DoS / DDoS útoky

Doporučení pro případ napadení DDoS útokem - jak se zachovat a jak postupovat

Tento dokument popisuje doporučený postup, jak se zachovat v případě DDoS útoku na instituci nebo společnost v České republice. Zabývá se spoluprací mezi obětí takovéhoto útoku a bezpečnostním pracovištěm CERT/CSIRT. V druhé části podává konkrétní doporučení pro správce komunikačních sítí a další infrastruktury na bázi protokolu IP.

Definice pojmů

Autonomní systém (AS): množina směrovačů pod jednotnou technickou správou, využívající vnitřní směrovací protokol a společné metriky ke směrování paketů v rámci AS a využívající vnější směrovací protokol ke směrování paketů do jiných AS.

Páteřní síťová infrastruktura: páteřní síťovou infrastrukturou se rozumí všechny technické a administrativní prostředky pro provoz autonomního systému.

Provozovatel páteřní síťové infrastruktury: organizace, která disponuje technickými a administrativními prostředky pro provoz autonomního systému.

Kybernetický útok: jednání, které má za cíl způsobit škodu omezením či vyřazením služeb počítačových systémů z provozu, získaní či podvržení dat v elektronické podobě bez autorizace nebo získání neautorizovaných práv na cizím počítačovém systému.

Kybernetický útok typu DoS: kybernetický útok, který má za cíl omezit nebo vyřadit služby počítačových systémů. Zpravidla se jedná buď o generování velkého množství podvržených požadavků s cílem zahltit systém a/nebo přenosovou cestu nebo jde o sofistikovaný útok na slabá místa v cílovém systému a/nebo přenosové cestě.

Kybernetický útok typu DDoS: kybernetický útok typu DoS, který probíhá najednou koordinovaně z mnoha uzlů sítě.

IP spoofing: odesíláni datagramů s podvrženou zdrojovou adresou s cílem zakrýt skutečnou síťovou polohu a identitu útočníka.

IP squatting: dočasné nebo trvalé neautorizované použití prostoru IP adres ke komunikaci. V užším smyslu jde o propagaci prefixů protokolem BGP, které nebyly přiděleny propagujícímu autonomnímu systému příslušnou regionální autoritou.

Detekce útoku

Neoddělitelnou a velmi podstatnou součástí jakéhokoli ICT prostředí je jeho monitoring. Pokud existují monitorovací nástroje, které jsou správně nastaveny, detekce nestandardního chování na základě anomálií je většinou velmi rychlá. Po detekci nestandardního chování je nutné anomálie analyzovat a potvrdit, že se skutečně jedná o útok. Důležitý je důsledný monitoring jak jednotlivých systémů, tak síťového provozu. Po potvrzení probíhajícího útoku je třeba neprodleně kontaktovat svého poskytovatele internetu a příslušný bezpečnostní tým (CERT/CSIRT).

Kontakt mezi obětí útoku a příslušným CERT/CSIRT týmem

Tento kontakt by měl být možný oboustranně. Kontaktní informace vládního a národního CERT/CSIRT týmu jsou následující:

- Vládní CERT (GovCERT.CZ) - cert.incident@nbu.cz;
- Národní CSIRT (CSIRT.CZ) - abuse@csirt.cz.

Aby mohli členové CERT/CSIRT týmu kontaktovat zástupce Vaší instituce nebo společnosti, je třeba mít definované kontaktní údaje i na Vaší straně. Důležité je dobře zvolit kontaktní osobu. Musí se jednat o někoho, kdo má povědomí o celkové IT infrastruktuře v organizaci a zároveň má možnost přijímat konkrétní protiopatření. Současně s kontaktováním CERT/CSIRT týmu byste se měli spojit i se svým poskytovatelem internetu a požádat ho o dostupné informace a součinnost při řešení útoku.

