Processi e Rischi

Traccia

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

2 - Sul processo appena definito, identificare 3 “catene” del rischio in forma qualitativa e descrittiva

Traccia 1

1. **Valutare la necessità dell'aggiornamento:**
   Cercare possibili Exploit disponibili sul Web per la versione attuale del Web Server

2. **Fare un Backup del Server:**
   Salvare i dati per un possibile rollback in caso di problemi

3. **Leggere il changelog dell'aggiornamento:**
4. Capire cosa va a modificare esattamente l'aggiornamento

5. **Decidere modalità di aggiornamento:**
   Scegliere fra un aggiornamento automatico o manuale

6. **Installare e testare l'aggiornamento in ambiente di staging:**
   Testare l'aggiornamento su un clone virtuale del Web Server prima di procedere con quello effettivo

7. **Installare l'aggiornamento in ambiente di produzione:**
   Applicare l'aggiornamento nel Web Server finale di produzione

8. **Verificare che l'aggiornamento sia andato a buon fine**:
   Accertarsi che tutte le funzionalità del Web Server siano operative al 100%

Traccia 2

Catena 1 - Criminale Informatico

Threat Agent: Criminale Informatico

Threat: Utilizzo di Exploit per una versione non aggiornata del server

Vulnerability: Versione del Web Server non aggiornata

Impact: Exfiltrazione/modifica di dati da parte del Threat Agent e possibile Pivot nella rete interna

Risk: Alto: l'esistenza di Exploit conosciuti per la versione non aggiornata del Web Server

Catena 2 - Insider Threat

Threat Agent: Dipendente interno all'azienda

Threat: Accesso non autorizzato da parte del dipendente

Vulnerability: Mancanza di un monitoraggio approfondito degli accessi dalla rete interna al Web Server

Impact: Distruzione/modifica dei dati da parte del Threat Agent

Risk: Moderato: Un possibile dipendente scontento con accesso alla rete interna può essere pericoloso quasi quanto un criminale informatico

Catena 3 - APT

Threat Agent: APT (Advanced Persistent Threat)

Threat: Utilizzo di Exploit ad HOC (possibilmente zero days) per il Web Server in questione

Vulnerability: Web Server aggiornato a qualsiasi versione

Impact: Infiltrazione nella rete interna che può protrarsi per lunghi periodi

Risk: Critico: Un APT sponsorizzata da uno stato avversario ha a disposizione risorse quasi illimitate