E-Bezpečí 2023, 8(1): Page 40-42. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=3172

CO JE TO DOS A DDOS?

Kamil KOPECKÝ

DoS (Denial of Service) je druh kybernetického útoku, který je zaměřen na zahlcení cílového serveru nebo sítě takovým množstvím dat, že uživatelé nejsou schopni přistupovat k požadovaným službám. DoS útoky jsou často spouštěny pomocí botnetů, což jsou sítě počítačů, které byly infikovány škodlivým softwarem a jsou ovládány útočníkem. Útoky DoS se staly běžnou taktikou pro hackery a kyberzločince, kteří chtějí způsobit podnikům a organizacím ztráty v produktivitě a výpadky služeb, což může mít vliv na finanční výsledky a pověst dané společnosti. DoS útoky se také používají k odstraňování konkurence, získávání informací nebo k vyjádření politických názorů.

Typy DoS útoků zahrnují:

Flooding: útok, při kterém útočník pošle velké množství datových paketů na server, aby jej zahltil a způsobil výpadky.

Amplification: útočník využívá nefunkčních serverů, které odpovídají na požadavky s velkým množstvím dat, aby vytvořil zvýšený tok datového provozu na cílový server.

Application: útoky na konkrétní aplikace, které jsou součástí webového serveru, jako jsou například SQL injection útoky.

Distributed: útoky, které využívají botnety, tedy sítě počítačů, které byly infikovány malwarem a jsou ovládány útočníkem.

Organizace mohou ochránit své servery a sítě před útoky DoS pomocí několika opatření, jako jsou například využívání firewallů,

antivirových programů a nástrojů na detekci DoS útoků. Další možností je využití služeb specializovaných firem, které poskytují ochranu proti DoS útokům. V případě, že organizace (firmy, státní instituce) nejsou schopny předcházet DoS útokům, mohou se stát obětí podnikové špionáže, ztráty citlivých informací, ztráty zákazníků a reputace. Proto by organizace měly být obezřetné a chránit své sítě a servery před kybernetickými útoky.

Výsledky DoS útoků mohou být velmi škodlivé a mohou vést k výpadkům v online službách, jako jsou například internetové bankovnictví, e-shopy, emailové servery nebo sociální sítě. Tímto způsobem mohou útočníci způsobit značné finanční ztráty a poškodit pověst společnosti.

V některých případech jsou DoS útoky používány k vyhrožování nebo vydírání. Útočník může například vydírat podnik, že pokud mu nezaplatí výkupné, bude nadále podniku blokovat přístup k internetovým službám. Tento typ útoku se nazývá DDoS (Distributed Denial of Service) a využívá botnety, které jsou rozmístěny po celém světě.

Existují různé způsoby, jak mohou organizace chránit své servery a sítě před DoS útoky. Jedním z nejúčinnějších opatření je využívání **specializovaného hardwarového zařízení**, jako jsou například tzv. anti-DDoS boxy, které jsou schopné filtrovat a omezovat nežádoucí datový provoz a bránit tak vzniku přetížení. Dále organizace mohou využít **softwarových nástrojů pro detekci a prevenci DoS útoků**, které jsou schopny analyzovat provoz na síti a bránit se nežádoucímu datovému provozu.

Organizace by měly také pravidelně aktualizovat své firewally a antivirové programy a chránit své sítě před neoprávněným přístupem. Je důležité také implementovat silná hesla a zabezpečit přístupová práva k datům a aplikacím na serveru.

Vzhledem k tomu, že DoS útoky jsou stále častější a sofistikovanější, je nutné, aby organizace přistupovaly k ochraně svých sítí a serverů velmi vážně a pravidelně prováděly **analýzu zranitelností**. Je důležité investovat do kvalitního hardwaru a softwaru pro ochranu proti DoS útokům a zavést adekvátní bezpečnostní opatření, aby byla ochrana proti útokům na co

nejvyšší úrovni.

Pro E-Bezpečí
Kamil Kopecký a AI
Univerzita Palackého v Olomouci