ČD-Telematika

Kybernetická bezpečnost - jak se bránit útokům

Ing. Tomáš Havlíček
Produktový manažer

5 | 04 | 2016

ČD - Telematika a.s.

- Poskytuje služby servisu, správy a výstavby optických sítí, ICT a velkoobchodní telekomunikační a datové služby
- Řadí se mezi největší poskytovatele datových služeb a internetového připojení v České republice
- Služby poskytuje segmentu státní správy, významným telekomunikačním operátorům, korporacím i lokálním poskytovatelům internetu

- Má více než 500 zaměstnanců s jedinečným know-how
- V roce 2013 dosáhla obratu přes 1,1 miliardy, zisk před zdaněním činil 36 milionů korun
- Majoritní akcionář České dráhy a.s. 59 %, Dial Telecom, a.s. 29%

www.cdt.cz

ČD - Telematika a.s. Korespondenční adresa Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938

ČD-Telematika

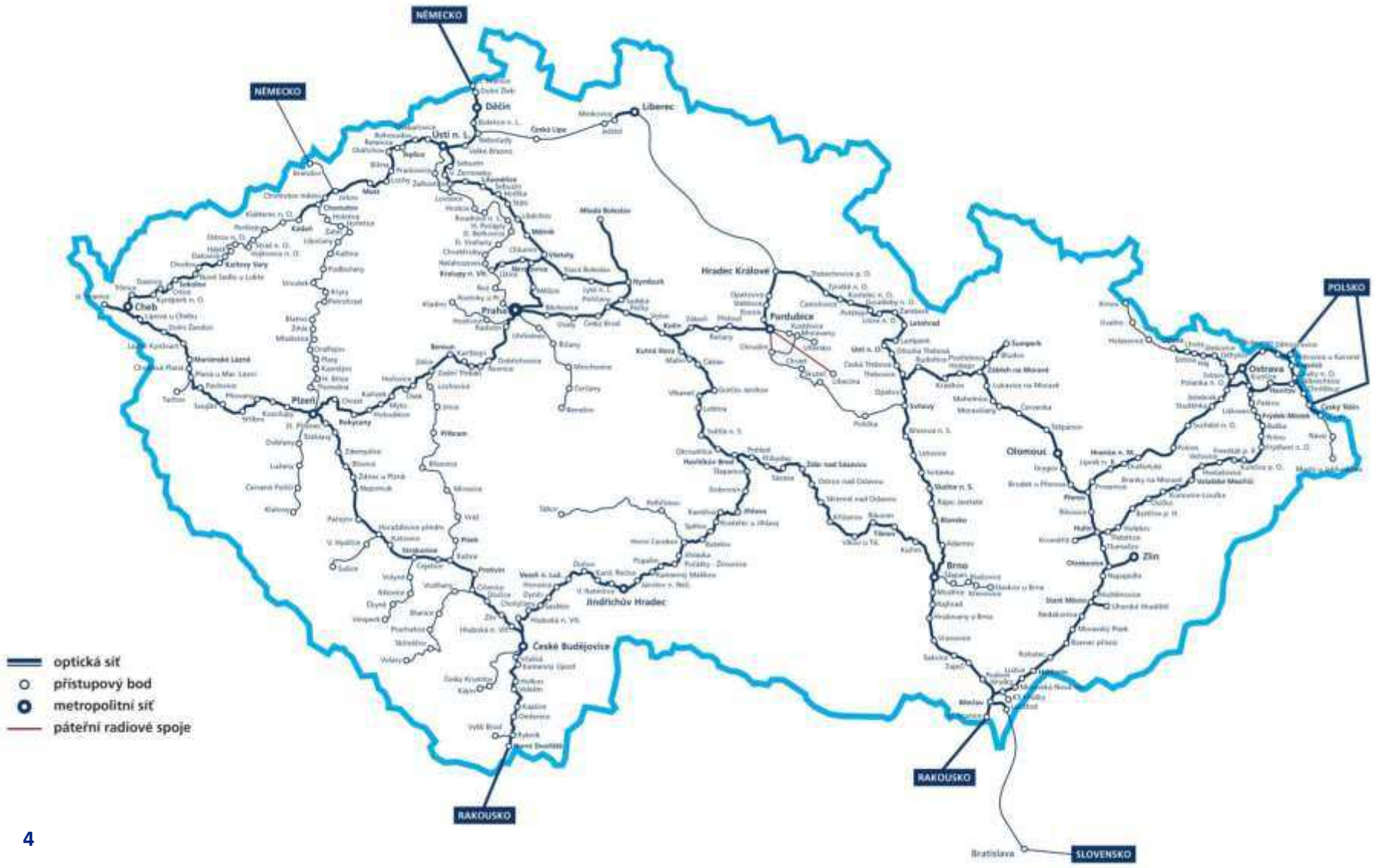
Zázemí ČD-T

- **Druhá největší optická infrastruktura v ČR**
- 3 500 km optických tras
- Optická síť ve více než 400 přípojných bodech
- Přenosová kapacita až 80 x 10 Gbps
- Metropolitní sítě ve 26 velkých městech
- Dohled 365/24/7
- 3 geograficky nezávislá datová centra
- 42 servisních pracovišť v ČR

ČD - Telematika a.s. Korespondenční adresa Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938

ČD-Telematika

OPTICKÁ SÍŤ ČD-T v roce 2015



ČD-Telematika

Telekomunikační služby

- **Pronájem vláken**
- **Přenosové služby**
- **Internetové služby**
- **Hlasové služby**
- **Serverhousing**

