# RISK MANAGEMENT
# PROCESSI E RISCHI

MARIA HUAPAYA

# INDICE

# INDICE

# 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, identificare3 "catene" del rischio in forma qualitativa e descrittiva:

Threat agent → Threat → Vulnerability → Impact → Risk

# INTRODUZIONE

### Definizione di un Processo

Un processo è una serie di azioni o passi presi per raggiungere un particolare fine. Nel contesto tecnologico, un processo può essere definito come un insieme di attività sequenziali e interdipendenti che utilizzano risorse per trasformare input (dati, materie prime, etc.) in output (prodotti, servizi, etc.). I processi sono fondamentali per assicurare la ripetibilità e la qualità delle operazioni, offrendo un framework strutturato che aiuta a mantenere l'efficienza operativa e a minimizzare gli errori.

### Importanza e Funzionamento di un Processo

I processi sono cruciali per qualsiasi organizzazione poiché stabiliscono un metodo controllato per eseguire attività. Nel campo IT, il processo di aggiornamento di un sistema software, come un server web Microsoft IIS, è vitale per:

- Mantenere la Sicurezza: aggiornare il software per proteggere i dati e le operazioni da nuove vulnerabilità e attacchi cibernetici.
- Migliorare le Prestazioni: implementare miglioramenti che ottimizzano la velocità e l'efficacia del server.
- Garantire la Compatibilità: assicurare che il software rimanga compatibile con altri sistemi e tecnologie emergenti.
- Conformità Normativa: rispettare le normative e le leggi applicabili che possono influenzare le operazioni dell'azienda.

# IL PROCESSO DI AGGIORNAMENTO DEL SERVER WEB MICROSOFT IIS

### Valutazione della Necessità dell'Aggiornamento

La valutazione inizia con un'analisi completa dello stato attuale del sistema, specificatamente la versione 8.5 di Microsoft IIS. Le motivazioni principali per l'aggiornamento includono:

- Fine del Supporto: la versione 8.5 si avvicina alla fine del suo ciclo di vita supportato da Microsoft, riducendo la disponibilità di aggiornamenti di sicurezza.
- Miglioramenti Tecnologici: la versione 10.0 offre funzionalità avanzate e miglioramenti delle prestazioni che sono essenziali per le attuali esigenze aziendali.
- Rischi di Sicurezza: vulnerabilità non corrette nella versione 8.5 possono esporre l'organizzazione a rischi significativi, come violazioni dei dati e attacchi DDoS.

### Analisi delle Vulnerabilità

Identificazione specifica delle vulnerabilità nella versione 8.5 che includono:

- Vulnerabilità Conosciute: elenco delle vulnerabilità segnalate da fonti affidabili come il National Vulnerability Database (NVD) e il Microsoft Security Response Center (MSRC), che potrebbero essere sfruttate da attori malevoli.
- Valutazione dell'Impatto: analisi dell'impatto potenziale di queste vulnerabilità sull'ambiente aziendale, valutando la probabilità di sfruttamento e le conseguenze possibili.

### Revisione dei Log di Cambiamento

Esame dei log di cambiamento forniti da Microsoft per la versione 10.0 di IIS, per comprendere dettagliatamente le correzioni di sicurezza apportate, le nuove funzionalità introdotte e le eventuali modifiche alle configurazioni esistenti che possono influenzare sistemi e applicazioni integrati.

# IL PROCESSO DI AGGIORNAMENTO DEL SERVER WEB MICROSOFT IIS

**Preparazione all'Aggiornamento**

- Backup Completo: creazione di backup completi del server, inclusi tutti i dati, applicazioni e configurazioni, utilizzando strumenti come Windows Server Backup o soluzioni di terze parti, per garantire un ripristino sicuro in caso di fallimento dell'aggiornamento.
- Revisione della Documentazione: studio approfondito della documentazione tecnica dell'aggiornamento per comprendere i requisiti di sistema, le dipendenze e le procedure raccomandate.

