Man-in-the-Middle (MITM)

Man-in-the-Middle je útok na důvěrnost a integritu dat. Útočník se v digitálním světě chová jako falešný pošťák, který otevírá vaše dopisy, čte je, případně přepíše jejich obsah a pak je zalepí a doručí adresátovi. Obě strany se domnívají, že mluví přímo spolu, ale ve skutečnosti komunikují s útočníkem.

Jak útok probíhá

Útok MITM se obvykle skládá ze dvou fází:

```
1. **Intercepce (Zachycení):** Útočník přesměruje síťový provoz oběti přes své vlastní zařízení. Toho lze dosáhnout například vytvořením falešné Wi-Fi sítě nebo technikou zvanou **ARP Spoofing**.
2. **Dešifrování (Decryption):** Pokud je provoz šifrovaný (např. [[https|HTTPS]]), útočník se pokusí vynutit slabší šifrování nebo podvrhnout vlastní certifikát, aby mohl data číst a upravovat.
```

Běžné techniky útoku

Technika	Popis
Rogue Access Point	Útočník vytvoří Wi-Fi se stejným jménem jako kavárna. Uživatelé se k ní připojí a veškerá data tečou přes útočníka.
ARP Spoofing	Útočník pošle v lokální síti falešné zprávy, které přesvědčí váš počítač, že útočníkův počítač je router (brána do internetu).
DNS Spoofing	Útočník „otráví“ záznamy DNS, takže když napíšete `facebook.com`, prohlížeč vás pošle na falešnou IP adresu útočníka.
SSL Stripping	Útočník přinutí prohlížeč komunikovat přes nezabezpečené HTTP místo šifrovaného HTTPS.

Příklady zneužití

- **Krádež identit:** Získání přihlašovacích údajů k e-mailům, sociálním sítím nebo bankovnictví.
- **Modifikace dat:** Útočník může v rozpracovaném bankovním převodu změnit číslo účtu příjemce na své vlastní.
- **Sledování (Eavesdropping):** Odposlech soukromých konverzací a firemních tajemství.

Jak se bránit?

Obrana proti MITM vyžaduje kombinaci technických opatření a obezřetnosti uživatele:

```
1. **Využívání [[ssl_tls|SSL/TLS]]:** Vždy kontrolujte, zda web běží na
**HTTPS** a má platný certifikát (ikona zámku).
2. **[[certificate_pinning|Certificate Pinning]]:** Mobilní aplikace mohou
mít "připnutý" konkrétní certifikát, takže útočníkův falešný certifikát
okamžitě poznají a spojení ukončí.
3. **VPN (Virtual Private Network):** Vytváří bezpečný šifrovaný tunel,
který je pro útočníka v lokální síti prakticky neproniknutelný.
4. **Dvoufázové ověření (2FA):** I když útočník získá vaše heslo, bez
druhého faktoru (např. kódu v mobilu) se k účtu nedostane.
5. **Veřejné sítě:** Vyhněte se provádění citlivých operací (bankovnictví)
na nezabezpečených veřejných Wi-Fi sítích.
```

Související pojmy: SSL/TLS, HTTPS, VPN, Certificate Pinning, ARP Spoofing, DNS, Šifrování, 2FA.