BCC ICCREA -
PROGETTO S1/L1
SARA
SPACCIALBELLI

PROCESSI E RISCHI

Traccia:

Definire un processo (semplificato) di aggiornamento di un server web (es. Apache), includendo le procedure per ogni attività.
In seguito, sul processo appena definito, identificare 3 “catene” del rischio in forma qualitativa e descrittiva:
Threat agent → Threat → Vulnerability → Impact → Risk

Processo di Aggiornamento del Server Web (Apache)

1. Valutare la Necessità dell'Aggiornamento

Descrizione: Prima di procedere con l'aggiornamento del server Apache, è importante valutare se è necessario. Questo può essere dovuto a nuove funzionalità o correzioni di sicurezza.

Procedura:

a. Controllare le note di rilascio dell'ultima versione per vedere cosa è cambiato.

b. Verificare se sono state segnalate vulnerabilità di sicurezza nella versione attuale.

c. Consultare le linee guida della sicurezza informatica per determinare se l'aggiornamento è raccomandato.

2. Effettuare Backup Completo del Server Web

Descrizione: Prima di apportare modifiche al server, è fondamentale eseguire un backup completo per evitare la perdita di dati critici in caso di problemi durante l'aggiornamento.

Procedura:

a. Utilizzare uno strumento di backup affidabile per creare una copia di tutti i file di configurazione, dati del sito web e file di registro.

b. Verificare che il backup sia stato completato con successo e che tutti i file necessari siano inclusi.

3. Scegliere il Metodo di Aggiornamento e scaricarlo

Descrizione: scegliere il metodo di aggiornamento e successivamento scaricarlo correttamente

Procedura:

a. Decidere se l'aggiornamento verrà gestito tramite il gestore di pacchetti del sistema operativo (se disponibile) o manualmente.
b. Se si sceglie il gestore di pacchetti, identificare il comando corretto per l'aggiornamento di Apache.
c. Se si sceglie l'aggiornamento manuale, identificare il sito web ufficiale di Apache per scaricare i file dell'aggiornamento.

Considerazioni:

Dopo aver scaricato l'aggiornamento, seguire le istruzioni specifiche fornite nella documentazione di Apache o dalle istruzioni del gestore di pacchetti per completare l'installazione.
Verificare poi, che il server sia funzionante dopo l'aggiornamento e monitorare eventuali errori nei file di registro.

Catena del rischio 1:

Threat agent: black hat
Threat: Attacco di exploit nota vulnerabilità in Apache
Vulnerability: Versione non aggiornata di Apache
Impact: Possibile accesso non autorizzato al server web, compromissione dei dati
Risk: Rischio elevato di violazione dei dati e interruzione dei servizi web

Catena del rischio 2:

Threat agent: fallimento dell’aggiornamento
Threat: Errore durante l'aggiornamento
Vulnerability: Interruzione del servizio durante l'aggiornamento di Apache
Impact: Downtime del server web, inaccessibilità del sito
Risk: Rischio medio di interruzione dei servizi e perdita di disponibilità

Catena del rischio 3:

Threat agent: Dipendente scontento
Threat: Manipolazione dei file di configurazione di Apache, da parte del dipendente, il quale modifica intenzionalmente i file di configurazione per alterare il funzionamento del server.
Vulnerability: Le autorizzazioni di accesso ai file di configurazione non sono state adeguatamente limitate.
Impact: Cambiamenti non autorizzati alla configurazione del server, possibile interruzione dei servizi
Risk: Rischio medio di compromissione dell'integrità dei dati e interruzione dei servizi: Il server potrebbe non essere più affidabile o fornire servizi in modo errato.

GRAZIE

Sara Spaccialbelli