5 modi per rendere il Mainframe “hackerabile”



È incredibile come ancora oggi le più grandi organizzazioni, spaventate dai continui attacchi informatici come ad esempio il Ransomware, stiano ragionando sull’aggiornamento evolutivo di sicurezza della propria infrastruttura IT, senza includere nel perimetro di valutazione la sicurezza del Mainframe, dove molto probabilmente risiedono i dati più preziosi.

Ed è ancora più impressionante notare come le stesse organizzazioni ignorino completamente l’incomparabile qualità di sicurezza offerta dalla piattaforma Z, ricorrendo spesso ad una serie di valutazioni di “replatforming”, tipicamente cloud, con la pura illusione della riduzione dei costi, che andrebbe misurata sul medio-lungo termine, ma soprattutto senza considerare il concreto aumento dei livelli di rischio a cui ci si espone tralasciando la struttura mainframe-centrica e concentrandosi esclusivamente ad una più distribuita.

E allora, seguendo questa tendenza, ecco cinque punti fondamentali su cui possiamo agire per facilitare maggiormente l’opera dell’insider di turno, rendendo più facile l’hacking sul proprio mainframe:

1) **Continuiamo ad utilizzare la Basic-Authentication**, senza considerare la possibilità di adottare una più moderna ed efficace autenticazione a più fattori (zMFA)che la stessa piattaforma Z mette a disposizione. Questo perché risulterebbe fastidioso cambiare i propri processi di autenticazione andando ad impattare con le abitudini degli utenti oramai consolidate da tempo. Utilizzando l’autenticazione di base non facciamo altro che aiutare gli hacker a catturare le credenziali degli utenti e ad agire indisturbati nel sistema,

specialmente se la password utilizzata risulta di scarsa qualità. L'hacker può essere certo di confidare sulla negligenza dell'utente e attendere il momento propizio per acquisire e utilizzare le credenziali rubate aggirando completamente ogni sistema di sicurezza messo in atto.

2) **Non eseguiamo mai un assessment di sicurezza**! La conoscenza delle lacune nella sicurezza porta a preoccupazioni inutili che non consentono di svolgere il proprio lavoro in tranquillità. Meglio non conoscere i possibili pericoli e alimentare un giusto senso di incoscienza, lasciando la polvere sotto il tappeto, che tanto ne passa di tempo prima che possa essere scoperta.

3) **Non attiviamo alcun monitoraggio e/o alerting in tempo reale**. Sul mainframe non serve! Perché già si registrano e si raccolgono moltissime informazioni di quanto accade sul sistema, sufficienti per andare con calma serafica ad effettuare le opportune indagini. Se attiviamo sia il monitoraggio che gli allarmi di sicurezza si è poi obbligati ad essere reperibili e reattivi a fronte di continue segnalazioni relative alle anomalie riscontrate. Meglio aspettare e quando succede qualcosa, se dovesse mai succedere, allora andremo a scoprire cosa è successo.

4) **Assegniamo più privilegi allo stesso utente**, in particolare se ha compiti amministrativi. In questo modo si riducono le persone e le risorse necessarie per gestire e amministrare l'intero sistema. Una separazione dei compiti produce inutili complicazioni nelle attività ordinaria, creando ostacoli e vincoli che interrompono il workflow operativo.

5) **Non applichiamo alcun tipo di crittografia ai dati**. In questo modo è più facile utilizzare tecniche diverse per sniffare importanti dati che viaggiano sulla rete senza il rischio di essere scoperto. Inoltre, utilizzando credenziali improprie posso facilmente intraprendere una escalation di privilegi per poter installare codice malevolo (backdoor)

utile poi nell’agevolare un’esfiltrazione di dati sensibili che risultano in chiaro, perché opportunamente non coperti da crittografia.

Molto bene! Fatto questo possiamo stare tranquilli che il nostro Mainframe continua a funzionare senza alcun problema, non avendo fatto mai modiche impattanti sul sistema ed avendo evitato possibili rallentamenti ed interruzioni dei servizi, in un contesto in cui la sicurezza è demandata a componenti esterne perimetrali di cui non si è diretti responsabili. Solo così possiamo essere sicuri di diventare in breve tempo buoni amici degli hacker!

Articolo a cura di **Luigi Perrone**

https://www.ictsecuritymagazine.com/articoli/5-modi-per-rendere-il-mainframe-hackerabile/