EPICODE

ESERCIZIO W23D1 EXTRA

HARDENING WINDOWS SERVER 2022

Mungiovì Fabio

TASK

- Descrivere cos'è l'hardening dei sistemi.
- Produrre una checklist di hardening per Windows Server 2022 e per ogni voce descrivere le caratteristiche.

ESECUZIONE

L'hardening dei sistemi, che in italiano potremmo tradurre come "irrobustimento" o "indurimento", rappresenta un insieme di pratiche e tecniche volte a migliorare la sicurezza di un sistema informatico, sia esso un server, un client o un dispositivo di rete.

L'obiettivo principale è quello di ridurre la superficie di attacco, ovvero l'insieme dei punti vulnerabili che un aggressore potrebbe sfruttare per compromettere il sistema. S
i tratta di un approccio proattivo alla sicurezza, che non si limita a reagire agli attacchi, ma cerca di prevenire il più possibile che si verifichino.

L'hardening va oltre la semplice installazione di un antivirus o un firewall. È un processo continuo che coinvolge la configurazione del sistema operativo, delle applicazioni e dei servizi, rendendoli più resistenti a minacce esterne e interne.
Si basa sul principio del "privilegio minimo", ovvero garantire che ogni utente, processo o servizio abbia solo i permessi strettamente necessari per svolgere le proprie funzioni.

Per un sistema come Windows Server 2022, un'attività di hardening si rivela fondamentale.
Di seguito, viene proposta una checklist di hardening che illustra alcune delle principali aree di intervento, descrivendo per ogni voce le caratteristiche e i motivi per cui è importante applicarla.

Checklist di Hardening per Windows Server 2022

- **Aggiornamenti e Patch Management:**
    - **Caratteristiche:** Mantenere il sistema operativo e tutte le applicazioni installate costantemente aggiornate. Questo include l'installazione delle patch di sicurezza rilasciate da Microsoft e dagli sviluppatori di software di terze parti.
    - **Descrizione:** Molti attacchi sfruttano vulnerabilità note per le quali esistono già delle patch correttive. Mantenere il sistema aggiornato è la prima e più semplice difesa. L'automazione di questo processo tramite strumenti come Windows Server Update Services (WSUS) può garantire che nessun aggiornamento venga trascurato.
- **Rimozione di Servizi e Ruoli Non Necessari:**
    - **Caratteristiche:** Disattivare o disinstallare tutti i servizi, ruoli, e funzionalità che non sono indispensabili per le attività del server.
    - **Descrizione:** Ogni servizio in esecuzione, ogni ruolo installato, rappresenta un potenziale punto di ingresso per un malintenzionato. Ridurre il numero di servizi attivi minimizza la superficie di attacco e riduce il rischio di vulnerabilità associate a software che non vengono utilizzati.
- **Configurazione del Firewall:**
    - **Caratteristiche:** Configurare Windows Defender Firewall con sicurezza avanzata per bloccare tutto il traffico in entrata per impostazione predefinita, permettendo solo le connessioni strettamente necessarie.
    - **Descrizione:** Il firewall agisce come un guardiano, controllando il traffico di rete. Un approccio di tipo "deny by default" (neghiamo tutto per impostazione predefinita) garantisce che solo i servizi esposti intenzionalmente (ad esempio, RDP, HTTP/HTTPS) possano ricevere connessioni dall'esterno, impedendo attacchi su porte e servizi non autorizzati.

- **Politiche di Account e Password:**
    - **Caratteristiche:** Implementare politiche di password complesse, che richiedano una lunghezza minima, la combinazione di caratteri speciali, numeri e lettere maiuscole e minuscole. È inoltre consigliabile bloccare gli account dopo un certo numero di tentativi di accesso falliti.
    - **Descrizione:** Le password deboli sono uno dei modi più comuni per compromettere un sistema. Una politica di password robusta e l'applicazione di un meccanismo di blocco degli account ostacolano attacchi a forza bruta e di tipo "password guessing".
- **Controllo degli Accessi e Privilegi Minimi:**
    - **Caratteristiche:** Adottare il principio del privilegio minimo, assegnando agli utenti e ai servizi solo i permessi strettamente necessari per svolgere il proprio lavoro.
    - **Descrizione:** Garantire che un utente o un'applicazione non disponga di privilegi amministrativi se non è strettamente necessario riduce notevolmente il potenziale danno in caso di compromissione. Ad esempio, è preferibile utilizzare account utente standard per le attività quotidiane e ricorrere all'amministratore solo quando si effettuano modifiche di sistema.
- **Disabilitazione di Protocolli e Funzionalità Legacy:**
    - **Caratteristiche:** Disattivare protocolli di rete obsoleti o insicuri, come SMBv1 e TLS 1.0/1.1.
    - **Descrizione:** I protocolli più vecchi spesso contengono vulnerabilità note che i protocolli più moderni hanno risolto. Disabilitarli previene attacchi che sfruttano queste debolezze e allinea il sistema agli standard di sicurezza attuali.
- **Configurazione di Sicurezza del Sistema Operativo:**
    - **Caratteristiche:** Modificare le impostazioni del sistema operativo per rafforzarne la sicurezza. Questo include la configurazione di Group Policy, la disabilitazione di NTLM, l'attivazione di Credential Guard e l'impostazione di un audit di sicurezza.
    - **Descrizione:** Windows offre una vasta gamma di impostazioni di sicurezza che, se configurate correttamente, possono proteggere il sistema da molte minacce. Ad esempio, Credential Guard protegge le credenziali di accesso, mentre un audit dettagliato permette di tracciare le attività sospette.
- **Crittografia e Protezione dei Dati:**
    - **Caratteristiche:** Utilizzare strumenti come BitLocker per crittografare l'intero disco di sistema e proteggere i dati sensibili.
    - **Descrizione:** La crittografia dei dati garantisce che, anche in caso di accesso fisico non autorizzato al server, i dati rimangano illeggibili e inutilizzabili.
- **Monitoraggio e Logging:**
    - **Caratteristiche:** Configurare il sistema per registrare eventi di sicurezza importanti (ad esempio, tentativi di accesso falliti, modifiche ai permessi) e monitorare regolarmente questi log.
    - **Descrizione:** Un sistema di logging e monitoraggio efficace è cruciale per la rilevazione precoce di un'intrusione. L'analisi dei log può aiutare a identificare attività sospette, a capire come si è verificato un attacco e a prevenire future violazioni.
- **Sicurezza dei Servizi e delle Applicazioni:**
    - **Caratteristiche:** Configurare ogni applicazione e servizio installato (come IIS, SQL Server) secondo le migliori pratiche di sicurezza fornite dai rispettivi fornitori.
    - **Descrizione:** Ogni applicazione ha le proprie specifiche vulnerabilità e impostazioni di sicurezza. È fondamentale non lasciare le configurazioni di default e personalizzare ogni servizio per minimizzare il rischio di attacchi mirati.