Lühijuhend teenustõkestusrünnete ja hajutatud teenustõkestusrünnete (DoS ja DDoS) ennetamiseks ja lahendamiseks – tehnilised meetmed teenuste töö tagamiseks

Sissejuhatus

Teenustõkestusrünne (DoS) on tahtlik teenuse käideldavuse häirimine, mille võib tekitada süsteemi või võrguühendust üle koormates või süsteemi muul moel kahjustades. Hajutatud teenustõkestusrünnete (DDoS) toimepanemiseks, kasutatakse sihtsüsteemi või sihtvõrgu liikluse mahu oluliseks suurendamiseks suurt arvu ründavaid süsteeme (näiteks zombivõrke). DDoS rünnete käigus koormatakse võrgus asuvad teenused või nende taga olev infrastruktuur sissetuleva võrguliiklusega üle. Tihti kasutatakse rünnete läbiviimiseks ja teenuse töö katkestamiseks ära ka teadaolevaid seadmete tööd peatavaid turvanõrkuseid. Nii DoS kui DDoS ründe puhul võib olla tulemuseks teenustele ligipääsu puudumine nii oma töötajatele kui ka välistele klientidele.

Tehnilised meetmed

Rakendused / teenused

- Rakendustes võib esineda turvanõrkuseid, mis lubavad süsteemi vastu (D)DoS rünnete läbiviimist. Selle vältimiseks veendu, et kasutuselolevad rakendused kasutavad tarkvara uusimat versiooni ning paigaldatud on kõik saadaolevad turvauuendused. Organisatsioonispetsiifilistele rakendustele tuleks tellida majaväline turvatestimine, kindlustamaks, et rakenduses ei esineks ühtegi turvanõrkust. Nende ilmnemisel tuleb rakenduse arendajal teha vastavad muudatused turvanõrkuse eemaldamiseks.
- Võimalusel paigalda rakenduse-spetsiifilised turvaseaded, mis muudavad selle (D)DoS rünnete suhtes vastupidavamaks ja suuremat koormust taluvamaks. Näiteks veebilehtede optimeerimine, XML-RPC funktsiooni keelamine WordPressis või tsoonide ülekandmise keelamine DNS serverites.

- Rakenda serveripõhistes rakendustes turvameetmed. Üks populaarsemaid näiteid on Apache: rakenda mod_evasive, mod_reqtimeout ja mod_security.
- Muuda veebilehed võimalusel staatiliseks või kasuta veebipuhvrit (webcache). Staatiliste lehtede laadimine nõuab oluliselt vähem laadimisjõudlust kui andmebaasipäringute teostamine või dünaamiliselt genereeritud lehtede laadimine. Alternatiivne variant on hoida pidevalt uuendatuna dünaamilise lehe põhjal loodud staatilist versiooni, et ründe korral kiiresti staatilise ümber lülituda.
- Kaitse veebivorme CAPTCHA abil ennetamaks või aeglustamaks veebilehtede vastu läbiviidavaid automatiseeritud ründeid.
- Jaga oma võrgus asuvad teenused erinevate seadmete, teenusepakkujate või võrkude vahel. Näiteks paigalda veebileht teise serveri peale kui näiteks e-maili teenus, hoia DNS serverid erinevates võrkudes. Sellega kindlustad ühe teenuse vastu suunatud ründe puhul teiste teenuste jätkusuutliku toimimise.

Serverid

- Tõsta serverite turvataset tugevdamismeetmeid (*hardening*) kasutades:
  - ✓ Kindlusta, et nii operatsioonisüsteem kui ka serveri-spetsiifiline tarkvara on alati uuendatud ning kõik saadaolevad turvapaigad on paigaldatud.
  - ✓ Lülita välja/ keela kõik võrguteenused mis pole kasutusel ning milleks vajadus puudub ning sulge kõik kasutuseta pordid.
- Rakenda nii Windowsi kui Linuxi serveritele TCP/IP pinu (stack) tugevdamise meetodeid:
  - ✓ SYN-floodi vastaseks kaitseks luba Windowsil SynAttackProtect. Linuxil on olemas sarnane kaitsevõimalus SYN-cookies või SYN-cache kasutamisel. Sellise kaitse rakendamine on pigem tõhusam võrguperimeetrile lähemal asuvatele seadmetele kui serveritele endile.
- Võimalusel kasuta pahaloomulist liiklust tekitavate IP aadresside tuvastamiseks ja blokeerimiseks veebitulemüüri (Web Application Firewall/WAF):
  - ✓ WAF võib olla kasutusel nii võrguseadmena, serveri pistikprogrammina või isegi välise pilvepõhise teenusena.