ČD - Telematika a.s. Korespondenční adresa Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938

ČDT a internetová bezpečnost

- Účast v projektu FENIX
- ČDT – MONITOR
  detekce bezpečnostních rizik v internetové konektivitě
- ČDT – AntiDDoS
  čištění provozu při DDoS útoku ve scrubbing centru

ČD - Telematika a.s. Korespondenční adresa Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938

Projekt FENIX

- vznikl v prostředí NIXu
- nouzový prostředek vzájemné komunikace mezi členy NIXu v případě rozsáhlého útoku na český internet – „atomový bunkr“
- postaveno na vzájemné důvěře členů projektu
- založeno několika členy NIXu
- přistoupení dalších na základě:
  - splnění technických požadavků
  - nastavení procesů
  - důvěra existujících členů

ČD - Telematika a.s. Korespondenční adresa Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938

ČDT - Monitor

- detekce bezpečnostních rizik v internetové konektivitě
- Flowmon sondy
- omezený počet vybraných metod
- report zákazníkovi denně/týdně

ID	Timestamp	Type	Detail	Source	Targets	NetFlowSource
#5640767	2015-05-11 23:15:00	SSHDICT	Continuation of attack (unsuccessful), attempts: 92, targets: 12844, total upload: 158.21 KiB, maximal upload: 2.28 KiB. Single attack.	82.2[redacted].1[redacted].22	123.0.[redacted], 123.[redacted].77, [redacted].51.249, 123.[redacted].110, 123.[redacted].109, 123.[redacted].71, 123.0.[redacted], 123.[redacted].126.170, 123.0.[redacted] ...	localhost

ČD - Telematika a.s. Korespondenční adresa Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938

