



ČDT-ANTIDDOS

Účinná ochrana zákazníků před DDoS útoky. Speciální technologie hloubkové inspekce provozu scrubbing centra dokážou vyhodnotit, které pakety jsou regulérním provozem zákazníka a které jsou součástí DDoS útoku. Pakety, které jsou součástí DDoS útoku, scrubbing centrum zachytí a nepropustí k zákazníkovi.

DDoS (Distributed Denial of Service) útoky mají omezit dostupnost služby (např. webových stránek) a jsou charakteristické tím, že útok probíhá současně u velkého množství IP adres (což znemožňuje jejich jednoduché blokování) a zároveň je tak silný, že velmi rychle zahltí dostupné přenosové pásmo, systémové zdroje cíle útoku či prvky transportní infrastruktury balastním provozem, jehož podoba je velmi proměnná a předem nepředvídatelná.

Účinná ochrana před DDoS útoky vyžaduje použití metod hloubkové inspekce provozu a mechanismy rychlé adaptace na jeho různé formy.

www.cdt.cz

ČDT-ANTIDDOS

Služba ČDT-ANTIDDOS je poskytována ve 2 variantách

- **Připraveno k čištění** – při detekci DDoS útoku je provoz přesměrován do scrubbing centra. Přesměrování a začátek čištění provozu proběhne do 4 minut od začátku DDoS útoku.
- **Trvalé čištění** – provoz účastníka je trvale směřován přes scrubbing centrum. Začátek čištění proběhne do 1 minuty od začátku DDoS útoku.

Služba zachycuje následující typy útoků

- útoky generované známými nástroji dostupnými na internetu
- DDoS provoz generovaný známými botnety
- SYN FLOOD
- TCP ACK + FIN FLOOD
- TCP RST FLOOD
- TCP SYN + ACK FLOOD
- TCP fragmentation FLOOD
- UDP FLOOD
- ICMP FLOOD
- IGMP FLOOD

ČDT-ANTIDDOS zabraňuje

- nedostupnosti služby (e-shopu, webových stránek zákazníka) způsobené DDoS útokem
- ztrátám způsobeným DDoS útoky, jež nelze běžnými způsoby jednoduše blokovat
- zahlcení dostupného přenosového pásma a systémových zdrojů, které jsou cílem útoku
- zahlcení prvků transportní infrastruktury balastním provozem, jehož podoba bývá proměnná a předem nepředvídatelná
- nekalým konkurenčním praktikám prostřednictvím DDoS útoků

Hlavní výhody

- včasné odhalení DDoS útoků v internetové konektivitě
- odstranění balastního provozu
- nedochází k omezení či nedostupnosti služeb
- plně automatické řešení bez nutnosti manuálních zásahů
- výrazné zrychlení reakční doby na DDoS útok
- snížení zátěže na aktivních prvcích provozovatele sítě

Komu je služba určena

- lokálním poskytovatelům internetu
- velkým a středním společnostem
- státní správě a samosprávě
- poskytovatelům obsahu
- zpravodajským serverům
- provozovatelům e-shopů
- finančním institucím

ČDT-ANTIDDOS je doplňkovou službou k přístupu do sítě Internet poskytovanému společností ČD - Telematika.