**Scelta del Metodo di Aggiornamento**

- Aggiornamento Diretto: adatto per ambienti meno critici dove il tempo di downtime è gestibile.
- Aggiornamento in Ambiente di Test: creazione di un ambiente di test duplicato per verificare l'aggiornamento senza impattare l'ambiente di produzione, ideale per configurazioni complesse o critiche.

**Download dell'Aggiornamento**

- Fonti Affidabili: assicurarsi che l'aggiornamento venga scaricato direttamente dai siti ufficiali di Microsoft o attraverso il Microsoft Update Catalog.
- Verifica dell'Integrità: controllare l'integrità dei file scaricati con checksum o firme digitali per prevenire l'introduzione di software malevolo.

**Installazione dell'Aggiornamento**

- Fermare il Servizio: interrompere il servizio IIS durante l'aggiornamento per evitare corruzioni di dati o interruzioni di servizio.
- Aggiornamento del Software: applicare l'aggiornamento seguendo le procedure documentate, monitorando attentamente il processo per identificare eventuali errori.

# IL PROCESSO DI AGGIORNAMENTO DEL SERVER WEB MICROSOFT IIS

**Verifica Post-Aggiornamento**

- Test di Funzionalità: eseguire test completi per assicurarsi che tutte le funzioni del server operino come previsto.
- Monitoraggio degli Errori: verificare i log di sistema e di applicazione per rilevare anomalie o errori introdotti dall'aggiornamento.
- Test di Sicurezza: conduzione di test di sicurezza per verificare che le vulnerabilità note siano state correttamente mitigate e che non siano state introdotte nuove vulnerabilità.

**Documentazione del Processo**

- Rapporto di Aggiornamento: compilare un rapporto dettagliato che documenti ogni fase dell'aggiornamento, le decisioni prese, e i risultati dei test.
- Revisione delle Policy di Sicurezza: aggiornare le politiche di sicurezza interne per riflettere le nuove configurazioni e le pratiche di sicurezza migliorate.

**Ripristino del Servizio**

- Riavvio del Server: riavviare il server per applicare completamente l'aggiornamento e ripristinare il servizio.
- Conferma del Funzionamento: confermare il pieno funzionamento operativo attraverso monitoraggi e feedback degli utenti finali.

# MICROSOFT IIS: UNA PANORAMICA

## Cos'è Microsoft IIS

Microsoft Internet Information Services (IIS) è un servizio di server web estensibile che supporta HTTP, HTTPS, FTP, FTPS, SMTP e NNTP. È uno dei server web più utilizzati nelle infrastrutture basate su Windows e offre una piattaforma per la distribuzione di applicazioni web e servizi web. IIS è noto per la sua integrazione profonda con il resto dei prodotti Microsoft, offrendo funzionalità robuste per la gestione della configurazione e della sicurezza.

## Funzionalità e Utilizzo di Microsoft IIS

Microsoft IIS è utilizzato principalmente in ambienti aziendali per ospitare siti web, applicazioni web e servizi web. Tra le sue principali funzionalità figurano:

- Gestione centralizzata: IIS fornisce potenti strumenti di gestione che consentono agli amministratori di configurare e gestire molti server da un'unica console.
- Supporto per le applicazioni .NET: IIS è strettamente integrato con l'ambiente .NET Framework, il che facilita l'esecuzione di applicazioni ASP.NET.
- Sicurezza migliorata: con funzionalità come l'autenticazione integrata di Windows e il filtraggio delle richieste.