- ✓ WAF-i võib seadistada blokeerimaks kahtlustäratav ja/või pahaloomulist käitumist ilmutav IP aadress.
- ✓ WAF suudab blokeerida ka teisi ründeid, näiteks XSS ja SQL süstimist (injection).
- ✓ NB! WAF kasutamine nõuab serverilt lisavõimsust. Sõltuvalt WAF eesmärgipärastest tegevustest võib see avaldada mõju teistele samal serveril käitatavatele teenustele.

- Kasuta erinevate teenuste jaoks erinevaid servereid. Näiteks ära käita nii oma meiliteenust kui ka veebiteenuseid samal füüsilisel serveril.

Võrk

- Veendu, et kõik võrguseadmed kasutavad uusimat tarkvara ja püsivara versiooni ning kõik ajakohased turvauuendused on paigaldatud.
- Maksimaalse kaitse taseme saavutamiseks kasuta mitmekihilist turvet, sealhulgas pääsuloendeid (Access Control List/ ACL), tulemüüre, WAF, koormusejaotureid ja võimalusel ka spetsiifilisi (D)DoS ründeid tuvastada ja peatada võimaldavaid seadmeid.
- Veendu, et infrastruktuuril on piisavalt võimsust. Võrdluseks on soovitav kasutada keskmist ning tipphetke töövõimsust. Võrdluse põhjal saab määrata nii riskiprofiili kui ka vajamineva reservi võimsuse: piisava WANühenduse läbilaskevõime, piisava jõudlusega serverid, tulemüürid ja kommutaatorid (switchid).
- „Kõik-ühes“ seadmetes on IDS/IPS funktsionaalsus tihti juba tarkvarasse eelnevalt lisatud. Seda funktsionaalsust tuleks rakendada erinevates süsteemides või riistvara moodulites, nii et neid (D)DoS rünnete puhul kiiresti üle ei koormataks.
- Kasuta eraldi tulemüüri. Paigalda ruuter selle tulemüüri ette ja internetiteenuse pakkuja ruuteri vahele. Mitmed järgnevatest toimingutest on efektiivsemad, kui kasutada tulemüüri asemel ruuterit:
  - ✓ Seadista pääsuloend (ACL) mis reguleerib liiklust IP aadressi või pordi numbri alusel. Luba sissetulev liiklus ainult protokollidele mis on vajalikud Sinu võrguteenuste jaoks. Tavalise veebiserveri jaoks on TCP/80 ja TCP/443 pordid piisavad.

- ✓ Juhul kui puudub vajadus spetsiifiliste teenuste jaoks mis vajavad UDP transpordiprotokolli, näiteks DNS pordil UDP/53, blokeeri UDP täisulatuses.
- ✓ Blokeeri kahtlased lähtepordid, näiteks päringud portidelt 53 (DNS), 80 (HTTP), 443 (HTTPS), 1900 (uPnP), 19 (chargen) ja 123 (NTP).
- ✓ ACL võib seadistada kasutama ka libanimekirju, mis võivad näiteks sisaldada IP aadresse mida ei tohiks päringuteks kasutada. Nende nimekirjade kasutamisel on oluline ka nimekirjade järjepidev uuendamine.
- ✓ Mõned tulemüürid toetavad lähteaadressi filtreerimist IP aadressi reputatsiooni baasil (IPRF), mille abil on võimalik pahaloomulike IP aadresside blokeerimine. Juhul kui kasutusel olev tulemüür võimaldab IPRF teistamist, tuleks see kindlasti kasutusele võtta.
- ✓ Võimalusel rakenda uRPF (Unicast Reverse-Path Forwarding) funktsiooni IP võltsimise ennetamiseks. uRPF kasutab IP aadressi päritolu valideerimiseks ja kinnitamiseks, et pakett pärineb ka tegelikult võrguühendusest, kust ta väidab ennast tulevat, marsruuditabelit (routing table). See võltsimisevastane tehnika on väga efektiivne staatilisi marsruute kasutavates võrkudes. Dünaamilist marsruutimiprotokolli kasutavates võrkudes on lahtine (loose) uRPF parem variant ning sellise variandi puhul kontrollib uRPF vaid IP paketi pärinemist sellele vastava IP aadressi marsruuditabelis.
- ✓ o Võimalusel rakenda sekundis tehtavate päringute arvu piiramist IP aadressi kohta (rate-limiting), maksimumpäringute arvu määramiseks saad taas kasutada keskmist päringute arvu ning päringute arvu tipphetkel. Päringute arvu piiramist saab kasutada ka konkreetsele võrgule maksimumkiiruse määramiseks, näiteks saab ka piirata portide 53 ja 123 liiklust 10 MB/s, eeldusel et need pordid vajavadki väikest läbilaskevõimet.
    - o Segmenteeri võrk nii, et ühe komponendi vastu suunatud ründed (näiteks meiliserveri) ei mõjuta teisi võrgus asuvaid komponente (näiteks LAN). Serverid paigutatakse nende eraldamiseks sisevõrguliiklusest tihti perimeetritsooni (Demilitarized Zone / DMZ).

