MitM (Man-in-the-Middle Attack)

MitM je útok na principu odposlechu a manipulace. Útočník se vloží do komunikačního řetězce mezi klienta (např. váš prohlížeč) a server (např. internetové bankovnictví). Úspěšný MitM útok umožňuje útočníkovi číst zprávy v reálném čase, krást přihlašovací údaje, instalovat malware nebo podvrhnout falešné informace, aniž by o tom obě strany věděly.

Jak MitM útok funguje

Představte si, že posíláte dopis příteli, ale pošťák ho cestou otevře, přečte, přepíše jeho obsah a pak ho znovu zalepí a doručí. Přítel si myslí, že dopis je od vás, a vy si myslíte, že ho dostal v pořádku.

V digitálním světě se to děje ve dvou fázích:

```
1. **Intercepce (Zachycení):** Útočník přesměruje síťový provoz přes své zařízení. Často k tomu využívá veřejné Wi-Fi sítě nebo chyby v síťových protokolech.
2. **Dekrypce (Rozšifrování):** Pokud je provoz šifrovaný (např. přes [[https|HTTPS]]), útočník se pokusí oklamat prohlížeč oběti, aby přijal falešný certifikát, nebo využije zastaralé verze protokolů k prolomení šifry.
```

Nejčastější techniky MitM

Technika	Popis
Rogue Wi-Fi Access Point	Útočník vytvoří Wi-Fi síť se známým názvem (např. „Free_Starbucks_WiFi“). Jakmile se uživatel připojí, veškerý jeho provoz teče přes útočníkův notebook.
ARP Spoofing	Útočník v místní síti (LAN) oklame ostatní zařízení, aby si myslela, že jeho počítač je výchozí brána (router).
DNS Spoofing	Útočník podvrhne záznamy v DNS. Když zadáte „mojebanka.cz“, prohlížeč vás ve skutečnosti nasměruje na IP adresu útočníkova falešného webu.
Session Hijacking	Útočník ukradne vaši aktivní relaci (přihlášení) pomocí zachycení cookies, čímž získá přístup k vašemu účtu bez znalosti hesla.

MitM a šifrování

Hlavním nepřítelem MitM útoků je silné šifrování.

- **HSTS (HTTP Strict Transport Security):** Mechanismus, který prohlížeči přikazuje

komunikovat s daným webem výhradně přes HTTPS. Brání tak útočníkovi v pokusu o downgrade (přepnutí na nezabezpečené HTTP).
- **Certificate Pinning:** Aplikace (např. mobilní bankovnictví) má v sobě napevno uložen certifikát serveru. Pokud se útočník pokusí podvrhnout svůj certifikát, aplikace spojení odmítne.

Jak se bránit?

- **Nepoužívejte neznámé Wi-Fi sítě:** Pro citlivé operace (bankovnictví, e-maily) vždy preferujte mobilní data nebo důvěryhodnou domácí síť.
- **Sledujte varování prohlížeče:** Pokud prohlížeč nahlásí „Problém s certifikátem“ nebo „Spojení není soukromé“, stránku okamžitě opusťte.
- **Používejte VPN:** Virtuální privátní síť vytvoří šifrovaný tunel, kterým data proudí bezpečně i přes napadenou síť.
- **Dvoufaktorové ověření (2FA):** I když útočník díky MitM získá vaše heslo, bez druhého faktoru (SMS, kód v aplikaci) se do účtu nedostane.

Související pojmy: HTTPS, Šifrování, DNS, Cookie, Firewall, VPN, Malware, Certifikát.

From:
https://serviceit.cz/ - **IT ENCYKLOPEDIE**

Permanent link:
https://serviceit.cz/doku.php?id=mitm

Last update: **2025/12/31 19:35**