Co můžete čekat od CERT/CSIRT týmů při DDoS útoku

V současné době pracuje Vládní CERT na zlepšení komunikačních kanálů mezi jednotlivými bezpečnostními pracovišti státní, komerční a akademické sféry. To umožní efektivnější reakci na případné další útoky a rychlé sdílení informací mezi zainteresovanými složkami. Po nahlášení útoku z Vaší strany a poslání relevantních informací se budou členové jednotlivých týmů schopni rychle spojit a poskytnout Vám pomoc především v následujících oblastech:

- globální pohled na to, co se děje a o jaký typ útoku se jedná;
- přizvání zainteresovaných stran do konference;
- pomoc s definicí pravidel pro filtrování provozu.

Na druhou stranu je třeba, abyste byli schopni poskytnout veškeré dostupné informace, které mohou pomoci při řešení útoku.

Co nemůžete čekat od CERT/CSIRT týmů při DDoS útoku

DDoS útok využívá samotné podstaty fungování Internetu a neexistuje proti němu stoprocentní obrana. Dopady lze samozřejmě mírnit, ale vždy je třeba najít kompromis mezi investicemi do obrany a potenciální výší škody. Tomu se věnuje tzv. analýza rizik, se kterou počítá i připravovaný zákon o kybernetické bezpečnosti. Národní centrum kybernetické bezpečnosti (NCKB), Vládní CERT nebo Národní CSIRT nelze brát jako organizace, které budou schopné zabránit všem budoucím útokům. Jejich role je především koordinační. Bezpečnost konkrétních subjektů je vždy výhradně v rukou lokálního správce.

Důležité otázky, které byste si měli položit ještě před útokem

Jak rychle jste schopni zaznamenat/diagnostikovat incident za pomoci analýzy síťových dat, logů ze serverů, IPS, firewallu? Sbíráte a uchováváte tyto logy?

Jak rychle jste schopni zajistit spolupráci Vašeho poskytovatele internetu? Víte, co pro Vás v případě útoku může udělat, koho máte kontaktovat a jak bude probíhat eskalace dále?

Máte připravené procedury, včetně všech potřebných kontaktních údajů a jednotlivých rolí pro případ, že útok nastane?

Provozujete odděleně infrastrukturu služeb běžících na internetu od služeb běžících pouze interně? Nebude dotčena interní část v případě útoku na veřejné služby?

Zvážili jste možnosti rychlého navýšení kapacity serverové farmy a internetové konektivity? Popřípadě možnost využití privátního nebo veřejného cloudu?

Víte o limitech své sítě, úzkých místech a neredundantních prvcích? Neobsahuje Vaše páteřní síťová infrastruktura SPOF (*Single Point Of Failure*)?

Umí Vaše zařízení zpracovávat SYN-cookies (jedná se o obranu proti DDoS útoku typu SYN flood)?

Doručení pro správce komunikačních sítí a další infrastruktury na bázi protokolu IP

Provozovatelé autonomních systémů by měli přijmout opatření a zavést procesy ke zvýšení bezpečnosti a odolnosti jimi spravovaných IP sítí. Navrhovaná opatřeni se skládají z:

- ochrany *control plane* směrovačů před útoky typu DoS;
- ochrany před útoky na směrovací protokol BGP typu DoS;
- ochrany před IP squattingem pomoci filtrovaní.

Provozovatelé autonomních systémů a provozovatelé koncových sítí by měli přijmout navrhovaná opatření skládající se z:

- ochrany před IP spoofingem;
- pasivního monitorování provozu a uchovávání dat;
- aktivní reakce na probíhající útok v podobě zintenzivněni monitorování a sběru forenzních informací;
- aktivní reakce na probíhající útok v podobě zablokování útoku.

Navrhovaná opatření nejsou vyčerpávající.

Ochrana *control plane* směrovačů

Smyslem ochrany *control plane* směrovačů je bránit se rozmanitým DoS útokům, které mají za cíl vyřadit řídící logiku směrovačů a způsobit kolaps časti sítě, případně vyvolat dominový efekt v celé síti. Provozovatelé páteřní síťové infrastruktury by se měli řídit doporučeními výrobců svých směrovačů k zajištění ochrany před útoky na *control plane*. Příklad je nastaveni *Control Plane Policying*.