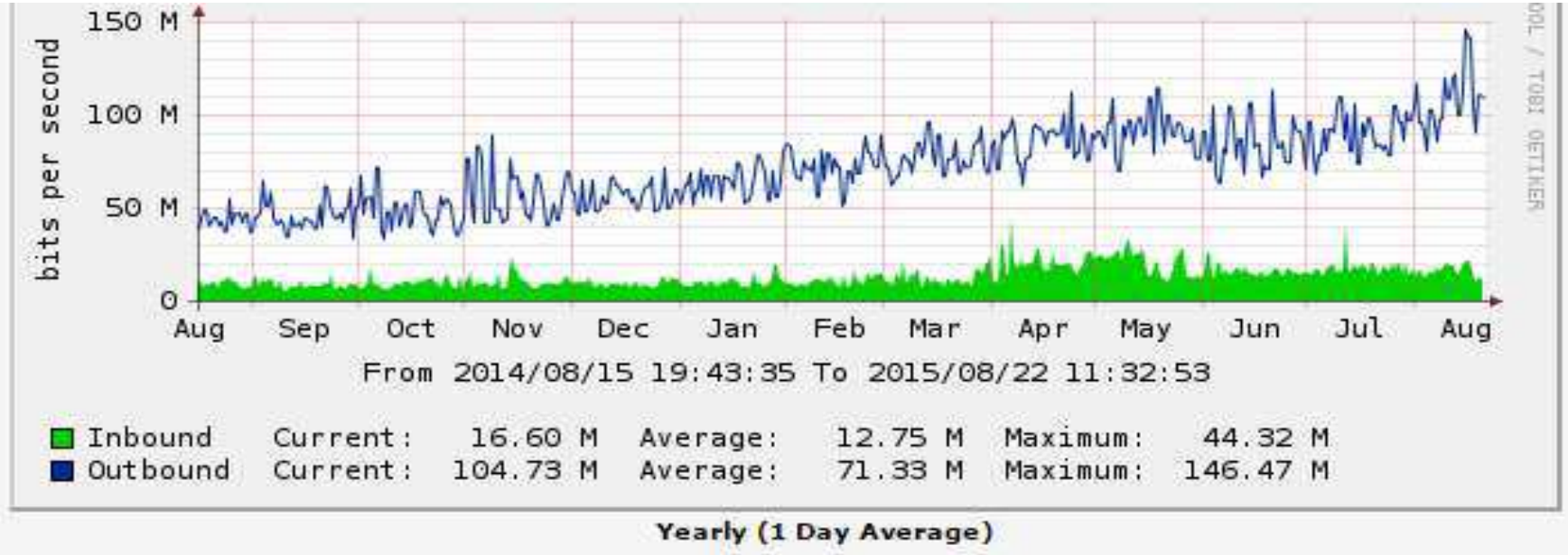
Vybrané metody ČDT-Monitor

- **Telnet** – zvýšené použití služby Telnet. Detekuje veškeré spojení, včetně pokusů o spojení na TCP port 23 a pro jednotlivé IP adresy počítá počty těchto spojení;
- **SSHDICT** – pokusy o uhodnutí jména/hesla, přihlášení podvrženým certifikátem ;
- **OUTSPAM** – odesílání nebo pokusy zvýšeného počtu e-mailů;
- **SCANS** – různé typy scanování sítě a způsoby provedení;
- **DNSQUERY** – zvýšený počet DNS dotazů z konkrétních IP adres;
- **DNSANOMALY** – podezřelá komunikaci DNS provozu;
- **BLACKLIST** – kontrola provozu (podle přiřazených filtrů) a rozpoznání komunikace s IP adresami uvedenými na blacklistu;
- **RDP Dictionary Attacks** – pokusy o uhádnutí uživatelského jména/hesla do RDP;
- **REFLECTDOS Amplificated DoS attack** – detekuje DoS útoky skrze nedostatky některých služeb (např. nezabezpečené NTP servery);
- **DOS** – Detekční metoda odhaluje útoky typu Denial-of-Service nebo Distributed-Denial-of-Service.

ČD - Telematika a.s. Korespondenční adresa Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938

Příběh zákazníka „zahoryzadoly-net“ I.