## Versione Vulnerabile di Microsoft IIS

La versione 8.5 di IIS, che abbiamo identificato come la versione vulnerabile da cui si aggiorna, presenta una serie di vulnerabilità che hanno necessitato di un aggiornamento:

- CVE-2015-1635 (HTTP.sys): una vulnerabilità nel driver HTTP.sys che potrebbe permettere attacchi di tipo denial of service (DoS) attraverso una richiesta HTTP speciale.
- CVE-2017-7269: sfruttamento di una vulnerabilità nel servizio WebDAV che potrebbe consentire l'esecuzione remota di codice se l'attaccante invia una richiesta HTTP o HTTPS manipolata a un server IIS interessato.

# MICROSOFT IIS: UNA PANORAMICA

- Problemi di scalabilità e prestazioni: sotto carico pesante, IIS 8.5 poteva soffrire di problemi di prestazioni che potevano essere mitigati solo parzialmente con ottimizzazioni hardware e software.

Queste vulnerabilità, insieme alle limitazioni di prestazioni, hanno reso imperativo un aggiornamento a versioni più recenti e sicure del server web IIS.

**Aggiornamento a Microsoft IIS 10.0**

Caratteristiche di Microsoft IIS 10.0:
la versione 10.0 di IIS introduce miglioramenti significativi sia in termini di funzionalità che di sicurezza:

- Supporto per HTTP/2: IIS 10.0 aggiunge supporto per il protocollo HTTP/2, che offre una migliore efficienza, minor latenza e miglioramenti nella gestione delle connessioni rispetto a HTTP/1.1.
- Miglioramenti della sicurezza: comprendono nuove funzionalità per limitare l'esposizione a vulnerabilità di sicurezza e per migliorare la gestione delle identità e delle autorizzazioni.

Miglioramenti di Sicurezza in Microsoft IIS 10.0

IIS 10.0 affronta specificamente le vulnerabilità presenti nelle versioni precedenti e migliora la robustezza del server contro attacchi futuri:

- Patch e correzioni: tutte le vulnerabilità note come CVE-2015-1635 e CVE-2017-7269 sono state risolte.
- Miglioramenti alla configurazione di default: configurazioni più sicure di default che aiutano a prevenire abusi e attacchi non appena il server viene installato.

# IDENTIFICAZIONE DELLE CATENE DEL RISCHIO

Nella gestione dei rischi informatici, è essenziale avere una comprensione chiara del flusso di lavoro che caratterizza l'emergere e l'evoluzione di un rischio. Questo processo inizia con l'identificazione di un threat agent, che è una fonte potenziale di minaccia, come una persona o un programma che può sfruttare una vulnerabilità per causare danno. La minaccia stessa è l'evento o l'azione che può causare danni o avere altri impatti negativi.
La vulnerabilità rappresenta una debolezza nel sistema che il threat agent potrebbe sfruttare. Questa può esistere a causa di configurazioni errate, software non aggiornato, mancanza di controlli di sicurezza adeguati, o semplicemente a causa di un errore umano. L'aspetto cruciale è che una vulnerabilità da sola non causa danno fino a quando non viene sfruttata da una minaccia.
L'impact è la conseguenza di un evento di minaccia che sfrutta una vulnerabilità. L'impatto può variare notevolmente, da una lieve interruzione a gravi danni finanziari o perdita di reputazione. L'impatto valuta il danno potenziale che le minacce possono causare se non adeguatamente gestite.
Infine, il risk è una valutazione combinata dell'impatto e della probabilità che una minaccia si verifichi e sfrutti una vulnerabilità. È un concetto fondamentale nella gestione dei rischi, poiché aiuta a determinare quali vulnerabilità richiedono attenzione e risorse per la mitigazione.
Il workflow tipico del rischio aiuta le organizzazioni a identificare e valutare sistematicamente i rischi potenziali, a pianificare interventi per mitigarli e a stabilire una gerarchia di risposta che consenta di affrontare prima i rischi più gravi.

Analizziamo tre catene di rischio principali che potrebbero presentarsi durante l'aggiornamento di IIS alla versione 10.0:

**Catena del Rischio 1: Interruzione del Servizio**

- Threat agent: personale IT interno o processi automatizzati.
- Threat: errori nell'applicazione dell'aggiornamento che causano configurazioni errate o incompatibilità con applicazioni esistenti.

