Esercizio 22/04/24

Traccia

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

Esempio delle sole attività:

1. Valutarela necessitàdell'aggiornamento

2.Effettuarebackup complete del server web

3.Sceglieremetododi aggiornamento

4.Scaricarel'aggiornamento

5....

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

Introduzione

Questo report delinea un processo semplificato per l'aggiornamento di un server web basato su Microsoft Windows, con particolare attenzione al server IIS 7.5.

Lo scenario in esame prevede che l'azienda per il quale stiamo lavorando deve effettuare l'aggiornamento del proprio server, in questo caso Microsoft windows Server IIS 7.5 e passare ad una versione più recente, la versione IIS 10.

Prima di procedere con l'installazione dell'aggiornamento bisogna tenere in considerazione le best practice e le policy aziendali previste per l'aggiornamento degli Asset.

Le fasi iniziali prima di un aggiornamento prevedono l'analisi del rischio intrinseco degli asset aziendali, questo permette di identificare le vulnerabilità e i rischi possibili per la nostra organizzazione.

Dall'analisi del rischio abbiamo scoperto che il nostro web server presenta una vulnerabilità critica, "CVE-2010-3972", questa consente agli utenti malintenzionati remoti di eseguire codice arbitrario o causare un attacco di tipo Denial of Service (arresto anomalo del daemon) tramite un comando FTP predisposto. Il team di Digital risk Assessment ha deciso quindi, di stipulare una governance che illustra le attività e le procedure necessarie per applicare l'aggiornamento del web server, senza che questo crei situazioni impreviste o danni irreparabili all'infrastruttura.

Il processo è strutturato in diverse attività, ciascuna accompagnata da procedure specifiche per garantire un aggiornamento sicuro ed efficiente del server.

Attività e Procedure

1. **Valutazione della Necessità di Aggiornamento**

Data la vulnerabilità a cui è esposto il web server è necessario aggiornarne il sistema operativo. Un attacco DDoS potrebbe mettere fuori uso il server e di conseguenza i servizi associati ad esso.

Procedura:

- **Monitoraggio delle release di sicurezza di Microsoft e degli aggiornamenti disponibili per il server IIS 7.5.**
  Il team tecnico dovrà tramite i siti ufficiali identificare gli aggiornamenti o le patch idonee a sanare la vulnerabilità.

- **Analisi dei changelog per identificare correzioni di bug critici e vulnerabilità.**
  Il team tecnico dovrà intraprende un analisi dei changelog per fornire una panoramica delle modifiche apportate al sistema nel tempo, consentendo agli sviluppatori e agli stakeholder di comprendere meglio l'evoluzione e lo stato attuale del software.

- **Valutazione dell'impatto potenziale degli aggiornamenti sugli utenti e sui servizi.**
  L'installazione dell'aggiornamento porta a nuove funzionalità del software che non sempre sono uguali a quelle delle versioni precedenti. Bisogna tenere conto di queste possibili modifiche per poter gestire al meglio i cambiamenti post aggiornamento.

2. **Effettuare Backup Completo del Server Web**

Dato che gli asset presentano un elevata quantità di dati critici è necessario effettuare un backup completo del sistema. Questo permette di ripristinare il sistema alle condizioni pre-aggiornamento nel caso si presentino dei problemi durante o dopo l'aggiornamento.

Procedura:

- **Creare una copia di backup completa dei file di configurazione, dei dati del sito e delle impostazioni del server IIS 8.**

  È possibile effettuare il backup off-line o online a seconda delle esigenze di ripristino dell'azienda. Inoltre, la copia di backup dovrà essere convalidata per garantire che il backup corrisponda al file originale.

- **Utilizzare strumenti di backup affidabili e testati per garantire l'integrità dei dati.**

  Gli strumenti scelti per il backup dipendono dalla scelta del backup off-line (cioè su unità di memorizzazione fisiche) o online. È possibile utilizzare la crittografia durante l'archiviazione e il trasporto dei dati.

3. **Scegliere Metodo di Aggiornamento**

È necessario scegliere se effettuare l'aggiornamento in modo manuale o automatizzato. L'esempio considera un server windows, la gestione degli aggiornamenti per gli asset windows può avvenire con l'ausilio di software di gestione come (MECM, Microsoft endpoint configuration manager).

Procedura:

- **Valutare le opzioni di aggiornamento disponibili, come l'installazione di patch di sicurezza tramite Windows Update o manualmente tramite download dai canali ufficiali di Microsoft.**
- **Considerare la compatibilità degli aggiornamenti con la versione corrente di IIS 7.5 e del sistema operativo Windows.**

4. **Scaricare l'Aggiornamento**

Procedura:

- **Accedere al sito web ufficiale di Microsoft o ai suoi canali di distribuzione per scaricare gli aggiornamenti più recenti per IIS 8 e il sistema operativo Windows.**
- **Verificare l'autenticità e l'integrità degli aggiornamenti prima del download.**

5. **Installare l'Aggiornamento**

Per evitare possibili problemi dovuti all'aggiornamento appena installato è una buona prassi optare ad installare l'aggiornamento su una VM (che sia una copia esatta dell'asset da aggiornare) ed aspettare un periodo di staging (di prova) per monitorare le possibili problematiche che l'aggiornamento può causare al sistema e ai servizi annessi.

Procedura:

- Sospendere temporaneamente i servizi web ospitati su IIS 7.5 per evitare interruzioni durante l'installazione degli aggiornamenti.
- Eseguire l'installazione degli aggiornamenti seguendo le istruzioni fornite da Microsoft.
- Verificare che l'installazione sia stata completata con successo e ripristinare i servizi web.

Task 2

Immaginare tre Catene di rischio possibili sullo scenario trattato precedentemente.

Identificazione delle Catene di Rischio

Catena 1: Attacco Esterno

- **Threat Actors:** APT.
- **Threat:** Attacco di hacking.
- **Vulnerability:** Versione obsoleta di IIS 7.5 con vulnerabilità conosciute.
- **Impact:** Interruzione dei servizi web, potenziale perdita di dati sensibili.
- **Risk:** Elevato rischio di compromissione della sicurezza e danni alla riservatezza, all'integrità e alla disponibilità dei dati.

Catena 2: Mancata Valutazione dei Rischi

- **Threat:** Mancata identificazione di patch critiche o vulnerabilità.
- **Vulnerability:** Assenza di un processo strutturato di valutazione degli aggiornamenti.
- **Impact:** Esposizione a rischi di sicurezza non mitigati, possibili attacchi.
- **Risk:** Potenziale esposizione a minacce informatiche e perdita di dati.

Catena 3: Errore nell'Aggiornamento

- **Threat:** Installazione fallita o configurazione errata durante l'aggiornamento.
- **Vulnerability:** Errori umani o mancanza di procedure di backup.
- **Impact:** Interruzione dei servizi, perdita di dati critici.
- **Risk:** Possibili perdite finanziarie e danni alla reputazione dell'azienda.

Conclusioni

L'aggiornamento regolare del server web basato su Microsoft Windows, come IIS 7.5, è fondamentale per garantire la sicurezza e l'affidabilità delle operazioni online.

Identificare e mitigare le catene di rischio associate a questo processo è essenziale per proteggere i dati e garantire la continuità operativa del server. L'Implementazione di procedure e aggiornamenti regolari è cruciale per ridurre al minimo l'esposizione a minacce informatiche e mantenere un ambiente web sicuro e funzionale.