- zákazník ČDT 2 roky
- 250 Mbps konektivity

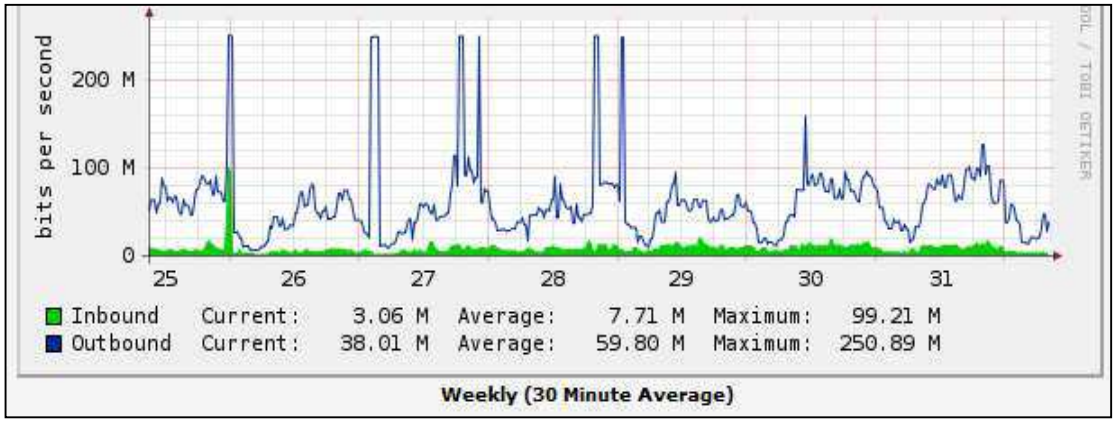


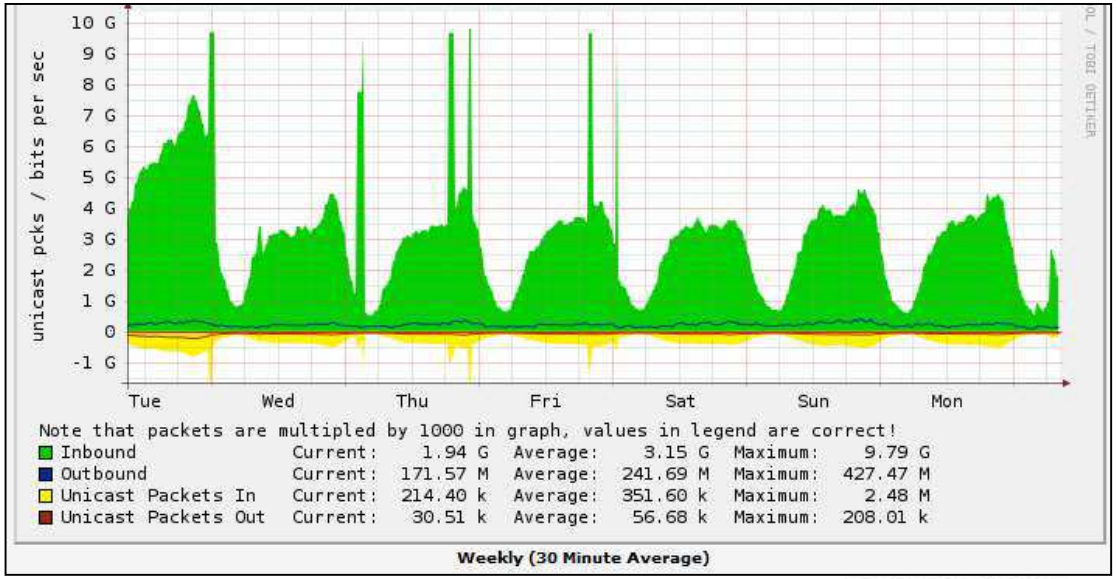
www.cdt.cz

ČD - Telematika a.s. Korespondenční adresa Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938

Příběh zákazníka „zahoryzadoly-net“ II.

- 25. – 28. 8. 2015
- opakované a cílené útoky na konkrétní IP adresu zákazníka
- po zablokování IP se útočník rychle adaptoval a útočil dále na novou IP adresu
- přístupová linka 250 Mbps – útok cca 8 Gbps v součtu
- útoky o délce 1 – 2 hodin v době špičky
- UDP Flood prostřednictvím NTP serverů ve světě
- obdobný případ cca 2x měsíčně





ČD - Telematika a.s. Korespondenční adresa Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938

ČD-Telematika

Co s tím??

- **Zablokovat celý rozsah IP adres**
  - filtry
  - RTBH
  - *do sítě ale nejde ani legitimní provoz*

