Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Continuïteit van onlinediensten

Bescherm uw organisatie tegen (D)DoS-aanvallen

Factsheet FS-2013-01 | versie 2.0 | 14 maart 2016

Het NCSC adviseert om zowel technische als organisatorische 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.

Maak een overzicht van uw ICT-infrastructuur. Tref voor onderdelen binnen uw eigen beheer technische maatregelen. Maak voor overige onderdelen afspraken met de desbetreffende leverancier. Bereid uw organisatie voor op een aanval door middel van een duidelijke respons- en communicatiestrategie.

Doelgroep

IT-managers en andere verantwoordelijken voor informatiebeveiliging 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 *Denial-of-Service (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. In veel gevallen wordt dit soort aanvallen vanaf meerdere computers tegelijkertijd uitgevoerd. In dat geval heet het een *Distributed* DoS (DDoS)-aanval. Het effect voor uw organisatie is uiteindelijk hetzelfde dus worden beide soorten aanvallen in deze factsheet met één term benoemd: **(D)DoS**.

De belangrijkste feiten

1. Een (D)DoS-aanval kan uw onlinediensten verstoren.
2. Aanvallen worden steeds groter en complexer. Tegelijkertijd wordt het steeds makkelijker en goedkoper om aanvallen uit te voeren.
3. Ook kleine bedrijven, zoals webshops, kunnen worden afgeperst met behulp van (D)DoS-aanvallen.
4. Tref technische en organisatorische maatregelen om uw onlinediensten weerbaarder te maken.
5. Maak afspraken met uw ICT-leveranciers over hun (D)DoS-bescherming.

Een (D)DoS-aanval kan plaatsvinden op veel verschillende manieren.[1] Er zijn tientallen vormen van (D)DoS-aanvallen bekend die zich richten op de routering, specifieke netwerkservices of het overbelasten van de rekencapaciteit van specifieke apparatuur. Aanvallen zijn tegenwoordig meestal 'multi-vector'. Meerdere aanvalstechnieken worden gelijktijdig of achter elkaar ingezet tijdens de aanval. Ook passen aanvallers soms hun tactieken aan tijdens een aanval aan. Het blokkeren van één aanval leidt dan tot een ander aanvalspatroon.
Er zijn verschillende kwaadwillenden die (D)DoS-aanvallen kunnen uitvoeren.[2] **Hacktivisten**, waaronder het hacktivistencollectief 'Anonymous', gebruiken (D)DoS-aanvallen om een politieke boodschap af te geven. **Criminelen** zetten dit soort aanvallen in om geld te verdienen door bedrijven af te persen. Zelfs kleine bedrijven hebben hier last van. Ook worden aanvallen ingezet om andere criminele activiteiten te verhullen. **Statelijke actoren** gebruiken (D)DoS-aanvallen tegenstanders het zwijgen op te leggen. **Scriptkiddies** gebruiken eenvoudige tools om aanvallen uit te voeren, soms zonder een duidelijke motivatie. **Gebruikers van de eigen diensten** voeren aanvallen uit om verschillende redenen. Voorbeelden zijn een ontevreden medewerker of een scholier die onder een toets probeert uit te komen.

Kwaadwillenden gebruiken diverse middelen en technieken om hun identiteit te verbergen. Hierdoor is de pakkans over het algemeen klein. Met **IP-spoofing** is het is mogelijk om netwerkverkeer aan te passen zodat het uit andere netwerken lijkt te komen. Vaak worden aanvallen uitgevoerd vanaf **botnets**, dit zijn netwerken van een groot aantal besmette computers die vanuit een centraal punt gestuurd worden. In plaats van uw netwerk rechtstreeks aan te vallen, gebruiken aanvallers ook **reflectie-aanvallen**. Hierbij vragen aanvallers meerdere middelen, zoals DNS-servers en uPnP-diensten op modems, om antwoord te geven op een verzoek. Dit antwoord wordt echter gestuurd naar het slachtoffer. Tegenwoordig kunnen kwaadwillenden gebruikmaken van **betaalde (D)DoS-diensten**. Zonder enige kennis kan men hiermee voor weinig geld en met een druk op de knop een grootschalige aanval uitvoeren.

De meeste aanvallen waarover geschreven wordt, zijn op websites. In principe is elke dienst op internet kwetsbaar.
- Applicaties worden aangevallen door deze te overbelasten met veel verzoeken. Hierdoor kunnen geen legitieme gebruikers worden bediend. Ook kunnen 'dure' verzoeken worden uitgevoerd. Een voorbeeld hiervan is het laden van een webpagina die veel gegevens uit een database moet halen. Een steeds populairder type aanval is de *slow HTTP post* aanval. Door periodiek onvolledige verzoeken naar een server te sturen, worden verbindingen opgezet en heel lang opengehouden terwijl die server op de rest van het verzoek wacht. Deze aanvallen zijn lastig te detecteren omdat de verzoeken legitiem lijken te zijn.
- Servers worden overbelast met aanvallen op het netwerk- of transportniveau. Een voorbeeld hiervan is de zogenaamd *TCP SYN-flood* waarbij de server meerdere verzoeken ontvangt om een TCP-verbinding op te zetten. De server reserveert alvast de nodige middelen voor iedere connectie totdat alle middelen gereserveerd zijn. Hierna kunnen gebruikers geen verbinding meer maken.
- Sommige aanvallen zijn gericht op een netwerk of netwerkapparatuur. Vaak richt dit soort aanvallen zich op het verbruiken van de beschikbare netwerkbandbreedte of de verwerkingscapaciteit van de netwerkapparatuur. Ook kan netwerkapparatuur te maken krijgen met dezelfde aanvallen als servers, zoals TCP SYN-flood.
- Als uw applicatie een met TLS beveiligde verbinding biedt, kunnen aanvallen zich hierop richten. Aanvallers kunnen hierdoor relatief veel rekenkracht van uw server vragen zonder zelf veel te doen.