- ✓ (D)DoS ründe korral on võimalik eraldada sihikule võetud teenused ülejäänud võrgust või suunata ründeliiklus tupikusse (blackholing või NULL-ruutimine). mille rakendamisel ei mõjuta rünne enam ülejäänud võrgu toimimist. Puuduseks on siiski sihikule võetud teenuse kättesaamatus. Mahtrünnete puhul tuleb NULL-ruutingu rakendamiseks pöörduda oma internetiteenuse pakkuja poole.
- ✓ Veendu, et autoriteetsed DNS serverid on eraldatud rekursiivsetest/ puhverserveritest.
- ✓ Võimalusel kasuta tagasüsteemide (*back-end*) koormuse vähendamiseks TLS mahalaadimis-seadmeid (*TLS off-loader*).

- Kasuta päringute jagamiseks erinevate serverite vahel koormusjaoturit *(load balancer*). SYN küpsiste kasutamisel on võimalik neid koormusjaoturi poolt rakendada serveritele tekkiva koormuse jaotamiseks. Samal eesmärgil on võimalik kasutada ka pöördproksi (*reverse proxy*) serverit, mis veebiserveri koormust vähendada aitab ning mille abil on võimalik blokeerida ka pahaloomulist HTTP liiklust.
- Juhtudel kus asutuses/ ettevõttes ei ole erinevatel põhjustel iseseisvalt ülalmainitud meetmete rakendamine on soovitatav pöörduda teenuse sisseostmiseks internetiteenusepakkuja, majutusteenusepakkuja ja või kolmandate osapoolte poole, kes (D)DoS kaitset teenusena pakuvad.

Kasulikke nõuandeid

- Vähenda oma nimeserveri DNS kirjete eluiga (Time To Live/ TTL). See võimaldab vajadusel kiiret teisele IP aadressile ülekolimist.
- Uuri IPv4 puhul kas kasutatavad kaitsemeetmed on vajalikud ja rakendatavad ka IPv6 puhul.
- Juhul kui Su teenused on suunatud ainult Eesti kasutajatele, on võimalik (D)DoS ründe korral pöörduda oma internetiteenuse pakkuja poole ajutiseks liikluse piiramiseks kõikidest teistest asukohtadest jättes teenuse kättesaadavaks vaid Eesti kasutajatele.
- Võimalusel testi oma võrkude vastupidavust (D)DoS rünnetele välistest võrkudest. Pea meeles, et vastupidavuse testimiseks välisvõrkudest tuleks

probleemide vältimiseks testide läbiviimisest teavitada ka oma internetiteenuse pakkujat või CERT-EE-d.

