Co je Man-in-the-Middle (MitM) útok

Poslední aktualizace 15 listopadu, 2024

Man-in-the-Middle (MitM) je forma kybernetického útoku, při němž útočník tajně zachytává a někdy i upravuje data posílaná v síti, aniž by o tom uživatelé věděli.

Nejčastěji se tak kradou přihlašovací a platební údaje a hesla na nezabezpečených webových stránkách nebo veřejné WiFi. Stejně tak se MitM používá k šíření škodlivého kódu (malware).

Jak k MitM dochází?

Největší riziko MitM hrozí v případě, že kliknete na nebezpečný odkaz ve phishingovém e-mailu nebo se přihlásíte k veřejné, nechráněné WiFi (například v kavárnách, letištích nebo knihovnách).

Průběh je vždy podobný:

1. Útočník vytvoří kopii cílové stránky nebo WiFi.
2. Nic netušící uživatel na ní provede nějakou akci (zadá své přihlašovací údaje, nakoupí produkt).
3. Útočník citlivé údaje zachytí a může je zneužít na pravých stránkách, aby se dostal do účtů.

Jak se proti MitM bránit?

Nejúčinnější obrana proti MitM je použití šifrovaného přenosu dat.

- V případě webů je nejjednodušší použít SSL certifikát. Z pohledu návštěvníka je tedy dobré si vždy ověřit, že webové stránky používají HTTPS protokol (Google vás na jeho nepřítomnost automaticky upozorňuje).
- Na veřejné WiFi doporučujeme použít šifrování a maskování vaší IP adresy pomocí VPN.

Je však důležité vědět, že tato ochrana není 100%. Pokrývá však 2 zdaleka nejběžnější metody MitM.

Metody Man-in-the-Middle útoků

Man-in-the-Middle útoky mohou být provedeny různými metodami, přičemž některé jsou častější nebo efektivnější v určitých kontextech. Nejčastější MitM jsou:

1. **DNS Spoofing**: útočník změní DNS záznamy a přesměruje uživatele na podvodnou webovou stránku, která na první pohled vypadá jako legitimní.
2. **Interceptace Wi-Fi**: útočník vytvoří falešný přístupový bod Wi-Fi, ke kterému se uživatelé připojí, nebo odposlouchává komunikaci v nezabezpečené síti.
3. **ARP Spoofing**: Tato metoda spočívá v zneužití protokolu Address Resolution Protocol (ARP), který se používá v lokálních sítích k zjištění fyzické (MAC) adresy (ekvivalent IP adresy). Útočník odesílá falešné ARP zprávy do sítě, čímž přesměruje síťový provoz na své zařízení.
4. **SSL Stripping**: Při SSL strippingu útočník nuceně snižuje úroveň zabezpečení spojení z HTTPS (šifrovaného) na HTTP (nešifrované), což umožňuje odposlech a manipulaci s daty.
5. **Hijacking relací**: Útočník zachytí a využije platné relační tokeny nebo cookies k převzetí stávajících uživatelských relací, například na webových stránkách.
6. **E-mail Hijacking**: Útočník zachytí nebo přesměruje e-mailovou komunikaci, což mu umožní získávat informace nebo provádět další podvodné aktivity.