INDICE

1. 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 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

2. Riferimenti teorici

Esempio 1: Rischio di accesso non autorizzato a dati sensibili.

Minaccia: Hacker tenta di accedere ai dati sensibili dell'azienda.

Vulnerabilità: Debole password di un account utente con privilegi elevati.

Asset: Database contenente informazioni finanziarie dei clienti.

Danno: Furto di dati sensibili, con possibili conseguenze come danni finanziari, danni alla reputazione e sanzioni da parte delle autorità competenti.

Esempio 2: Rischio di malware che infetta i sistemi informatici aziendali.

Minaccia: Malware inviato tramite email di phishing.

Vulnerabilità: Software obsoleto non aggiornato con le ultime patch di sicurezza.

Asset: Sistema informatico utilizzato per la gestione dei processi aziendali.

Danno: Interruzione dei processi aziendali, perdita di dati e danni finanziari.

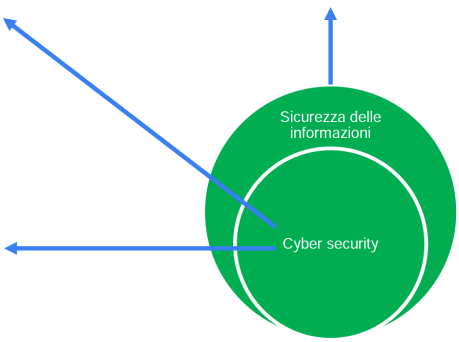
Esempio 3: Rischio di incendio che danneggia il data center.

Minaccia: Incidente elettrico che causa un incendio.

Vulnerabilità: Mancanza di un sistema di antincendio adeguato nel data center.

Asset: Server che contengono dati aziendali critici.

Danno: Perdita di dati aziendali critici, con possibili conseguenze come interruzione dell'attività, danni finanziari e perdita di competitività.



Gestione del rischio (risk management)

- attività coordinate per dirigere e controllare (misurare) un'organizzazione in relazione al rischio. (ISO 31000:2018)
- Uno degli obiettivi della governance. Consiste nel riconoscere il rischio, valutarne l'impatto e la probabilità e sviluppare strategie, come evitare il rischio, ridurne l'effetto negativo e/o trasferirlo, per gestirlo nel contesto della propensione al rischio dell'impresa. (Control Objectives for Information and related Technology - COBIT)

Workflow tipico del rischio

Threat agent
- Entità (persona, organizzazione, oggetto, ecc.) che mette in atto la minaccia.
- Si tiene conto della probabilità che la minaccia si verifichi.

Threat
- Un evento che, se si verificasse, arrecherebbe danno a qualcuno o avrebbe un impatto.
- Una minaccia sfrutta (exploits) una vulnerabilità.
- Va considerata la probabilità che la minaccia riesca a causare un impatto.

Vulnerability
- Una debolezza specifica in un sistema, in un processo o in una persona che potrebbe non riuscire a prevenire una minaccia indesiderata.
- Una vulnerabilità causa un impatto.

Impact
- Conseguenze per un'organizzazione al verificarsi di una minaccia.
- Un impatto produce un rischio.

Risk
- La possibilità e l'impatto di un danno che potrebbe verificarsi a un asset, in base al valore dell'asset stesso e ad eventuali vulnerabilità e minacce correlate.

3. Esecuzione dei task

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

È importante considerare che questo è un processo generico per l'aggiornamento di un server web, per stabilire i passaggi specifici bisognerebbe conoscere la specifica distribuzione e configurazione del server.

1. **Valutare la necessità dell'aggiornamento**
2. **Effettuare backup completo del server web**
3. **Aggiornare il sistema operativo**
4. **Scegliere metodo di aggiornamento (manuale o automatico)**
5. **Testare preventivamente l'aggiornamento, se possibile, su sandbox:** passaggio utile per identificare potenziali problemi, ridurre il rischio di downtime, valutare l'impatto e osservare il processo di aggiornamento.
6. **Scaricare l'aggiornamento**
7. **Istallare l'aggiornamento**
8. **Aggiornare i moduli**
9. **Riavviare il server web**
10. **Verifica post-aggiornamento:** Controllare i log del server, verificare lo stato dei servizi per assicurarsi che le impostazioni di configurazione del server web non siano state modificate accidentalmente durante l'aggiornamento.
11. **Testare il sito web:** Aprire un browser web e navigare sul sito web ospitato dal server per assicurarsi che tutto funzioni correttamente dopo l'aggiornamento.
12. **Monitorare gli accessi e le prestazioni,** se possibile raccogliere feedback dagli utenti.

È molto importante documentare il processo di aggiornamento: Registrare i passaggi eseguiti, i problemi riscontrati e le soluzioni adottate per creare una documentazione di riferimento per futuri aggiornamenti.

