Bastion Host

Bastion Host je speciální počítač v síti, který je navržen a nakonfigurován tak, aby odolal útokům zvenčí. Funguje jako „brána“ nebo „předsunutá hlídka“ mezi veřejným internetem a soukromou vnitřní sítí, která obsahuje citlivá data a servery.

Jeho primárním účelem je minimalizovat tzv. **plochu útoku** (attack surface). Místo aby měly všechny servery v síti veřejnou IP adresu a byly vystaveny internetu, má ji pouze Bastion Host.

Architektura a princip fungování

V typickém nastavení (např. v AWS nebo Azure) jsou servery (databáze, aplikační servery) umístěny v **soukromé podsíti** (Private Subnet) bez přístupu zvenčí.

```
1. Administrátor se nejprve připojí pomocí SSH nebo RDP k **Bastion Hostu**, který se nachází ve veřejné podsíti (Public Subnet).
2. Teprve po úspěšném ověření na Bastion Hostu může administrátor navázat další spojení na vnitřní servery v soukromé síti.
```

Klíčové bezpečnostní vlastnosti

Aby Bastion Host plnil svou roli, musí být „opevněn“ (tzv. **Hardening**):

- **Minimalismus:** Na serveru běží pouze nezbytně nutné služby (např. jen SSH). Žádné webové prohlížeče, grafické rozhraní nebo nepotřebný software.
- **Pevná pravidla Firewallu:** Povoluje příchozí spojení pouze ze specifických IP adres (např. z VPN firmy) a pouze na konkrétním portu (např. TCP 22 pro SSH).
- **Vícefaktorová autentizace (MFA):** Přihlášení k Bastion Hostu by mělo vyžadovat kromě klíče/hesla i druhý faktor.
- **Logování a Audit:** Každá akce, kterou administrátor na Bastion Hostu provede, je pečlivě zaznamenávána pro případnou zpětnou kontrolu.

Rozdíl mezi Bastion Hostem a VPN

Ačkoliv oba slouží k bezpečnému přístupu, princip je jiný:

- **VPN (Virtual Private Network):** Vytvoří šifrovaný tunel a uživatel se stává „součástí“ vnitřní sítě (může přímo vidět více serverů).

- **Bastion Host:** Funguje jako prostředník na aplikační úrovni. Uživatel se musí nejdříve přihlásit na tento „skokový“ stroj a z něj teprve pokračovat dál.

Výhody nasazení

- **Centrální správa přístupu:** Všechny přístupy do vnitřní sítě procházejí skrze jeden uzel.
- **Ochrana před útoky typu Brute Force:** Útočníci nevidí IP adresy vnitřních serverů, takže na ně nemohou útočit přímo.
- **Zjednodušení pravidel:** Vnitřní servery mají ve svých firewallech nastaveno: „Povolit přístup pouze z IP adresy Bastion Hostu“.

Moderní alternativy (Cloud-Native)

V moderních cloudových infrastrukturách se od klasických Bastion Hostů (virtuálních strojů) často upouští ve prospěch spravovaných služeb:

- **AWS Systems Manager Session Manager:** Umožňuje přístup k serverům bez nutnosti mít otevřené porty nebo veřejnou IP adresu.
- **Azure Bastion:** Plně spravovaná služba (PaaS), která poskytuje přístup k VM přímo skrze prohlížeč přes SSL, aniž by servery musely mít veřejné adresy.

Související pojmy: SSH, Firewall, Azure Bastion, DMZ, Network Segmentation, MFA.