Report Windows Server 2022 W23D1

Pratica extra

Hardening dei sistemi

L’hardening dei sistemi è un insieme di pratiche, configurazioni ed accorgimenti volti a ridurre la vulnerabilità di un sistema informatico. È un processo che ha lo scopo di rafforzare la sicurezza di un sistema e renderlo meno esposto a potenziali minacce, interne ed esterne.

Hardening Windows Server 2022

- **Update regolari**: È importante mantenere il sistema aggiornato con le ultime patch distribuite in modo da evitare falle nella sicurezza dovute ad un sistema obsoleto.
- **Account utenti sicuri**: Mantenere delle policy sicure per gli account degli utenti è fondamentale per un ambiente di lavoro sicuro, questo comprende vari accorgimenti tra cui ad esempio cambiare il nome dell’account Administrator, disattivare prontamente account non più utilizzati e usare policy di privilegio minimo per gli utenti.
- **Configurazione ruoli**: Rimuovere funzioni e ruoli non necessari per lo scopo del server.
- **Configurazione app e servizi**: Minimizzare le applicazioni ed i servizi installati in modo che non ci sia niente di superfluo.
- **Configurazione di rete**: La configurazione corretta della rete impatta di molto la sicurezza generale, isolare correttamente le macchine da reti non affidabili, applicare restrizioni e sistemi di filtraggio per gli IP in modo da controlare quali IP possono comunicare con il server.
- **Configurazione Firewall**: Un firewall ben configurato con regole ben pensate è essenziale per la protezione dei sistemi.
- **Configurazione NTP**: NTP offre un sistema di timestamps che aiuta nell’organizzazione degli eventi e protegge contro attacchi di time-spoofing e replay.
- **Criptazione**: Abilitare BitLocker per il disco del sistema.
- **Amministrare gli accessi**: L’amministrazione degli accessi è fondamentale per la sicurezza del sistema, controlla chi può accedere a quali risorse e quale livello di permessi è assegnato ad ogni utente.
- **Configurazione accesso da remoto**: RDP è un target comunemente preso di mira dagli hacker, dovrebbe quindi essere abilitato solo se necessario, nel qual caso la criptazione della connessione dovrebbe essere settata su high e si dovrebbe fare uso di MFA se possible.