Man-in-the-Middle (MitM) útok

Last updated March 17, 2025

Man-in-the-Middle (MitM) je forma kybernetického útoku, pri ktorom útočník tajne zachytáva a niekedy aj upravuje dáta posielané v sieti bez toho, aby o tom používatelia vedeli.

Najčastejšie sa tak kradnú prihlasovacie, platobné údaje a heslá na nezabezpečených webových stránkach alebo verejnej WiFi. Rovnako sa tak MitM používa na šírenie škodlivého kódu (malvéru).

Ako k MitM dochádza?

Najväčšie riziko MitM hrozí v prípade, že kliknite na nebezpečný odkaz v phishingovom e-maile alebo sa prihlásite na verejnú, nechránenú WiFi (napríklad v kaviarňach, knižniciach alebo na letiskách).

Priebeh je vždy podobný:

1. Útočník vytvorí kópiu cieľovej stránky alebo WiFi.
2. Nič netušiaci používateľ na nej uskutoční nejakú akciu (zadá svoje prihlasovacie údaje, nakúpi produkt).
3. Útočník citlivé údaje zachytí a môže ich zneužiť na pravých stránkach, aby sa dostal do účtov.

Ako sa pred MitM brániť?

Najúčinnejšia obrana proti MitM je použitie šifrovaného prenosu dát.

- V prípade webov je najjednoduchšie použiť SSL certifikát. Z pohľadu návštevníka je teda dobré si vždy overiť, že webové stránky používajú HTTPS protokol (Google vás na jeho neprítomnosť automaticky upozorňuje).
- Na verejnej WiFi odporúčame použiť šifrovanie a maskovanie vašej IP adresy pomocou VPN.

Je však dôležité vedieť, že táto ochrana nie je 100 %. Pokrýva však 2 zďaleka najbežnejšie metódy MitM.

Metódy Man-in-the-Middle útokov

Man-in-the-Middle útoky môžu byť uskutočnené rôznymi metódami, pričom niektoré sú častejšie alebo efektívnejšie v určitých kontextoch. Najčastejšie MitM sú:

1. **DNS Spoofing**: útočník zmení DNS záznamy a presmeruje používateľov na podvodnú webovú stránku, ktorá na prvý pohľad vyzerá ako legitímny.
2. **Interceptácia Wi-Fi**: útočník vytvorí falošný prístupový bod Wi-Fi, ku ktorému sa používatelia pripoja alebo odpočúva komunikáciu v nezabezpečenej sieti.
3. **ARP Spoofing**: Táto metóda spočíva v zneužití protokolu Address Resolution Protocol (ARP), ktorý sa používa v lokálnych sieťach na zistenie fyzickej (MAC) adresy (ekvivalent IP adresy). Útočník odosiela falošné ARP správy do siete, čím presmeruje sieťovú prevádzku na svoje zariadenia.
4. **SSL Stripping**: Pri SSL strippingu útočník nútene znižuje úroveň zabezpečenia spojení z HTTPS (šifrovaného) na HTTP (nešifrované), čo umožňuje odpočúvanie a manipuláciu s dátami.
5. **Hijacking relácií**: Útočník zachytí a využije platné relačné tokeny alebo cookies na prevzatie existujúcich používateľských relácií, napríklad na webových stránkach.
6. **E-mail Hijacking**: Útočník zachytí alebo presmeruje e-mailovú komunikáciu, čo mu umožní získavať informácie alebo uskutočňovať ďalšie podvodné aktivity.