Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Technische maatregelen voor de continuïteit van onlinediensten

Bescherm uw eigen infrastructuur tegen (D)DoS-aanvallen

Factsheet FS-2016-04 | versie 1.0 | 14 maart 2016

Het NCSC adviseert om technische maatregelen te treffen om uw organisatie tegen de verschillende vormen van (D)DoS-aanvallen te beschermen. Deze aanvallen kunnen de ICT en de daarvan afhankelijke werkzaamheden van uw organisatie verstoren. Dit kan leiden tot (imago)schade. Het vormt een reële dreiging voor organisaties die onlinediensten verlenen, zoals websites.

Doelgroep

Systeembeheerders, netwerkbeheerders en informatiebeveiligers van organisaties die onlinediensten verlenen, zoals websites.

Aan deze factsheet hebben bijgedragen:

De Belastingdienst, Capgemini Infrastructure Services, de NaWas (onderdeel van NBIP), Schuberg Philis, SURFcert en andere domeinexperts.

Achtergrond

Bij een *(Distributed) Denial-of-Service ((D)DoS)*-aanval wordt de capaciteit van onlinediensten of de ondersteunende servers en netwerkapparatuur aangevallen door deze te overbelasten of te overladen met netwerkverkeer. Ook kan er misbruik worden gemaakt van fouten in software waardoor ondersteunende apparaten onbeschikbaar worden. Het resultaat is dat deze diensten slecht of helemaal niet meer bereikbaar zijn voor uw medewerkers of klanten. Meer informatie over (D)DoS-aanvallen en (organisatorische) maatregelen vindt u in de factsheet **Continuïteit van onlinediensten**.[1]

Wat adviseert het NCSC?

Het NCSC adviseert het treffen van meerdere technische maatregelen om uw infrastructuur te beschermen tegen (D)DoS-aanvallen. **Bepaal op basis van risicomanagement en technische analyses de inzet van verschillende maatregelen uit Tabel 1.**

Welke maatregelen u zelf kunt toepassen, hangt af van welk deel van een dienst u zelf beheert. Beheert u bijvoorbeeld een applicatie maar niet de onderliggende server, dan kunt u alleen maatregelen treffen voor die applicatie. De maatregelen in Tabel 1 zijn volgens dit onderscheid ingedeeld. Is uw organisatie verantwoordelijk voor het aangegeven onderdeel? Dan zijn de daar genoemde maatregelen voor uw organisatie bedoeld.

[1] https://www.ncsc.nl/actueel/factsheets/factsheet-continuiteit-van-online-diensten.html

Tabel 1 **Technische maatregelen**

Applicaties/diensten

- Applicaties kunnen kwetsbaarheden bevatten die een (D)DoS van de applicatie of het systeem waarop de applicatie draait kunnen veroorzaken. Let er daarom op dat de applicaties die u gebruikt, voorzien zijn van de recentste beveiligingsupdates. Laat uw maatwerkapplicaties testen op kwetsbaarheden en repareer gevonden kwetsbaarheden.
- Onderzoek welke applicatiespecifieke instellingen er mogelijk zijn om ervoor te zorgen dat een applicatie bestendig is tegen een (D)DoS-aanval. Voorbeelden zijn het optimaliseren van websites, het uitschakelen van de XML-RPC-functionaliteit in WordPress of bij DNS-servers het uitschakelen van zone-transfers.
- Bij sommige serverspecifieke software kunt u specifieke maatregelen[2] toepassen. Apache is een voorbeeld: pas hier mod_evasive[3], mod_reqtimeout[4] en ModSecurity[5] toe.
- Overweeg om voor uw websites gebruik te maken van statische pagina's of een *webcache*. Het laden van statische pagina's vergt minder rekenkracht dan het uitvoeren van een database query of het laden van een dynamisch gegenereerde pagina.
- Bescherm webformulieren met een CAPTCHA[6] om geautomatiseerde aanvallen hierop te vertragen.
- Spreid uw onlinediensten over verschillende componenten, providers of netwerken. Bij een aanval worden dan niet alle diensten van uw organisatie getroffen. Draai bijvoorbeeld uw website op een andere server dan uw mail.

