W17D3

HACKING WINDOWS XP

La 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?

Buon divertimento

Remediation vulnerabilità windows Xp

La vulnerabilità ad oggetto è il 'Server service'.

Per rimediare a tale situazione possiamo attivare l'aggiornamento automatico o manuale dell'OS, altrimenti dal catalogo di Microsoft scarico manualmente la patch 'KB4012598'.

Per quanto riguarda l'effort dipende dal contesto in cui viene lanciato l'attacco.
Se si tratta di un numero esiguo di pc può aver senso applicare la patch o l'aggiornamento su ogni pc, ma se la dimensione dell'organizzazione è alta la situazione potrebbe cambiare.
L'installazione della patch va fatta secondo un certo metodo e tenendo conto di produzione, compatibilità e dipendenze.
Per esempio può succedere che la patch non fa funzionare bene un sistema o un programma di quel sistema per cui si può fare prima un test, quindi senza fare cambiamenti in produzione (a meno che l'urgenza e la criticità siano alte).
Nel primo caso parleremo di un problema, nel secondo si tratterà di un incidente.

Remediation vulnerabilità windows Xp

Nel caso si tratti di un problema posso fare un test.
Se ho tutto su un S1, predispongo una macchina S2 uguale, testo e vedo se il servizio va bene lo stesso e switcho il servizio su S2, risolvo il problema sulla S1 e vedo se switchare nuovamente su S2 o bilanciare sui 2 sistemi.
Se si tratta di un incidente: il servizio non è disponibile e risolvo in produzione, mantengo sicurezza a scapito della disponibilità del servizio.
Nel caso del problema invece mantengo la disponibilità del servizio a scapito della sicurezza.
Prima di decidere se è un incidente o un problema si fa una Risk Analysis, in base al rischio vedrò se configurare la situazione come un problema o un incidente.

Remediation vulnerabilità windows Xp

Cosa succede a livello di endpoint?
Si pensi anche a dispositivi personali usati nella rete aziendale, a quel punto dovremmo contemplare l'ipotesi di utilizzare un IDS.

Oltre ad installare un antivirus sugli endpoint aziendali possiamo vedere qualche soluzione a livello enterprise come EDR o XDR.

Un membro del SOC controlla gli endpoint tramite l'agent che controlla l'accesso a periferiche e programmi, vede tentativi di accesso (traffico malevolo), controlla processi (ogni processo ha una firma ma se qualcuno lo manipola l'agent lo rileva).