Čo to je DDoS útok

Last updated 13 marca, 2025

DDoS (Distributed Denial of Service) je forma kybernetického útoku, pri ktorom sa útočník pokúša preťažiť server obrovským množstvom žiadostí o pripojenie, a tým ho spomaliť alebo úplne vyradiť z prevádzky.

Cieľom DDoS je, **aby legálni používatelia nemohli služby či web uložené na danom serveri normálne využívať**.

Predstavte si to, ako keby si niekto najal dav záškodníkov a poslal ich do reštaurácie, kam sa vy práve chystáte na obed. Títo záškodníci naplnia jej kapacitu, nič si neobjednajú a pre vás už v nej nie je miesto.

Je dôležité uvedomiť si, že útočník zvyčajne nekoná sám. Používa **armádu infikovaných počítačov, tzv. botnet**, umiestnených po celom svete. Tieto počítače môžu byť napadnuté malvérom (Trojským koňom) a súčasťou útoku sa stávajú bez vedomia ich vlastníkov.

Útočníci DDoS často používajú na vydieranie, vyjadrenie protestu proti konkrétnej spoločnosti alebo jednoducho pre vlastné potešenie. V ich hľadáčiku sú predovšetkým **veľké firmy, finančné inštitúcie alebo vládne webové stránky**.

Ako sa pred DDoS útokmi brániť?

Koncový používateľ služieb a webov sa proti dôsledkom DDoS sám nijak brániť nemôže.

> *TIP: Môže však zabrániť tomu, aby sa z jeho počítača stal infikovaný bot. Trojské kone odhalia antivírus.*

Ochrana pred DDoS útokmi **prebieha na úrovni serveru**. Je samozrejme v najlepšom záujme každej firmy, aby zabezpečila maximálna dostupnosť svojich služieb.

Na prevenciu DDoS útokov sa využíva kombinácia rôznych nástrojov a taktik, napr.:

- automatická detekcia nezvyčajnej sieťovej prevádzky
- cloudová DDoS ochrana poskytovaná špecializovanými službami
- zvýšenie šírky pásma (bandwidth) a vytvorenie redundantnej infraštruktúry