Servers

- Verhoog het beveiligingsniveau van uw servers door *hardening*maatregelen[7] te treffen:
  - Zorg dat de besturingssystemen van uw servers en serverspecifieke software altijd voorzien zijn van de recentste updates.
  - Schakel alle niet-gebruikte en overbodige netwerkdiensten uit en sluit alle niet-gebruikte poorten.
- Configureer de TCP/IP-stack van zowel Windows Server[8] als Linux[9] met een aantal hardeninginstellingen.
  - Om u te beschermen tegen een SYN-flood[10] kunt u op Windows bijvoorbeeld *SynAttackProtect* inschakelen. Op Linux kan dezelfde soort bescherming worden verkregen door SYN-cookies of een SYN-cache. Over het algemeen is het beter om dit soort bescherming eerder in het netwerk te plaatsen, op hiervoor geschikte netwerkapparatuur, dan op de servers zelf.[11]
- Overweeg het gebruik van een Web Application Firewall (WAF) om aanvallen te herkennen en IP-adressen te blokkeren.
  - Een WAF kan zowel een netwerkcomponent zijn als een serverplugin of externe clouddienst.
  - Een WAF kan ingesteld worden om IP-adressen te blokkeren wanneer die verdacht verdrag vertonen.
  - Een WAF kan ook andere aanvallen tegenhouden, zoals XSS en SQL-injectie.
  - Let op! Het gebruik van een WAF vergt extra rekenkracht van uw server. Afhankelijk van de complexiteit van de werkzaamheden van een WAF, kan dit impact hebben op alle andere diensten die hiermee worden ontsloten.
- Gebruik verschillende fysieke servers voor verschillende diensten. Draai bijvoorbeeld uw mail- en web-diensten niet op dezelfde fysieke server.

Netwerk

- Zorg dat uw netwerkapparatuur altijd wordt voorzien van de recentste updates (firmware en software).
- Een ideale verdediging bestaat uit meerdere lagen van bescherming, waaronder een router met ACL, een firewall, een WAF, een loadbalancer en, eventueel, gespecialiseerde (D)DoS-filters om aanvallen te detecteren en te weren.
- Zorg dat uw infrastructuur voldoende capaciteit heeft. Gebruik een baseline om gemiddeld en piek werklasten vast te stellen. Bepaal uw risicoprofiel en reserveer aan de hand daarvan voldoende capaciteit: voldoende WAN/ISP-bandbreedte, servers, firewalls en switches.
- In alles-in-een-netwerkapparatuur kan het zijn dat IDS/IPS-systemen softwarematig wordt afgehandeld. Overweeg om dit soort systemen via aparte systemen of hardwaremodules te implementeren zodat die bij een (D)DoS-aanval minder snel overbelast raken.
- Maak gebruik van een dedicated netwerkfirewall. Om deze firewall te beschermen tegen overbelasting, kunt u tussen de firewall en uw internetprovider een router plaatsen. Een deel van de onderstaande maatregelen kan namelijk efficiënter door een router worden gedaan.
  - Configureer een *Access Control List (ACL)* die dataverkeer reguleert op basis van IP-adres of poortnummer. Sta alleen inkomend verkeer toe op

[2] https://httpd.apache.org/docs/trunk/misc/security_tips.html
[3] http://www.zdziarski.com/blog/?page_id=442
[4] https://httpd.apache.org/docs/trunk/mod/mod_reqtimeout.html
[5] http://www.modsecurity.org/documentation.html
[6] http://www.captcha.net/
[7] Voor Windows servers zie: https://technet.microsoft.com/en-us/library/cc526440.aspx.Voor Linux servers zie: https://www.sans.org/media/score/checklists/linuxchecklist.pdf.
[8] https://msdn.microsoft.com/en-us/library/ff648853.aspx
[9] https://wiki.archlinux.org/index.php/Sysctl#TCP.2FIP_stack_hardening
[10] https://tools.ietf.org/html/rfc4987
[11] https://tools.ietf.org/html/rfc4987#section-3.6

