la sicurezza, le prestazioni e la funzionalità ottimali del nostro ambiente server. Tuttavia, questo processo presenta rischi che devono essere attentamente gestiti per garantire un'operatività senza problemi e la protezione dei nostri asset digitali.

## Fasi del Processo di Aggiornamento:

### 1. Valutazione della Necessità di Aggiornamento:

- Analizziamo i changelog di Apache per identificare le nuove funzionalità, le correzioni di bug e le vulnerabilità di sicurezza risolte.
- Valutiamo l'urgenza dell'aggiornamento in base ai rischi associati, come potenziali violazioni della sicurezza o riduzione delle prestazioni.

In questa fase, è fondamentale analizzare attentamente i changelog di Apache per comprendere le nuove funzionalità introdotte, le correzioni di bug e le vulnerabilità di sicurezza risolte. Questa valutazione ci aiuta a determinare l'urgenza dell'aggiornamento in base ai rischi associati. Ad esempio, patch di sicurezza critiche richiedono un'installazione immediata per mitigare il rischio di compromissione del server.

### 2. Backup Completo del Server Web:

- Effettuiamo un backup completo di tutti i file di configurazione, documenti del sito web e database.
- Utilizziamo strumenti di backup affidabili e testati per garantire l'integrità dei dati e la possibilità di ripristino in caso di necessità.

Prima di procedere con l'aggiornamento, è essenziale eseguire un backup completo di tutti i file di configurazione, documenti del sito web e database. Utilizzando strumenti di backup affidabili, assicuriamo l'integrità dei dati e la possibilità di ripristino in caso di necessità. Questo passaggio è cruciale per mitigare il rischio di perdita di dati durante l'aggiornamento.

### 3. Scelta del Metodo di Aggiornamento:

- Valutiamo se utilizzare il gestore dei pacchetti del sistema operativo o eseguire l'aggiornamento manuale.
- Consideriamo i rischi e i benefici di ciascun metodo in relazione alla complessità del nostro ambiente server e alla criticità del sito web.

La decisione sul metodo di aggiornamento (tramite il gestore dei pacchetti del sistema operativo o l'aggiornamento manuale) dipende dalla complessità dell'ambiente server e dalla criticità del sito web. È importante valutare attentamente i rischi e i benefici di ciascun metodo per garantire un processo sicuro ed efficiente.

### 4. Download e Installazione dell'Aggiornamento:

- Utilizziamo il gestore dei pacchetti del sistema operativo o scarichiamo manualmente l'aggiornamento dal sito ufficiale di Apache.
- Seguiamo attentamente le istruzioni per l'installazione per garantire un processo senza errori e sicuro.

Durante questa fase, scarichiamo l'aggiornamento da fonti attendibili e seguiamo attentamente le istruzioni per l'installazione per garantire un processo senza errori e sicuro. Verifichiamo che l'aggiornamento sia autentico e non compromesso, riducendo così il rischio di installare software dannoso o vulnerabile.

### 5. Verifica del Corretto Funzionamento del Server:

- Avviamo il server web Apache e testiamo tutte le funzionalità critiche per garantire che operino correttamente.
- Monitoriamo i log del server per individuare eventuali errori o problemi durante l'avvio.

Avviamo il server web Apache e testiamo tutte le funzionalità critiche per garantire che operino correttamente. Monitoriamo attentamente i log del server per individuare eventuali errori o problemi durante l'avvio. Questo ci aiuta a identificare tempestivamente e risolvere eventuali problemi post-aggiornamento.

#### 6. Monitoraggio Post - Aggiornamento:

- Monitoriamo attentamente il server per individuare eventuali anomalie di prestazione o problemi di compatibilità.
- Utilizziamo strumenti di monitoraggio delle prestazioni per rilevare eventuali problemi in tempo reale.

Dopo l'aggiornamento, monitoriamo attentamente il server per individuare eventuali anomalie di prestazione o problemi di compatibilità. Utilizziamo strumenti di monitoraggio delle prestazioni per rilevare e risolvere tempestivamente eventuali problemi in tempo reale.