# IDENTIFICAZIONE DELLE CATENE DEL RISCHIO

- Vulnerability: mancanza di conoscenza specifica della nuova versione di IIS o errori nella migrazione delle configurazioni esistenti.
- Impact: interruzioni temporanee o prolungate del servizio, che possono portare a perdita di produttività e danni alla reputazione aziendale.
- Risk: alto, considerando la dipendenza dell'azienda dai servizi web per le operazioni quotidiane.

**Catena del Rischio 2: Compromissione della Sicurezza**

- Threat agent: attaccanti esterni che cercano di sfruttare vulnerabilità non ancora scoperte o non correttamente mitigate.
- Threat: esecuzione di attacchi che sfruttano le vulnerabilità durante la finestra di vulnerabilità prima che l'aggiornamento sia completamente applicato.
- Vulnerability: brevi periodi durante il processo di aggiornamento quando le difese possono essere ridotte o quando il sistema è particolarmente esposto.
- Impact: potenziale perdita di dati sensibili, accesso non autorizzato a informazioni riservate, e compromissione dell'integrità dei dati.
- Risk: medio-alto, dipendente dalla velocità di esecuzione dell'aggiornamento e dall'efficacia delle misure di sicurezza transitorie.

**Catena del Rischio 3: Non Conformità Regolamentare**

- Threat agent: revisioni interne o ispezioni da parte di enti regolatori.
- Threat: non conformità alle normative sulla privacy dei dati o sulla sicurezza informatica a seguito di modifiche non documentate o mal gestite durante l'aggiornamento.
- Vulnerability: mancanza di adeguata documentazione o fallimento nel mantenere l'allineamento con le politiche di conformità durante l'aggiornamento.
- Impact: sanzioni, multe o altre ripercussioni legali e finanziarie.
- Risk: medio, con impatti significativi sulla posizione legale e finanziaria dell'azienda.

# CONCLUSIONI

Questo processo di aggiornamento del server web Microsoft IIS dalla versione 8.5 alla 10.0 è stato condotto seguendo un rigoroso workflow di gestione del rischio.
Il processo ha richiesto un'analisi meticolosa delle vulnerabilità esistenti e delle nuove funzionalità fornite dall'aggiornamento, assicurando che ogni passaggio fosse eseguito con la massima attenzione per minimizzare il downtime e garantire la sicurezza.

## Riepilogo del processo di aggiornamento

Il processo di aggiornamento si è concentrato sulla pianificazione dettagliata e sull'esecuzione controllata. Particolare attenzione è stata dedicata a garantire che tutte le misure preventive, come i backup e i test di sicurezza, fossero in atto prima dell'aggiornamento effettivo. L'implementazione è stata eseguita con precisione, e ogni fase è stata accuratamente documentata per fornire una chiara traccia auditabile.

## Benefici dell’aggiornamento a Microsoft IIS 10.0

Gli aggiornamenti hanno portato significativi miglioramenti di sicurezza, tra cui la correzione delle vulnerabilità note e il rafforzamento delle difese contro potenziali future minacce. Le prestazioni sono state ottimizzate grazie al supporto per HTTP/2, risultando in un servizio più rapido e reattivo. La compatibilità con gli ultimi standard e tecnologie mantiene il server web all'avanguardia, offrendo ai nostri utenti un'esperienza migliore e più sicura.

## Gestione del rischio nel processo di aggiornamento

La gestione del rischio è stata un elemento fondamentale di questo aggiornamento. Le catene di rischio identificate sono state affrontate proattivamente, con misure di mitigazione sviluppate per ciascuna. Questo approccio ha minimizzato gli impatti negativi e ha garantito che l'aggiornamento non interrompesse le operazioni aziendali.

# GRAZIE

MARIA HUAPAYA