DDOS OCHRANA

VÁŠ ŠTÍT PROTI KYBERNETICKÝM ÚTOKŮM

Distribuované útoky typu Denial of Service (DDoS) jsou stále jednou z největších hrozeb, kterým čelí dnešní internetová infrastruktura. Útočníci se DDoS útoky snaží o přetížení cílových serverů, sítí nebo aplikací masivním množstvím falešného provozu, což vede k nedostupnosti služeb pro skutečné uživatele. Tyto útoky pak firmám způsobují značné finanční ztráty, poškození reputace a ztrátu důvěry jejich koncových zákazníků.

O SLUŽBĚ DDOS OCHRANA

Služba DDoS ochrana je postavena na špičkové technologii Arbor společnosti NetScout, lídra v oblasti kybernetické bezpečnosti. Představuje robustní, nepřetržitou a inteligentně automatizovanou ochranu konektivity zákazníka před kybernetickými útoky typu DDoS. Monitoruje v režimu 24x7 a v případě útoku na vybrané cíle zákazníka je spuštěna automatická nebo manuální mitigace (čištění provozu). Způsob mitigace útoku je proveden dle zvolené varianty produktu a s ohledem na typ a vedení daného útoku (tzv. vektory útoku). Nabídka služby DDoS ochrana obsahuje několik variant, od základní ochrany konektivity s elementární sadou pravidel až po komplexní řešení na míru zákazníka. Specifikace cílů je definována formou tzv. Managed objektů, Whitelistů apod.

JAK SLUŽBA DDOS OCHRANA FUNGUJE?

1. DETEKCE ÚTOKŮ:

- Neustálé monitorování síťového provozu s cílem identifikovat anomálie a potenciální DDoS útoky.
- Pokročilé analytické nástroje pro rozpoznání různých typů útoků, včetně volumetrických, protokolových a aplikačních útoků.

2. MITIGACE ÚTOKŮ:

- Okamžitá reakce na detekované hrozby.
- Automatické přesměrování podezřelého provozu přes filtrační centrum, kde je škodlivý provoz eliminován, zatímco legitimní provoz je bezpečně doručen k cíli.

3. NEPŘETRŽITÁ OCHRANA:

- 24 x 7 monitoring a podpora.
- Pravidelné aktualizace a přizpůsobení ochrany novým typům hrozeb.

PARAMETRY	MONITORING	BASIC	STANDARD	ADVANCED
Monitoring 24 x 7	✓	✓	✓	✓
Reporty	✓	✓	✓	✓
Počet mitigací	✗	neomezeně	neomezeně	neomezeně
Asistence během útoku	✗	✗	8 x 5	24 x 7
Možnost rozšíření služby o dedikovanou ochranu AED	✗	✗	✗	✓
Specifická konfigurace služby na míru zákazníka	✗	✗	✗	✓
PŘÍKLADY ÚTOKŮ				
Volumetrický útok (NTP Amplifikace)	✗	✓	✓	✓
Útok proti specifickým serverům, např. útoky na VPN Gateway (HTTP Flood)	✗	✗	✓	✓
Cílený DNS útok na DNS servery (Water Torture)	✗	✗	✗	✓

Ochranu zákaznické infrastruktury lze zvýšit nasazením koncových dedikovaných zařízení Arbor Edge Defense (AED). Tato on-premise zařízení poskytují in-line bezstavovou paketovou detekci a obranu v reálném čase. AED komunikuje s operátorskou vrstvou DDoS ochrany a je možné ho plně přizpůsobit potřebám a chování jednotlivých serverů a vytvořit tak komplexní obranu proti DDoS útokům.

SECURITYHUB

Součástí služby DDoS ochrana je Portál (CRA Security Hub), který zákazníkům přináší online přehled o stavu jeho infrastruktury, formou přehledných grafů a tabulek. Umožňuje manažerské pohledy a definici oprávnění dle rolí uživatelů. Součástí portálu je i možnost spuštění a vypnutí mitigace uživatelem, napojení na rozhraní Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) pro hlášení incidentů a událostí a také napojení na nativní portál technologie Arbor (Sightline).

PRO KOHO JE SLUŽBA URČENA?

KORPORACE A VELKÉ SPOLEČNOSTI	Firmy závislé na nepřetržité dostupnosti svých online služeb. Organizace, které musí chránit citlivá data a zajistit kontinuitu obchodních operací.
E-COMMERCE A ONLINE OBCHODY	Obchodníci, kteří potřebují zajistit nepřetržitý přístup zákazníků k jejich e-shopům. Firmy, které chtějí ochránit svůj online prodej a reputaci.
FINANČNÍ INSTITUCE	Banky, pojišťovny a další finanční instituce, které musí chránit transakční systémy a osobní údaje zákazníků.
VEŘEJNÝ SEKTOR	Vládní instituce a veřejné služby (zdravotnictví, školství apod.), které potřebují zabezpečit své online systémy proti kybernetickým hrozbám.
MALÉ A STŘEDNÍ PODNIKY	Podniky všech velikostí, které chtějí zabezpečit své digitální aktivity a minimalizovat rizika spojená s DDoS útoky.

VÝHODY SLUŽBY DDOS OCHRANA:

- **Zajištění dostupnosti** – nepřetržitý přístup k vašim online službám a aplikacím, i během pokusů o DDoS útok,
- **Ochrana reputace** – minimalizace rizika výpadků, které by mohly poškodit vaši pověst a důvěru zákazníků,
- **Finanční úspory** – redukce potenciálních finančních ztrát způsobených výpadky služeb a nákladů na obnovu po útoku,
- **Klid na práci** – profesionální a nepřetržitá ochrana poskytovaná CRA týmem certifikovaných odborníků v oblasti kybernetické bezpečnosti,
- **Přizpůsobitelnost a flexibilita** – Možnost škálovat ochranu podle vašich konkrétních požadavků a růstu vašich potřeb.

Investice do služby DDoS ochrana je významným krokem k zabezpečení vaší digitální infrastruktury proti nejmodernějším kybernetickým hrozbám. Nezáleží na velikosti vaší firmy nebo oblasti podnikání, získáte jistotu, že vaše online aktivity zůstanou chráněny a dostupné za všech okolností. Pro více informací a konzultaci na míru navštivte naše webové stránky nebo kontaktujte náš tým odborníků.