Report pratica S1/L1: Processi e rischi

Sommario

Abstract

Il presente report simula la definizione di un processo di aggiornamento semplificato di un Web Server che stabilisca le procedure da seguire per ogni attività elencata.
Inoltre, nello svolgimento dell'esercitazione si è proceduto ad elencare tre diverse catene del rischio, le quali possono verificarsi durante il processo di aggiornamento.
Nonostante le due esercitazioni possano sembrare separate, entrambe ruotano attorno all'importanza della gestione del rischio, intesa come la probabilità che una minaccia si verifichi e produca effetti dannosi per un'organizzazione.

Traccia

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 completi 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

Introduzione

Per facilitare la comprensione del contenuto del presente report si riportano brevemente concetti tecnici correlati.

Che cos'è un Web Server?

È un software, un programma basato sul modello client/server che utilizza il protocollo di rete HTTP/HTTPS per fornire accesso alle risorse sul web, come file e pagine web, da parte degli utenti (client) che ne facciano richiesta tramite il loro browser.
In particolare, quando un utente digita un URL, il browser invia una richiesta HTTP al server corrispondente per ottenere il contenuto desiderato.
Il server elabora la richiesta e crea una risposta HTTP. Questa risposta contiene l'header HTTP che include informazioni come il codice di stato (ad esempio 200 per "OK", quando il server trova la risorsa richiesta o 404 per "Non trovato", quando il server non trova la risorsa richiesta), i tipi di contenuto, i cookie e altre informazioni. Infine, il server invia la risposta HTTP al client attraverso la connessione di rete. Il client riceve la risposta e interpreta i dati ricevuti, visualizzando la pagina web o eseguendo altre azioni in base al contenuto ricevuto dal server.

Che cos' è il rischio e la sua identificazione?

Nell'ambito della gestione del rischio, le definizioni di rischio sono molteplici e desumibili dalle principali norme di standard internazionali (ISO) ma è possibile definirlo genericamente come la probabilità che si verifichi un evento dannoso e che questo evento abbia impatti negativi sugli asset di un'organizzazioni. Gli impatti negativi che il verificarsi di tali eventi comporta sono tali da rendere fondamentale la gestione del rischio, il cui punto di partenza sta nell'identificazione, ovvero nel processo che consente di individuare e documentare il rischio da affrontare.

Catena del rischio

Quando si parla nel presente report di catena del rischio si intende l'insieme sequenziale di vari elementi che portano alla manifestazione di un rischio. In particolare, si possono individuare i seguenti elementi:

- **Threat agent**: la fonte della minaccia, ovvero l'entità, intesa come persone, società, oggetti etc, che mettono in atto la minaccia.

- **Threat**: la minaccia è un evento potenziale, il cui verificarsi comporterebbe un impatto dannoso per l'organizzazione.

- **Vulnerability**: la vulnerabilità è una debolezza di un sistema o processo che può essere sfruttata (exploitata) per generare il danno.

- **Impact**: l'impatto è inteso come conseguenza negativa per l'organizzazione.

- **Risk**: la possibilità che una minaccia si verifichi e l'impatto che il danno comporterebbe sugli asset della società, calcolando il valore degli asset stessi e tenendo presenti eventuali vulnerabilità e minacce correlate.

Svolgimento

Definizione processo di aggiornamento di un server Web

Di seguito si riportano le linee guida da rispettare nel processo di aggiornamento del web server aziendale al fine di garantire un corretto update della versione del software riducendo al minimo i rischi informatici correlati.

1. Valutazione della necessità dell'aggiornamento

La prima fase del processo consiste nel valutare la necessità dell'aggiornamento del web server attraverso l'esame delle note e delle specifiche sulla versione aggiornata del web server.
In tal modo è possibile identificare correzioni di bug, patch di sicurezza e nuove funzionalità che sono fondamentali per comprendere le conseguenze dell'aggiornamento sull'organizzazione.

