UDRŽTE KONTINUITU PODNIKÁNÍ I PŘES SÍLÍCÍ INTENZITU DDoS ÚTOKŮ

ÚTOČNÍCI CÍLÍ NA DOSTUPNOST SYSTÉMŮ

DDoS (*Distributed Denial of Service*) je druh kybernetického útoku, při kterém útočník zahlcuje servery a další síťové prvky nepřiměřeným množstvím dat. To se projevuje např. zpomalením výkonu, zastavením systému, nebo nedostupností webových stránek. Takový útok může vyřadit významné systémy na mnoho dní a jejich nedostupnost pak napáchat škody likvidačních rozměrů.

PŘIBÝVAJÍ NOVÉ TAKTIKY A ADAPTABILITA

Už nejde jen o zahlcování systémů masivními objemy dat z různých míst internetu (volumetrické útoky). Přibývá multi-vektorových útoků kombinujících více metod. Zaměřují se na více prvků a vrstev IT infrastruktury (aplikační a stavové útoky). Zvyšuje se jejich četnost, rozsah a délka trvání. Objevují se adaptivní DDoS útoky, které mění útočné vektory podle typu průběžně zjištěné obrany. DDoS útoky mohou také být jen prvním krokem k dalšímu mnohem rozsáhlejšímu cílenému útoku s úmyslem proniknout do interní sítě a zneužít data.

ODHADOVANÁ PRŮMĚRNÁ CENA ZA MINUTU VÝPADKU IT SYSTÉMŮ

Zdroj: Gartner

ZTRÁTY JSOU OKAMŽITÉ A MOHOU BÝT FATÁLNÍ

Provozní náklady na eliminaci útoku, zpomalení výkonu a nižší produktivita, ztráta kreditu, opětovné budování důvěry zákazníků, pokuty a penále.

V HLEDÁČKU JSOU INSTITUCE A POSKYTOVATELÉ

Útoky na infrastrukturu síťové konektivity spouští celou kaskádu dalších negativních dopadů na všechny další subjekty, které jsou přes ni připojeny. U státních institucí může mít útok za cíl vytvářet politický nátlak a vyvolávat nestabilitu, pokud by kromě nedostupností webových stránek úřadů vedl také k omezení provozu klíčových systémů kritické infrastruktury jako jsou např. řídící a regulační systémy distribučních sítí, zabezpečovací systémy v dopravě nebo informační systémy nemocnic.

I OBCHODNÍ FIRMY JSOU V OHROŽENÍ

DDoS útok může vyřadit firemní systémy závislé na internetu a v důsledku tak může např. snížit dostupnost objednávkového systému nebo viditelnost webových stránek zrovna v době probíhající marketingové kampaně. Útočníkům často jde i o vydírání a za zastavení útoku požadují zaplacení výkupného.

ŘEŠENÍM JE MODERNÍ ANTI-DDoS

Útokům se nelze úplně vyhnout, lze se jen efektivně bránit. Nejúčinnější je několikaúrovňová ochrana kombinující on-prem a cloud nasazení. Svou roli hraje i domluvená spolupráce na úrovni ISP poskytovatele, protože, kdo se snaží řešit ochranu pouze vlastními silami, nemusí mít pro odražení rozsáhlejších útoků dostatečnou kapacitu.

S aktualizovanými plány obrany proti DDoS útokům včetně dostatečné kapacity pro mitigaci útoků a s kvalifikovaným poskytovatelem antiDDoS řešení je možno DDoS útokům úspěšně čelit.

SLUŽBY ŘÍZENÉ BEZPEČNOSTI | OCHRANA PROTI DDoS ÚTOKŮM

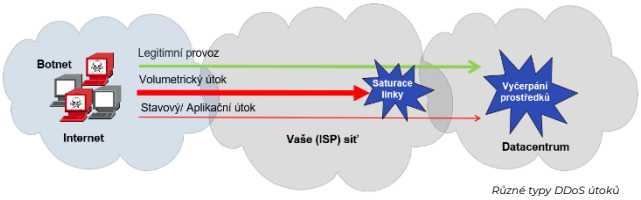
thein.security

CO MŮŽETE OČEKÁVAT OD NÁS:

Zajistíme nasazení a průběžnou správu AntiDDoS řešení od předního výrobce ochrany proti DDoS útokům.

