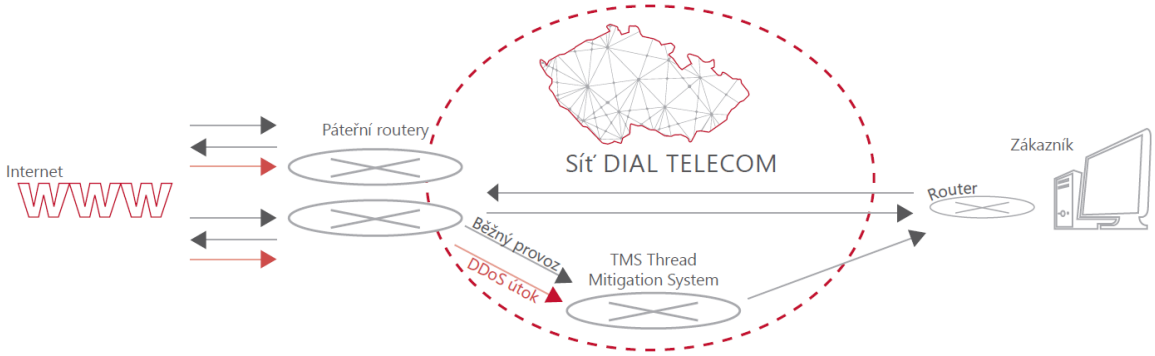
AntiDDoS

Chraňte svoje servery před největší hrozbou ve světě Internetu. Pouze za loňský rok bylo na světě spácháno 8,4 milionů DDoS útoků. To znamená 23 000 napadení za den, 16 za minutu.

DDoS (Distributed Denial of service - distribuované odepření služby) je typem útoku na internetové služby nebo stránky. Záměrem je vyřadit cílovou službu z provozu. Útočník toho dosahuje pomocí přehlcení serveru obrovským množstvím požadavků.

Službu si lze pořídit jako doplněk k produktům Profi Internet a IP Konektivita. Služba omezuje nežádoucí provoz na základě statistického zjišťování anomálií předem nastavených parametrů. Dále umožňuje prostřednictvím webového administračního rozhraní manuální nastavení čištění při probíhajícím útoku. Součástí služby je úvodní konzultace a analýza provozu, na jejímž základě proběhne nastavení pravidel ochrany proti DDoS.

a. Schéma služby



b. Technický popis

Ochrana zákaznické sítě před DDoS útoky je řešena kombinací hardwarových a softwarových prostředků Dial Telecom. Jedná se zejména o systém detekce a vyhodnocování anomálií v provozu zákaznické sítě, což je realizováno pomocí platformy PeakFlow SP od společnosti Netscout. Samotná reaktivní ochrana je pak postavena na několika klíčových komponentech. Ty jsou tvořeny jednak podporou technologie BGP FlowSpec a dalších v páteřních směrovačích Cisco ASR 9900 a Juniper MX a dále pak samotným zařízením pro selektivní odstraňování nežádoucího provozu Netscout TMS (Threat mitigation system – systém zmírňování hrozeb).

Strukturované řešení umožňuje odfiltrování některých druhů nežádoucího provozu již v páteřních směrovačích Dial Telecom. Filtraci na výrazně jemnější úrovni lze posléze provádět na zařízení TMS. K dispozici je možnost automatické aplikace připravené šablony pro filtrování provozu v případě detekce aktivity, která svým charakterem připomíná volumetrický útok. Konkrétní nastavení a vyladění takové šablony bude provedeno ve spolupráci se specialisty společnosti Dial Telecom.

Součástí služby je přístup k speciálnímu webovému rozhraní , které je zabezpečeno prostřednictvím kryptované VPN a dále SSL (https), kde lze sledovat volumetrické bezpečnostní incidenty, jež se týkají zákaznické sítě, a také zadávat a měnit specifická opatření proti konkrétním druhům provozu.

c. Obsah služby

Služba je navrhnuta tak, aby splnila Vaše požadavky v oblasti telekomunikačních služeb. V následující tabulce je popis jednotlivých komponentů služby:

Služba AntiDDoS obsahuje
Úvodní konzultaci analýzy provozu, nastavení a základní zaškolení
Zřízení a provozování DDoS ochrany
Automatické čištění podle předem nastavených pravidel, případně manuální nastavení čištění v průběhu útoku
Online přístup k administračnímu rozhraní prostřednictvím kryptované VPN
Zaslání emailu o začátku a konci útoku
Měsíční reporty emailem
Volitelnou profesionální pomoc s doladěním služby podle vašich požadavků
Volitelné pokročilé školení vhodné pro plné využití systému (rozsah cca 2 dny)
Uživatelskou podporu 24 /7

d. výhody navrhovaného řešení

- Individuální přístup a nastavení na míru zákaznickému provozu
- Úvodní zaškolení v ceně služby
- Online monitoring provozu a změny nastavení prostřednictvím administračního rozhraní
- Profesionální pomoc při závažných útocích
- Dohled 24/7