- Kontrolli, kas TLSi kasutavatel süsteemidel on võimalik keelata TLS ümberkõlastus (*TLS renegotiation*). Juhul kui seda pole võimalik keelata, seadista mahupiirang ümberkõlastustele sessiooni kohta TLS ümberkõlastusrünnete vältimiseks.
- Saada võimalikult palju võrgulogidest SNMP-d kasutades eraldiseisvatesse logiserveritesse vältimaks põhiserverite ülekoormatust ründe puhul. Juhul kui võrguvoo (netflow) logimine ründe ajal kulutab ründe ajal liiga palju ressursse tuleks suurendada diskreetimissagedust (*sampling rate*), näiteks 1:10, 1:100, 1:1000.
- Võimalusel logi DNS päringuid. See võib olla kasulik ründaja kohta info saamiseks, kui ründaja üritab monitoorida, kas rünne on edukas või mitte.
- Võimalusel teosta võrguteenuste seiret mitmest asukohast sealhulgas välisvõrgust. Teenuste *frontend* monitooringu puhul välisvõrgust on võimalik tuvastada ka teenuste taga oleva *backendi* toimimine.
- Veendu, et ettevõtte süsteeme ei kasutata ära teiste asutuste vastu suunatud (D)DoS rünnete läbiviimiseks. Kontrolli regulaarselt, et ükski ettevõtte arvuti poleks liidetud zombivõrguga ning ettevõtte serverid poleks seadistatud nii, et neid saaks ära kasutada peegeldus- ja võimendusrünnete läbiviimiseks. Näiteks valesti seadistatud Memcache süsteemid võimaldavad UDP ummistusrünnete võimendamist.
- Blokeeri väljuv võrguliiklus kui pakettide lähteaadressid on võltsitud.

Välised teenusepakkujad

- Juhul kui Su võrgukeskkond ei ole piisavalt võimas suuremahuliste (D)DoS rünnete tõrjumiseks on võimalik kasutada sisulevivõrku (Content Distribution Network/ CDN). See suunab ründeliikluse (ja ka legitiimse liikluse) nii, et see jaotub CDN võrgus. CDN teenuste osutajad pakuvad suurt võrgumahtu ning on võimelised ka (D)DoS ründeid tuvastama ja blokeerima. CDN teenuste osutajal on võimalus vahetada kodulehe esileht ka ajutise lehe vastu, kus kuvatakse info lehe ajutise kättesaamatuse kohta. Oluline on meeles pidada, et CDN teenuse osutajad jaotavad võrguteenuste liikluse väljaspool asukohariiki

asuvate serverite vahel ning see võib olla vastuolus ettevõtte/ asutuse andmekaitse kordade ja kohalike seaduste ja määrustega ning seetõttu tuleks enne teenuse tellimist konsulteerida ettevõtte juristi või andmekaitsespetsialistiga.

- Lisavõimalus (D)DoS rünnete vastaseks kaitseks on kasutada kommerts (D)DoS kaitse teenust, mille puhul toimub samuti võrguliikluse ümbersuunamine läbi teenusepakkuja serverite. Viimased asuvad suure tõenäosusega väljaspool Eestit ning see võib olla vastuolus ettevõtte/ asutuse andmekaitse kordade ja kohalike seaduste ja määrustega ning ka sel juhul tuleks enne teenuse tellimist konsulteerida ettevõtte juristi või andmekaitsespetsialistiga.

(D)DoS rünnetest teavitamine

(D)DoS rünnetest on võimalik teavitada Riigi Infosüsteemi Ameti intsidentide käsitlemise osakonda (CERT-EE), kes omakorda võtab ühendust välismaise teenusepakkujaga, kelle aadressi(de)lt rünne pärineb ning lähteriigi riikliku infoturbemeeskonnaga. Intsidendist sujuvamaks lahenduseks on vaja edastada piisavalt logitud informatsiooni, mille alusel teenusepakkuja omalt poolt juhtumit lahendama ja uurima saab asuda:

- ✓ Ründe ajaline kestus, sealhulgas täpne alguse ja lõpu aeg
- Ründe maht: pakettide arv sekundis (packets-per-second) ja läbilaskevõime (bits-per-second), pakettide suurus.
- Liikluse tüüp (ICMP, DNS, TCP, UDP)
- Ründe lähte- ja sihtpunktide IP aadressid ja pordid
  Võimalusel PCAP-id või netflow andmed

Juhend on koostatud Hollandi Riikliku Küberkaitsekeskuse juhendi põhjal ning muudetud vastamaks infoturbe korraldusele Eestis!