Traccia S1L1

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.Effettuare backup complete del server web

3.Scegliere metodo di aggiornamento

4.Scaricarel'aggiornamento 5.…

Sul processo appenadefinito, identificare3 "catene" del rischio in forma qualitativa e descrittiva: Threat agent → Threat → Vulnerability → Impact → Risk

Soluzione

1. Valutare la necessità dell'aggiornamento: Questo può essere fatto monitorando le notizie sulle ultime versioni e patch di sicurezza rilasciate per Apache. Inoltre, è importante considerare le esigenze specifiche del tuo server, come le nuove funzionalità o i miglioramenti delle prestazioni.
2. Effettuare backup completi del server web: Prima di qualsiasi aggiornamento, è fondamentale effettuare un backup completo del server web. Questo dovrebbe includere tutti i file di configurazione, i dati dell'applicazione e il database.
3. Scegliere metodi di aggiornamento: Ci sono vari metodi per aggiornare Apache, tra cui l'uso di gestori di pacchetti come apt o yum, o la compilazione e l'installazione da sorgente.
4. Scaricare l'aggiornamento: Una volta scelto il metodo di aggiornamento, il passo successivo è scaricare l'aggiornamento dal sito ufficiale di Apache o da un repository affidabile.
5. Installare l'aggiornamento: Dopo aver scaricato l'aggiornamento, il passo successivo è installarlo. Questo processo varierà a seconda del metodo di aggiornamento scelto.
6. Verificare l'aggiornamento: Dopo l'installazione, è importante verificare che l'aggiornamento sia stato installato correttamente e che il server web funzioni come previsto.

Catene del rischio:

1. Minaccia interna accidentale Agente minaccia Dipendente o amministratore del server.

   Minaccia Errore umano durante il processo di aggiornamento o durante la gestione dei backup.

   Vulnerabilità: Mancata comprensione delle procedure di aggiornamento o errori di configurazione

   Impatto:Possibile perdita di dati critici o interruzione del servizio.

Rischio: Medio, poiché gli errori umani sono possibili ma possono essere mitigati con una formazione adeguata e controlli di qualità.

2. Minaccia esterna:

Agente minaccia: Hacker o malintenzionati.

Minaccia: Attacco durante il download dell'aggiornamento o durante l'installazione.

Vulnerabilità: Utilizzo di pacchetti di aggiornamento contraffatti o compromessi.

Impatto: Possibile compromissione della sicurezza del server o della rete.

Rischio: Alto, poiché gli attori esterni possono mirare specificamente alle fasi di aggiornamento per infiltrarsi nei sistemi.

3. Attacco DDoS (Distributed Denial of Service):

Agente minaccia: Gruppo di hacker o botnet.

Minaccia: Attacco DDoS durante il processo di download o installazione dell'aggiornamento.

Vulnerabilità: Dipendenza esclusiva dall'accesso Internet per il download dell'aggiornamento.

ImpattoInterruzione totale o parziale dei servizi web a causa della saturazione delle risorse del server.

Rischio: Medio-alto, poiché gli attacchi DDoS possono essere lanciati in qualsiasi momento e possono compromettere gravemente la disponibilità dei servizi web.