Tema 6 – MITM

Un atac Man in the middle este o forma de atac cibernetic in care un atacator se pleaseaza intre doua parti care comunica pentru a intercepta, modifica si redirectiona comunicatia dintre acestea fara ca ele sa fie constiente de prezenta sa. Atacatorul actioneaza ca un intermediar avand acces la datele transmise. Exemple de astfel de metode sunt ARP spoofing, phising wi-fi sau interceptare https.

Schema de raspuns a unui atac MITM

1. Identificarea atacului: verificarea logurilor si descoperirea comportamentelor neobisnuite din retea precum intreruperi de conexiuni, timp mari de raspuns sau certificate suspicioase.

2. Izolarea incidentului: deconectarea echipamentelor sau sistemului compromis de la network-ul companiei, inchiderea conexiunilor suspecte din retea si limitarea accesului la resurse.

3. Evaluarea impactului: analiza datelor interceptate, verificarea IOC, verificarea daca utilizatorii au fost afectati si in ce masura

4. Remedierea incidentului: Restabilire certificate SSL/TLS si verificare infrastructura PKI, schimbarea parolelor utilizatorilor afectati.

5. Actiuni post-incident, documentare si raportare: documentare tuturor evenimentelor relevante legate de atac si raportarea incidentului catre echipele relevante, management, stakeholderi, actualizarea procedurilor de securitate pentru a preveni incidente similare.

Pentru un plan de actiune impotriva unui atac MITM, putem folosi framework-ul pentru raspunsul la incidente de la NIST format din cinci pasi Identificare, Protejare, Detectare, Raspuns, Recuperare:

1. Identificare: Evaluarea infrastructurii retelei, identificarea resurselor critice si fluxuri de date sensibile. Identificarea amenintarilor si scanare de vulnerabilitati care ar putea facilita un atac MITM cum ar fi retele nesecurizate sau lipsa certificatelor SSL/TLS.

2. Protejare: Implementarea SSL/TLS, activarea autentificarii multifactor pentru accesul in retea si aplicatii. Segmentarea network-ului pentru a izola datele critice.

3. Detectare: Utilizarea instrumentelor de monitorizare a retelei printr-un IDS/IPS sau next generation firewal si implementarea unui SIEM. Configurarea tool-urilor specificate pentru a detecta semnaturi tipice de atac MITM cum ar fi certificate falsificate sau redirectionarea traficului.

4. Raspuns: Izolarea incidentului prin intreruperea conexiunilor suspecte si izolarea dispozitivelor afectate. Investigarea incidentului prin logurile afisate in SIEM pentru a ddetermina amploarea atacului. Schimbarea credentialelor userilor afectati si actualizarea certificatelor afectate.

5. Recuperare: Restabilirea serviciilor si aplicatilor afectate dupa ce au fost rezolvate vulnerabilitatile. Revizuirea si actualizarea politicilor de securitate dupa evaluarea incidentului. Documentarea incident si masurile de raspuns aferente pentru viitoare atacuri si intruirea userilor.