Co to je DDoS útok

Poslední aktualizace 15 listopadu, 2024

DDoS (Distributed Denial of Service) je forma kybernetického útoku, při němž se útočník pokouší přetížit server obrovským množstvím žádostí o připojení, a tím jej zpomalit nebo zcela vyřadit z provozu.

Cílem DDoS je, **aby legální uživatelé nemohli služby či web uložené na daném serveru normálně využívat**.

Představte si to, jako kdyby si někdo najal dav záškodníků a poslal je do restaurace, kam se vy zrovna chystáte na oběd. Tito záškodníci naplní její kapacitu, nic si neobjednají a pro vás už v ní není místo.

Je důležité si uvědomit, že útočník obvykle nejedná sám. Používá **armádu infikovaných počítačů, tzv. botnet**, umístěných po celém světě. Tyto počítače mohou být napadeny malwarem (Trojským koněm) a součástí útoku se stávají bez vědomí jejich vlastníků.

Útočníci DDoS často používají k vydírání, vyjádření protestu proti konkrétní společnosti nebo jednoduše pro vlastní potěšení. V jejich hledáčku jsou především **velké firmy, finanční instituce nebo vládní webové stránky**.

Jak se před DDoS útoky bránit?

Koncový uživatel služeb a webů se proti dopadům DDoS sám nijak bránit nemůže.

> *Může ale zabránit tomu, aby se z jeho počítače stal infikovaný bot. Trojské koně odhalí antivirus.*

Ochrana před DDoS útoky **probíhá na úrovni serveru**. Je samozřejmě v nejlepším zájmu každé firmy, aby se zajistila maximální dostupnost svých služeb.

Pro prevenci DDoS útoků se využívá kombinace různých nástrojů a taktik, např.:

- automatická detekci neobvyklého síťového provozu
- cloudová DDoS ochrana poskytovaná specializovanými službami
- zvýšení šířky pásma (bandwidth) a vytvoření redundantní infrastruktury