L'analisi delle correzioni apportati ai *bug* (errori o difetti del programma) permette di determinare se l'aggiornamento risolve eventuali problemi che potrebbero compromettere la stabilità o le funzionalità del server web.
Le *patch di sicurezza* rilasciate dal vendor del web server per la correzione di vulnerabilità rilevanti sono fondamentali per comprendere quanto sia rilevante il rischio collegato allo sfruttamento di una vulnerabilità della versione attuale del web server da parte di un threat agent.
Infine, ai fini della valutazione in esame, è importante considerare anche l'impatto che l'implementazione di *nuove funzionalità* introdotte nell'aggiornamento potrebbe avere sulle operazioni aziendali in termini di prestazioni, funzionalità o sicurezza.

In sintesi, si deve effettuare una considerazione dei rischi associati alla versione attuale del software rispetto alle minacce esistenti e all'impatto sull'ambiente, sulla sicurezza e sulle esigenze aziendale per determinare se la nuova versione sia o meno utile e necessaria.
In ogni caso si consiglia di effettuare un aggiornamento costante del software, al più considerando di rimandarlo ad un momento successivo qualora il rischio associato alla versione attuale non sia di entità rilevante.

2. Esecuzione back up completo del web server

Ritenuto necessario l'update del web server, è indispensabile eseguire preventivamente un back completo dei contenuti del web server per impedire la perdita o la compromissione di dati, file di configurazione e impostazioni garantendo il ripristino del sistema originario.
È consigliabile avere già approntato una strategia di back adeguata che consideri la frequenza e il tipo di back up necessari utilizzando strumenti adeguati, che siano interni o di terze parti (back up in cloud).

3. Metodo di aggiornamento: approccio bilanciato tra manuale e automatico

L'aggiornamento del web server può avvenire manualmente oppure essere automatizzato di default.
Nel primo caso, sono gli amministratori di sistema ad intervenire direttamente per l'aggiornamento attraverso installazione dei pacchetti di update o aggiornamento di file di configurazione del web server. Il vantaggio di una simile opzione è un controllo maggiore circa l'aggiornamento che è bilanciato dal costo in termini di tempo e risorse umane, queste ultime peraltro suscettibili di errori.
Nel secondo caso, invece, il web server effettua l'aggiornamento di default garantendo maggiore efficienza e una sensibile riduzione del rischio di errori.
In compenso però questo approccio rende complesso valutare la necessità o meno dell'aggiornamento e l'impatto su un server critico come quello in esame.
Prendendo a riferimento un'organizzazione come quella di **ICCREA**, presumibilmente dotata di risorse umane e il cui bacino di dati sensibili è estremamente ampio, ***è consigliabile l'approccio manuale per gli aggiornamenti più delicati e cruciali*.**

4. Download dell'aggiornamento

Per la fase di download è bene accertarsi preventivamente che provenga dal sito ufficiale del vendor del software o utilizzare la repository di pacchetti dedicata.
In tal modo è possibile evitare di scaricare una versione del software dannosa e/o alterata.
Per evitare tale rischio, oltre a verificare la fonte, si deve utilizzare un protocollo di rete crittografato (HTTPS), verificare la presenza di un eventuale firma digitale a conferma dell'autenticità, confrontare

il checksum del file scaricato con quello fornito dal vendor o ispezionare il codice sorgente (qualora gli aggiornamenti siano open source).

5. **Staging**: Installazione dell'aggiornamento in ambiente virtualizzato

Procedere a installare e testare la versione aggiornata del software su un ambiente di lavoro con le stesse caratteristiche di quello aziendale ma che sia separato e isolato.
Infatti, con lo staging si replica il setup del web server impedendone però l'accesso al pubblico e l'influenza sull'ambiente operativo.
In tal modo è possibile una serie completa di test (di funzionalità, integrazione, prestazioni e sicurezza) assicurando l'integrità del server e la continuità dell'erogazione dei servizi ai client.