Ochrana před útoky na směrovací protokol BGP typu DoS

Provozovatelé páteřní síťové infrastruktury by měli používat MD5 autentizaci BGP datagramů v souladu s [RFC 2385], případně reagovat na další nebezpečí popsaná v [RFC 4272].

Ochrana před IP squattingem pomocí filtrování

Provozovatelé páteřní infrastruktury by měli používat konkrétní vstupní i výstupní filtry pro BGP a odvozovat či alespoň kontrolovat jejich obsah v příslušných veřejných směrovacích databázích v souladu s [RFC 2650].

Ochrana před IP spoofingem

Provozovatelé páteřní infrastruktury ve spolupráci se svými zákazníky, kteří spravují koncové sítě, by měli filtrovat provoz směrem ke koncovým sítím pomocí *reverse-path* filtrů, pokud to je technicky možné v souladu s [BCP 38]. Smyslem opatření je vyloučit šíření DoS útoků s podvrženými zdrojovými adresami a všechny typy útoků přes reflektory z koncových sítí do ostatních AS. Provozovatelé koncových sítí by potom měli zabezpečit, že veškerý odchozí provoz obsahuje zdrojovou IP adresu z přiděleného rozsahu a nejedná se o podvrženou adresu.

Pasivní monitorování provozu a uchovávání dat

Provozovatelé páteřní infrastruktury a provozovatelé koncových sítí by měli pasivně monitorovat provoz na svých směrovačích nejlépe pomocí exportu NetFlow, IPFIX apod., případně alespoň *packet dump* a uchovávat zaznamenaná data zpětně několik dní. Za nutné minimum lze považovat 10 dní a pro snížení objemu dat lze použít NetFlow sampling až do poměru 1:200. Pasivní monitoring provozu by měl sloužit především k identifikaci útoků a provozovatelé síťové infrastruktury by měli mít přehled o provozu na úrovni zdrojové i cílové IP adresy, zdrojového i cílového portu, protokolu, směru komunikace (vstupní interface) a přesných časových údajů.

Aktivní reakce na probíhající útok v podobě zintenzivnění monitorování a sběru forenzních informací

Provozovatelé páteřní infrastruktury a provozovatelé koncových sítí by měli být schopni získat podrobné informace o provozu z konkrétního směru a na konkrétní adresy a měli by zachytit podezřelý datový tok a vyexportovat jej pro další analýzu ve formátu pcap.

Aktivní reakce na probíhající útok v podobě zablokování útoku

Provozovatelé páteřní infrastruktury i provozovatelé koncových sítí by měli být schopni zablokovat podezřelý datový tok či množinu datových toků na základě specifického obsahu v protokolových hlavičkách, minimálně však zdrojové a cílové IP adresy, TCP portu a flagů a UDP portu. Provozovatele páteřní infrastruktury můžou nabízet svým zákazníkům služby *remote-triggered blackhole* či jiný druh automatizace zahazování podezřelého provozu.

Odkazy

[BCP 38] P. Ferguson and D. Senie. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. Tech. rep. BCP 38, RFC 2827. May 2000. http://www.rfc-editor.org/rfc/rfc2827.txt.

[RFC 2385] A. Heffernan. Protection of BGP Sessions via the TCP MD5 Signature Option. Tech. rep. RFC 2385. Aug. 1998. http://www.rfc-editor.org/rfc/rfc2385.txt.

[RFC 2650] D. Meyer et al. Using RPSL in Practice. Tech. rep. RFC 2650. Aug. 1999. http://www.rfc-editor.org/rfc/rfc2650.txt.

[RFC 4272] S. Murphy. BGP Security Vulnerabilities Analysis. Tech. rep. RFC 4272. Jan. 2006. http://www.rfc-editor.org/rfc/rfc4272.txt.