protocollen die noodzakelijk zijn voor uw onlinediensten.
  - Voor een standaard webserver is TCP/80 en TCP/443 voldoende.
  - U kunt UDP volledig blokkeren tenzij u specifieke diensten heeft die gebruikmaken van UDP (zoals DNS op UDP/53).
  - Verder kunt u verdachte bronpoorten blokkeren, zoals verzoeken vanaf poort 53 (DNS), 80 (HTTP), 443 (HTTPS), 1900 (uPnP), 19 (chargen) en 123 (NTP).
  - Uw ACL kan ook worden ingesteld met *bogon lists*[12]. Hierop staan IP-adressen die niet voor verzoeken gebruikt horen te worden. Zorg dat deze lijsten worden bijgehouden.
  - Bepaalde firewalls ondersteunen het filteren van bronnen op IP-reputatie (IPRF) waardoor mogelijke malafide IP-adressen kunnen worden geblokkeerd. Overweeg het gebruik hiervan.
  - Overweeg het gebruik van *Unicast Reverse-Path Forwarding (uRPF)* om IP-spoofing tegen te gaan. Hiermee wordt van IP-pakketten gecontroleerd of deze afkomstig zijn van een bron die volgens de routeringstabel bereikbaar is via de desbetreffende netwerkverbinding. Deze manier van anti-spoofing is zeer effectief in een netwerk met statische routes. In een netwerk met een dynamisch routeringsprotocol is *loose uRPF* een optie. Deze variant van uRPF controleert alleen of een IP-pakket afkomstig is van een IP-adres dat in de routeringstabel van de router voorkomt.
  - Overweeg het gebruik van *ratelimiting* om het aantal verzoeken per seconde per IP-adres te beperken. Gebruik hiervoor een maximum aantal dat gebaseerd is op een eerder vastgestelde baseline.[13] Ratelimiting kan ook worden toegepast om bepaalde netwerken van een maximale snelheid te voorzien. U kunt er ook voor kiezen om verkeer van poort 53 en 123 te ratelimiten op bijvoorbeeld 10MB/s gezien deze poorten slechts een relatief kleine hoeveelheid bandbreedte mogen vragen.
- Segmenteer uw netwerk zodat aanvallen op één component (bijvoorbeeld mailserver) andere componenten (bijv. het lokale netwerk) niet verstoren. Vaak worden servers van intern verkeer gescheiden door ze in een *Demilitarized Zone (DMZ)* te plaatsen.
  - U kunt er tijdens een aanval voor kiezen om de diensten die worden aangevallen af te scheiden van de rest van het netwerk of naar een dood punt te leiden (*blackholing* of *NULL-routering*). De rest van het netwerk heeft dan ook geen last meer van de (D)DoS-aanval. Het nadeel is dat de aangevallen dienst voor iedereen onbereikbaar is. Voor volume-based aanvallen moet NULL-routering bij uw ISP plaatsvinden.
  - Zorg ervoor dat authorative DNS-servers en recursive/caching DNS-servers gescheiden zijn.
  - Overweeg het gebruik van een TLS-offloader om uw servers niet te belasten met cryptografische berekeningen.
- Verdeel het afhandelen van verzoeken over meerdere servers met een *loadbalancer*. Als u SYN-cookies gebruikt kan de load-balancer deze zelf afhandelen om uw servers te ontlasten. Een *reverse-proxy server* kan deze rol vervullen om de werklast van uw webservers te beperken. Tevens biedt dit de mogelijkheid om gecontroleerd kwaadaardig HTTP-verkeer te blokkeren.
- Om de werklast van uw webserver te beperken, kunt u ook een webcachingserver gebruiken die verzoeken op vaak benaderde, statische pagina's zelf afhandelt. Deze server moet zo dicht mogelijk bij de webserveromgeving worden geplaatst, dus achter loadbalancers en andere stateful apparatuur.
- Indien de bovengenoemde maatregelen onvoldoende zijn, kunt u ervoor kiezen om gebruik te maken van gespecialiseerde apparatuur om (D)DoS-aanvallen af te weren of om gebruik te maken van externe diensten (zie onder).

Overige

- Als uw eigen netwerkomgeving niet in staat is om grote (D)DoS-aanvallen af te weren, kunt u gebruik maken van een *Content Distribution Network (CDN)*. Hierdoor worden aanvallen (en ook legitiem verkeer) niet direct naar uw onlinediensten gestuurd maar via een omleiding die verspreid wordt over het netwerk van het CDN. Aanbieders van CDN's hebben veel netwerkcapaciteit en kunnen (D)DoS-aanvallen detecteren en mitigeren. Ook kan een CDN een tijdelijke pagina laten zien op het moment dat uw website niet bereikbaar is.
  - CDN's distribueren het voor uw applicatie bestemde verkeer via servers in het buitenland. Vooral privacy- en bedrijfsgevoelige gegevens kunnen door het inzetten van deze oplossing mogelijk niet conform wet- en regelgeving of bedrijfsbeleid worden verwerkt. Stem daarom de oplossingen van de dienstverlener af met deze complianceafhankelijkheden.
- Een ander manier om het mitigeren van (D)DoS-aanvallen uit te besteden is door gebruik te maken van commerciële (D)DoS-mitigatiediensten, een *scrubbingcentrum*. Als u hier gebruik van maakt, wordt inkomend verkeer tijdens een aanval geherrouteerd door het netwerk van het scrubbingcentrum. Hier worden (D)DoS-aanvallen afgeweerd met behulp van gespecialiseerde apparatuur.
  - Net zoals bij CDN's kan deze herroutering impact hebben op het naleven van regelgeving of bedrijfsbeleid rondom privacy- en bedrijfsgevoelige gegevens. Stem daarom de oplossingen van de dienstverlener af met deze complianceafhankelijkheden.
- Verlaag de TTL van uw domeinrecords. Hierdoor kunt u uw diensten snel migreren naar een ander IP-adres.
- Onderzoek of de maatregelen voor IPv4 ook nodig en aanwezig zijn voor IPv6.
- Wanneer de dienstverlening enkel geleverd wordt aan gebruikers binnen Nederland, kunt u overwegen om tijdens een (D)DoS-aanval het overige