S naší pomocí je možno útok v reálném čase detekovat, zastavit a automaticky i spustit nápravu. Dokážeme poskytovat několikaúrovňovou ochranu využitím funkcí jako:

- **zastavení volumetrického útoku** již v cloudu SP / ISP poskytovatele.
- **eliminace aplikačních útoků** a ochrana proti sofistikovaným bezpečnostním hrozbám, detekce botů (inbound / outbound).
- **Cloud Signaling** - inteligentní komunikace mezi ISP (in-cloud) a zákaznickým (on-prem) systémem.
- **Threat Inteligence** - inteligentní update rozhodovací logiky systému, monitoring zdrojů útoků, analýza nových metod útoků.
- **DDoS Protection Service** v globálním scrubbing centru - cloud služba odkloní provoz v případě extrémního útoku.



Různé typy DDoS útoků

ANTIDDoS ŘEŠENÍ je možno dodat jako službu nebo jako on-prem řešení a využít tak dle individuálních potřeb všechny jeho schopnosti:

- **DETEKCE**

Nepřetržitý monitoring a detekce v reálném čase.

- **KAPACITA**

Klasická ochrana proti DDoS útokům dokáže zmírnit útoky pouze do kapacity přípojné linky zákazníka. V případě rozsáhlejších volumetrických útoků je však nutné využít ochrany v cloudu a zastavit útok ještě před tím, než zahltí přípojnou linku. Naše řešení umí kombinovat oba způsoby ochrany.

- **MULTIVEKTOROVÁ OCHRANA**

Umíme detekovat útoky na transportní (L4) i aplikační (L7) vrstvě OSI modelu. Parametry detekce jsou nastavitelné pro každý vektor nezávisle.

- **ADAPTACE**

Pokud útočník během útoku mění jeho vzorec, jsme schopni v reálném čase upravit nastavení ochranného systému a udržet firemní systémy v bezpečí.

- **PRAVIDELNÝ REPORTING**

O zjištěných incidentech je poskytován pravidelný report.

VE VÝSLEDKU...

- lze s pomocí hybridní ochrany významnou část útoků zastavit ještě před tím, než zasáhnou firemní systémy a ovlivní důležité prvky její síťové infrastruktury.
- v případě již detekovaných a probíhajících útoků je možné účinně zmírnit jejich dopad.

PROČ BYSTE SI MĚLI VYBRAT PRÁVĚ NAŠE ŘEŠENÍ

- Naše služby jsou postaveny na stabilních řešeních prověřených technologických partnerů
- Díky zkušenostem s implementací ochrany u ISP i firemních zákazníků jsme schopni nastavit hybridní ochranu včetně cloudového řešení - propojení firmy a ISP
- Máme za sebou velké projekty implementace DDoS ochrany v ČR, v EU i mimo ni v jižní a jihovýchodní Evropě

MŮŽEME STAVĚT NA POZITIVNÍ ZKUŠENOSTI NAŠICH ZÁKAZNÍKŮ

Spolupracují s námi velké korporace, mobilní operátoři, poskytovatelé internetu, finanční instituce a státní správa, včetně silových bezpečnostních složek.

DISPONUJEME TÝMEM EXPERTŮ S DLOUHOLETÝMI ZKUŠENOSTMI

Od roku **2010** patříme k průkopníkům kybernetické bezpečnosti se zaměřením na **prevenci úniku citlivých dat**, obrany proti **sofistikovaným útokům**, detekce neznámého **malwaru** a aktivní ochrany proti **útokům DDoS**. Dodáváme služby a technologie do **hybridních prostředí** (on prem / cloud) a specializujeme se na **Zero Trust přístup.**

STANEME SE VAŠÍM PARTNEREM PRO OBLAST KYBERNETICKÉ BEZPEČNOSTI.

Pro více informací o řešení na Ochranu proti DDoS útokům a dalších službách kontaktujte naše obchodní zástupce na obchod.security@thein.eu nebo navštivte naše webové stránky.

Thein Security s.r.o., Pikrtova 1737/1a, 140 00 Praha 4 – Nusle, e-mail: info.security@thein.eu
Společnost vedená u Městského soudu v Praze oddíl C, značka 109813, IČO: 27415546, DIČ: CZ27415546