Sul processo appena definito, identificare 3 "catene" del rischio in forma qualitativa e descrittiva:

Threat agent → Threat → Vulnerability → Impact → Risk

Catena del Rischio 1: Vulnerabilità del sistema operativo non aggiornato

Threat agent: Attaccanti informatici, hacker o malware
Threat: Uso di vulnerabilità note nel sistema operativo non aggiornato
Vulnerability: Il sistema operativo non ha ricevuto gli aggiornamenti di sicurezza più recenti
Impact: Possibile compromissione della sicurezza, accesso non autorizzato o perdita di dati
Risk: Rischio elevato di violazione della sicurezza se il sistema operativo non viene aggiornato regolarmente.

Catena del Rischio 2: Errore durante l'installazione dell'aggiornamento

Threat agent: Amministratori di sistema o personale incaricato dell'aggiornamento
Threat: Errore durante il processo di installazione dell'aggiornamento
Vulnerability: Mancata comprensione delle istruzioni di installazione o errori tecnici, di distrazione
Impact: Possibile interruzione del servizio o malfunzionamenti del server
Risk: Rischio moderato se l'installazione non viene eseguita correttamente.

Catena del Rischio 3: Problemi post-aggiornamento non rilevati

Threat agent: Amministratori di sistema o utenti finali
Threat: Problemi non rilevati dopo l'aggiornamento
Vulnerability: Mancanza di monitoraggio e di test post-aggiornamento o una scorretta esecuzione di quest'ultimi
Impact: Non rilevare problemi esistenti dopo l'aggiornamento potrebbe comportare rischi per la sicurezza, malfunzionamenti e impatti negativi sulle prestazioni
Risk: Rischio moderato se non vengono eseguiti controlli accurati, documentando ogni passaggio per ridurre al minimo il rischio.

4. Conclusioni

L'aggiornamento di un server web quindi, sebbene necessario per la sicurezza e la stabilità del sistema, può potenzialmente introdurre nuove vulnerabilità o causare malfunzionamenti che potrebbero essere sfruttati da threat actor per scopi dannosi. Di seguito, altri esempi di threat critici che potrebbero verificarsi dopo un aggiornamento:
- **Esecuzione di codice remoto (RCE):** potrebbe portare al furto di dati sensibili, all'installazione di malware o all'utilizzo del server per attacchi informatici verso altri sistemi.
- **Cross-Site Scripting (XSS):** potrebbe portare al furto di informazioni sensibili come credenziali di accesso, cookie di sessione o dati personali degli utenti.
- **Iniezione SQL:** potrebbe causare gravi danni finanziari o reputazionali all'azienda e compromettere la privacy dei clienti.
- **Denial-of-Service (DoS):** potrebbe causare interruzioni del servizio, perdite economiche e danni alla reputazione dell'azienda.
- **Attacco Man-in-the-Middle (MitM):** potrebbe portare alla perdita di informazioni sensibili o al dirottamento degli utenti verso siti web dannosi.

La **perdita di dati** può essere dovuta ad un errore umano durante l'aggiornamento, come la selezione di un pacchetto di aggiornamento errato o l'interruzione del processo di aggiornamento, potrebbe causare la perdita di dati o la corruzione di file importanti. Oppure a difetti nel software di aggiornamento come bug nel software di aggiornamento che potrebbero causare crash del server o danneggiare i dati durante il processo di aggiornamento. Ed infine attacchi informatici con cui l'utente malintenzionato potrebbe sfruttare l'aggiornamento per iniettare malware o virus sul server, causando la perdita o la corruzione di dati.

Nell'**errore umano** rientra la selezione errata del pacchetto di aggiornamento come l'installazione di un pacchetto di aggiornamento non compatibile con il sistema operativo o il software del server web che potrebbe causare malfunzionamenti, perdita di dati o crash del sistema; la mancata configurazione post-aggiornamento potrebbe esporre il sistema a vulnerabilità o causare malfunzionamenti ed infine è molto rischioso non avere un backup completo del server web prima dell'aggiornamento perchè questo potrebbe rendere impossibile il ripristino dei dati in caso di problemi.

Per minimizzare il rischio di threat critici dopo un aggiornamento del server web, è importante seguire le seguenti **best practice**:

- **Effettuare backup completi del server web prima di ogni aggiornamento;**
- **Aggiornare il server web solo da fonti ufficiali e verificate;**
- **Seguire attentamente le istruzioni di aggiornamento e testare accuratamente il server web dopo l'aggiornamento;**
- **Implementare misure di sicurezza come firewall, rilevamento delle intrusioni e sistemi di prevenzione;**
- **Mantenere il software aggiornato con le ultime patch di sicurezza;**
- **Formare gli amministratori del server web sulle migliori pratiche di sicurezza e sui processi di aggiornamento.**

Seguendo queste best practice, è possibile ridurre significativamente il rischio di threat critici dopo un aggiornamento del server web e mantenere la sicurezza e la stabilità del sistema.