[12] http://www.team-cymru.org/bogon-reference.html
[13] Zie de factsheet 'Continuïteit van onlinediensten' voor meer informatie over het vaststellen van een baseline: https://www.ncsc.nl/actueel/factsheets/factsheet-continuiteit-van-online-diensten.html.

verkeer door uw ISP te laten blokkeren. Hierdoor blijft de dienstverlening behouden voor gebruikers binnen Nederland.

- Overweeg het testen van uw weerbaarheid tegen (D)DoS-aanvallen als onderdeel van een *red/blue-teamoefening*. Voer dit soort tests uit vanaf externe netwerken om een realistisch beeld te krijgen van het netwerkpad dat gevolgd wordt tijdens een echte aanval. Stem altijd af met uw externe leveranciers, waaronder uw ISP en hostingprovider, en denk aan vrijwaringsverklaringen.
- Bekijk of het mogelijk is om TLS-renegotiation uit te schakelen op systemen waar TLS is toegepast. Indien deze optie niet uitgeschakeld kan worden, configureer dan een ratelimiter voor TLS-renegotiation per sessie. Dit voorkomt een (D)DoS-renegotiation-aanval.[14]
- Stuur logging van netwerkapparatuur zo veel mogelijk via SNMP naar externe logservers om te voorkomen dat die apparatuur onvoldoende reken- of opslagcapaciteit heeft tijdens een aanval. Als het loggen van netflow teveel capaciteit vergt tijdens een aanval, kunt u minder loggen, bijvoorbeeld elke tiende of honderdste flow.
- Indien u van een aanval aangifte bij de politie wilt doen, is het belangrijk om voldoende te hebben gelogd, waaronder:
  - een tijdlijn van de aanval inclusief start- en eindtijd;
  - de pakketgrootte, het aantal pakketten per seconde en bandbreedtegebruik;
  - het type verkeer (ICMP, DNS, TCP, UDP, etc.);
  - TCP- of UDP-flags die op de pakketten zijn gezet;
  - bron- en doel-IP–adressen en poort(en);
  - doelservices (web-, name-, mailserver, etc.);
  - doel-URL's;
  - HTTP-headers (user-agent, language, encoding, etc.);
  - dataverkeer en routeringsinformatie, bijvoorbeeld BGP;
  - welke mitigerende maatregelen er zijn getroffen; en
  - typerende PCAP's of netflowdata van de aanval.
- Overweeg om DNS-logs te bewaren. Deze zijn mogelijk relevant indien de aanvaller een DNS-verzoek doet voor of tijdens een aanval om te controleren of de aanval gelukt is.
- Overweeg of u de onlinediensten van buitenaf wilt monitoren. Door de frontend van uw onlinediensten van buitenaf te monitoren, kunt u vaststellen of de hele keten (backend) ook functioneert.
- Het is mogelijk om tijdelijk inkomend netwerkverkeer alleen toe te staan vanaf vertrouwde netwerken. Dit is een maatregel voor eigenaren van autonome systemen (AS'en), bijvoorbeeld uw internetprovider.
- Tref maatregelen om te voorkomen dat uw infrastructuur bijdraagt aan (D)DoS-aanvallen op andere organisaties.
  - Zorg dat er geen computers binnen uw organisatie deel uitmaken van een botnet.[15]
  - Let op dat uw servers niet kunnen worden gebruikt in reflectieaanvallen, bijvoorbeeld uw DNS-servers.[16]
  - Blokkeer uitgaand netwerkverkeer als het zich voordoet als verkeer uit een ander netwerk.

[14] Zie de 'ICT-beveiligingsrichtlijnen voor TLS' waar dit wordt aanbevolen https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html en https://community.qualys.com/blogs/securitylabs/2011/10/31/tls-renegotiation-and-denial-of-service-attacks voor meer informatie.
[15] Zie de factsheet 'Verlos me van een botnet' https://www.ncsc.nl/actueel/factsheets/factsheet-verlos-me-van-een-botnet.html.
[16] Zie de factsheet 'DNS-amplificatie' https://www.ncsc.nl/actueel/factsheets/factsheet-dns-amplificatie.html.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

FS-2016-04 | versie 1.0 | 14 maart 2016