Esercitazione W17D1 - Pratica 2

Remediation WinXP MS08-067

Fabio Benevento - 28/02/2024

Traccia

Sulla base di quanto visto nell'esercizio pratico di ieri, formulare delle ipotesi di remediation.
Ad esempio:
1. L'attacco colpisce Windows XP, possiamo risolvere in qualche modo? Se si, con quale effort?
2. L'attacco colpisce una particolare vulnerabilità, possiamo risolvere solo la vulnerabilità?
3. Una volta dentro l'attaccante, può accedere a webcam e/o tastiera, possiamo risolvere queste problematiche?

Implementazione

Di seguito sono riportate una serie di possibili remediation per la vulnerabilità MS08-067:

- Aggiornamento a una versione più recente di Windows:
  L'opzione più consigliata è l'aggiornamento del sistema operativo a una versione più recente di Windows, che riceva ancora il supporto di Microsoft. Questo ridurrà significativamente il rischio di sfruttamento di vulnerabilità note

- Isolamento del sistema:

  Isolare i sistemi Windows XP dalla rete principale può ridurre il rischio di essere compromessi. Tuttavia, questa non è una soluzione completa e può limitare la funzionalità del sistema.

- Implementazione di controlli di sicurezza aggiuntivi:

  Utilizzare soluzioni di sicurezza aggiuntive, come firewall, antivirus avanzati e sistemi di rilevamento delle intrusioni (IDS), per mitigare i rischi di attacchi.

- Monitoraggio costante:

  Implementare un sistema di monitoraggio costante per rilevare attività sospette e rispondere prontamente a eventuali intrusioni.

- Backup regolari:

  Eseguire backup regolari dei dati critici e assicurarsi che siano archiviati in un luogo sicuro. Questo consentirà un rapido ripristino in caso di compromissione.

- Consapevolezza degli utenti:

  Fornire formazione sulla sicurezza informatica agli utenti per aumentare la consapevolezza sui rischi e promuovere pratiche di sicurezza, come evitare clic su link sospetti o scaricare file da fonti non attendibili.

- Politiche di sicurezza rigorose:

  Implementare politiche di sicurezza rigorose, comprese l'autenticazione a due fattori e la crittografia dei dati, per aumentare la sicurezza del sistema.