#### 7. Gestione dei Problemi Riscontrati:

- Interveniamo prontamente per risolvere eventuali problemi riscontrati durante o dopo l'aggiornamento.
- Valutiamo l'opzione di rollback se necessario per ripristinare la continuità operativa in caso di malfunzionamenti critici.

In caso di problemi durante o dopo l'aggiornamento, interveniamo prontamente per risolverli e ripristinare la continuità operativa del server. Valutiamo l'opzione di rollback se necessario per tornare a una configurazione stabile e funzionante.

#### 8. Documentazione dell'Aggiornamento:

- Aggiorniamo la documentazione del server web con le informazioni relative alla versione aggiornata di Apache e ai cambiamenti apportati durante il processo di aggiornamento.
- Registriamo la data, l'ora e i dettagli dell'aggiornamento per scopi di audit e tracciabilità.

Infine, aggiorniamo la documentazione del server web con le informazioni relative alla versione aggiornata di Apache e ai cambiamenti apportati durante il processo di aggiornamento. Registriamo accuratamente la data, l'ora e i dettagli dell'aggiornamento per scopi di audit e tracciabilità.

# CATENE DEL RISCHIO IDENTIFICATE NEL PROCESSO DI AGGIORNAMENTO DEL SERVER WEB APACHE:

**Catena del rischio: Attacco da parte di un attaccante esterno:**



Hacker o gruppi di hacker.

Utilizzo di exploit noti o zero-day per sfruttare vulnerabilità non corrette nel server Apache non ancora aggiornato.

Presenza di vulnerabilità non corrette nella versione attuale di Apache.

Compromissione della sicurezza del server e dei dati ospitati, potenziali perdite finanziarie e danni reputazionali.

Rischio elevato di violazioni della sicurezza e di perdite finanziarie dovute all'accesso non autorizzato ai dati sensibili.

**Catena del Rischio: Errore Umano durante l'Aggiornamento:**



Operatori umani responsabili dell'aggiornamento del server.

Gli operatori umani commettono errori durante l'installazione dell'aggiornamento.

Installazione errata dell'aggiornamento o mancata verifica post-installazione.

Il server potrebbe smettere di funzionare correttamente o potrebbero verificarsi perdite di dati a causa di errori umani.

Moderato, poiché gli errori umani sono inevitabili, ma possono essere mitigati attraverso procedure di controllo di qualità e verifica.

## Catena del Rischio: Minaccia Interna (Utente Malevolo):



Dipendenti o ex dipendenti con accesso privilegiato al server.

Un utente interno malevolo tenta di ottenere accesso non autorizzato al server web Apache per danneggiare o rubare dati sensibili.

Il server potrebbe avere falle di sicurezza non corrette a seguito di aggiornamenti mancanti o incompleti.

L'utente malevolo potrebbe compromettere la sicurezza del server e dei dati, causando danni finanziari e reputazionali all'azienda.

Elevato, poiché gli utenti interni hanno familiarità con il sistema e possono sfruttare le vulnerabilità per scopi dannosi se non adeguatamente mitigati. Queste catene del rischio illustrano come diverse minacce, vulnerabilità e impatti possano interagire all'interno del processo di aggiornamento del server web Apache, evidenziando l'importanza di un'approfondita gestione dei rischi per garantire la sicurezza e l'affidabilità del sistema.

## CONSIGLI & CONCLUSIONI

Gestire efficacemente i rischi associati all'aggiornamento del server web Apache è essenziale per garantire un ambiente server sicuro e affidabile. Seguendo una procedura rigorosa e monitorando attentamente il processo, possiamo mitigare i rischi e assicurare un'operatività ottimale del nostro sistema.

Queste catene del rischio illustrano come diverse minacce, vulnerabilità e impatti possano interagire all'interno del processo di aggiornamento del server web Apache, evidenziando l'importanza di un'approfondita gestione dei rischi per garantire la sicurezza e l'affidabilità del sistema.