ČD - Telematika poskytuje

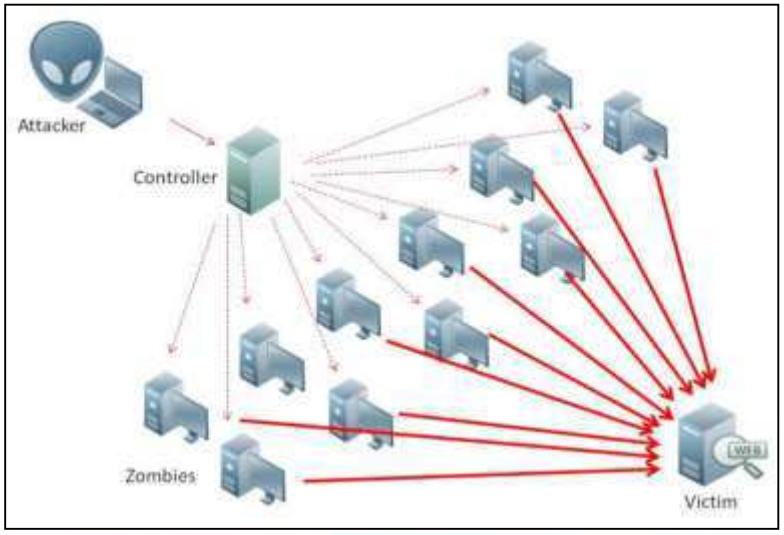
ČDT–ANTIDDOS

vyčištění provozu ve scrubbing centru

ČD - Telematika a.s. Korespondenční adresa Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938

Trocha teorie nikoho nezabije

- Cílem útoků typu odepření služby (*Denial of Service*, zkráceně DoS), „zamezení autorizovaného přístupu k systémovým zdrojům nebo zdržení operací a funkcí systému“
- DDoS útoky (*Distributed Denial of Service*), útočník využívá různý počet strojů, aby byl útok úspěšnější a pro oběť obtížněji zastavitelný.
- Pokud útočník při DoS/DDoS útoku uspěje, cílový stroj, služba nebo síť se stane nedostupnou.



ČD - Telematika a.s. Korespondenční adresa Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938

ČD-Telematika

Efektivní obrana

- **Prevence**
  - útoky jsou motivovány politicky nebo ekonomicky
  - čistota sítě – ne/zabezpečené prvky – botnety, spam stroje
- **Detekce**
  - monitoring flow - sondy na všech vstupech/výstupech z ASN
  - behaviorální analýza
- **Obrana**
  - filtry
  - RTBH
  - **čištění – scrubbing, mitigace**

ČD - Telematika a.s. Korespondenční adresa Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938

ČD-Telematika

ČDT-ANTIDDOS

technologické zázemí

- **detekce útoku** a automatické přesměrování provozu – sondy Flowmon, modul DDoS Defender

- **scrubbing centrum** – RADWARE DefensePro, kapacita 10 Gbps legitimního provozu + 12 Gbps útoku

ČD - Telematika a.s. Korespondenční adresa Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938