6. Installazione

Installare l'aggiornamento sul web server assicurandosi di eseguire correttamente le istruzioni fornite dal vendor (soprattutto in caso di approccio manuale).
Una volta completata, è necessario testare che la nuova versione funzioni correttamente e che sia compatibile con il resto dei sistemi aziendali (tale punto dovrà essere considerato preventivamente nella fase di valutazione della necessità dell'aggiornamento e testato in quella di staging).
Questi test possono includere la verifica delle funzionalità principali del server, come la risposta alle richieste HTTP, l'accesso ai siti web ospitati e il funzionamento delle applicazioni.

7. Monitoraggio post-installazione

Infine, è cruciale avviare un monitoraggio attivo, continuo e in tempo reale delle risorse (CPU, memoria, ecc.) e del server web per individuare qualsiasi segno di malfunzionamento o riduzione delle performance.

Identificazione di tre "catene" del rischio in forma qualitativa e descrittiva relativamente al processo di aggiornamento

1. Attacco di Hacker durante il Processo di Aggiornamento

- **Threat agent**: Black Hacker esperto.
- **Threat**: Utilizzo di exploit per attaccare una vulnerabilità nota nella versione attuale del software prima che l'aggiornamento vi ponga rimedio.
- **Vulnerability**: Mancanza di patch di sicurezza nel software.
- **Impact**: Possibile compromissione della sicurezza del server e conseguente accesso non autorizzato ai dati sensibili.
- **Risk**: Rischio elevato di perdita di dati riservati con gravi conseguenze finanziarie e reputazionali per l'organizzazione: potrebbe perdere i propri clienti a causa della diffusione della convinzione

che non sappia garantire la riservatezza dei dati e al contempo subire cause per risarcimento del danno da parte dei clienti o multe onerose da parte del Garante Della Privacy.

2. Disastro Ambientale durante l'Aggiornamento

- **Threat agent**: Maremoto
- **Threat**: Interruzione del processo di aggiornamento a causa di forza maggiore.
- **Vulnerability**: Mancanza di adeguata protezione fisiche contro i disastri ambientali e mancanza di procedure di ripristino in caso di emergenza (In tal caso è presente una vulnerabilità collegata, ovvero l'assenza di back up completi del web server).
- **Impact**: Danneggiamento o distruzione del web server o delle sue componenti durante l'aggiornamento.
- **Risk**: rischio elevato di perdita della disponibilità del servizio derivante dai danni materiali all'infrastruttura aziendale.

3. Errore umano durante l'installazione dell'aggiornamento

- **Threat agent**: Personale tecnico dell'IT
- **Threat**: errore nel procedimento di aggiornamento del software, per esempio relativamente alla configurazione di un pacchetto.
- **Vulnerability**: errore umano, ovvero la disattenzione nell'esecuzione della procedura di installazione.
- **Impact**: malfunzionamento o Interruzione del servizio del web server.
- **Risk**: Possibilità moderata di perdita di disponibilità del servizio e insoddisfazione degli utenti.

Conclusioni

La conduzione di una valutazione dettagliata della necessità dell'aggiornamento, l'esecuzione preventiva di backup dei dati, l'attenta pianificazione del metodo di aggiornamento, la verifica dell'autenticità, lo staging, una corretta installazione e il monitoraggio sono tutte fasi fondamentali per garantire un processo di aggiornamento del web server che sia il più corretto e sicuro possibile. Queste linee guida sono state delineate con l'obiettivo di mitigare i potenziali rischi e proteggere l'integrità del server web, considerando anche le varie minacce identificate durante l'analisi del rischio.
Infatti, l'identificazione delle tre catene del rischio nel contesto dell'aggiornamento sottolinea ulteriormente l'importanza di adottare un approccio metodico e completo per proteggere l'infrastruttura digitale aziendale da una vasta gamma di minacce, inclusi attacchi informatici e disastri ambientali.