ČDT-ANTIDDOS

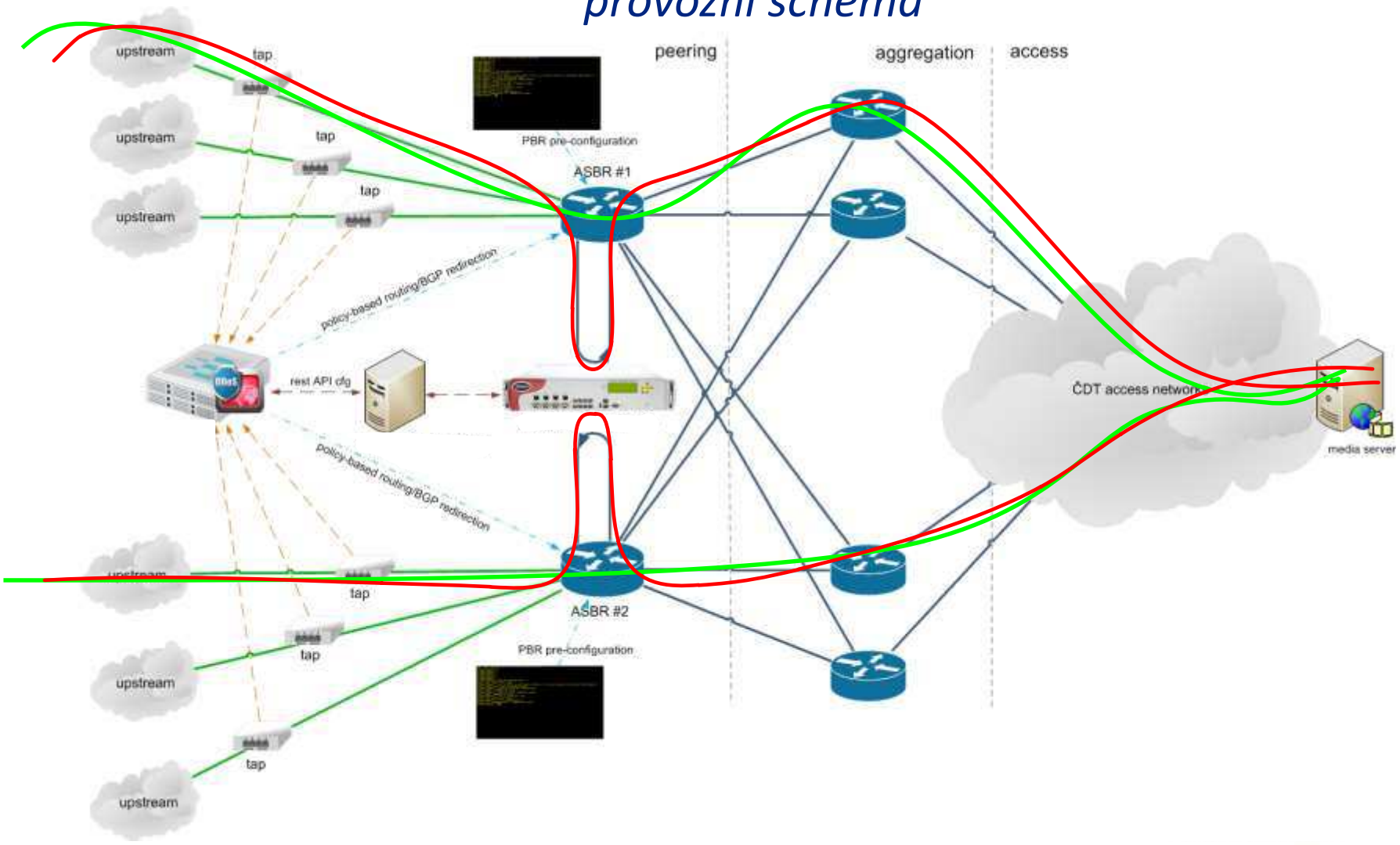
Proti čemu chrání

- Volumetrické (objemové) útoky
- útoky generované známými nástroji dostupnými na Internetu
- DDoS útoky generované známými botnety
- SYN FLOOD, TCP ACK + FIN FLOOD, TCP RST FLOOD, TCP SYN + ACK FLOOD, TCP fragmentation FLOOD, UDP FLOOD, ICMP FLOOD, IGMP FLOOD

ČD - Telematika a.s. Korespondenční adresa Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938

ČDT-ANTIDDOS

provozní schéma



ČD - Telematika a.s. Korespondenční adresa Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938

ČD-Telematika

ČDT-ANTIDDOS

varianty produktu

- **Připraveno k čištění**
  - provoz mimo scrubbing centrum
  - detekce útoku prostřednictvím flowmon sond
  - přesměrování do scrubbing centra
  - začátek čištění do 15 minut od zahájení útoku

- **Trvalé čištění**
  - provoz trvale přes scrubbing centrum
  - zahájení útoků do 2 minut od zahájení provozu

ČD - Telematika a.s. Korespondenční adresa Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938

ČDT-ANTIDDOS

výhody

- automatizace – odpadá ruční práce
- rychlost – odpadá hlášení problému a komunikace techniků, dohledů
- spolehlivost
- cena

ČD - Telematika a.s. Korespondenční adresa Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938

Dotazy?

Kontakt
ČD - Telematika a.s.
Ing. Tomáš Havlíček
Produktový manažer
e-mail: tomas.havlicek@cdt.cz

ČD - Telematika a.s.
Korespondenční adresa
Pod Táborem 369/8a | 190 00 Praha 9
tel.: +420 972 225 555
e-mail: poptavka@cdt.cz

Sídlo společnosti
Pernerova 2819/2a | 130 00 Praha 3
IČ: 61459445 | DIČ: CZ61459445
vedená u Městského soudu v Praze, spisová značka B 8938