Wat is het probleem?

Een (D)DoS-aanval kan de ICT en de daarvan afhankelijke werkzaamheden van uw organisatie verstoren. Dit vormt een reële dreiging voor alle organisaties met onlinedienstverlening, zoals websites, waarvan de continuïteit van belang is. Afhankelijk van het type aanval kan uw organisatie geen gebruik meer maken van ICT-systemen doordat deze traag of onbereikbaar zijn. Omdat uw onlinedienstverlening verstoord wordt, kunnen klanten niet meer geholpen worden.

Over het algemeen is de slagingskans en schade van een (D)DoS-aanval vrij groot. Imagoschade voor de meeste organisaties het grootste zorgpunt, naast de kosten van mitigatie en verloren inkomsten tijdens een aanval. Verder kan een aanval ervoor zorgen dat uw organisatie haar afspraken niet na kan komen wat tot andere problemen kan leiden.

[1] Deze factsheet richt zich enkel op opzettelijke aanvallen. "Natuurlijke" factoren, zoals buitengewoon veel gebruikers tegerlijkertijd op uw website, worden bewust buiten beschouwing gelaten.
[2] Meer informatie over actoren en motieven vindt u in het Cybersecuritybeeld Nederland: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-5.html.

Wat adviseert het NCSC?

Het NCSC adviseert om zowel technische als organisatorische maatregelen te treffen om uw organisatie te beschermen tegen de verschillende vormen van (D)DoS-aanvallen. Bespreek de onderstaande adviezen met de relevante stakeholders binnen uw organisatie, waaronder die personen die verantwoordelijk zijn voor het beheer en de continuïteit van uw onlinediensten.

Advies 1: maak een overzicht van en monitor uw infrastructuur

Maak een duidelijk overzicht van uw infrastructuur. Welke onlinediensten biedt uw organisatie aan en welke platformen en infrastructuur zijn hiervoor nodig? Welke hiervan zijn gevoelig voor een (D)DoS-aanval? Zijn er bepaalde diensten die belangrijker zijn dan andere? Wat is bijvoorbeeld de impact op uw organisatie als een bepaalde dienst niet meer beschikbaar is? Welke netwerksegmenten zijn er? Is alles binnen uw eigen beheer, of zijn er servers of diensten uitbesteed aan derden? Denk hierbij ook aan uw internetprovider en aan onlinediensten van derden. Breng de hele keten van uw dienstverlening in kaart zodat u deze adequaat kunt beschermen.

Heeft u een actueel overzicht van uw infrastructuur, stel dan een baseline vast van 'normaal' gedrag: de hoeveelheid websiteverkeer, gebruikelijke tijdstippen, type verkeer, gebruikte poorten, enzovoort. Stel de baseline vast op basis van een representatieve periode. Het is geen gemiddelde, maar een bandbreedte waarbinnen wordt gedefinieerd welk netwerkverkeer en systeemgedrag 'normaal' is. Voor infrastructuur binnen uw eigen beheer kunt u gebruikmaken van systeemlogs en statistieken van netwerkapparaten. Indien u diensten uitbesteed heeft aan derden, werkt u samen met die partijen aan oplossingen.

Nadat een baseline is vastgesteld, kan inkomend en uitgaand verkeer worden gemonitord. Dit betekent dat er geautomatiseerd wordt gekeken of de metingen significant afwijken van de vastgestelde baseline. Het type (D)DoS-aanval en de werking van de tegenmaatregelen kan zo geanalyseerd worden. Zonder geschikte monitoringsystemen is het lastig om aanvallen te onderscheiden van legitiem verkeer of van technische storingen. Houd ook rekening met voorspelbare afwijkingen van de baseline, bijvoorbeeld reclamecampagnes of jaarlijkse momenten wanneer er veel legitieme gebruikers worden verwacht.

Advies 2: ga bij elke externe leverancier na welke (D)DoS-maatregelen al genomen zijn en wat daar de afspraken over zijn

Maak gebruik van het bij Advies 1 gemaakte overzicht om bij alle externe leveranciers over hun (D)DoS-bescherming te informeren. Wat is hun aanpak bij (D)DoS-aanvallen en wat zijn de contractuele afspraken hierover?

Neem contact op met iedere externe leverancier en verifieer:

- de contactgegevens van personen die gebeld kunnen worden tijdens een aanval;
- welke maatregelen en ondersteuning zij bieden om aanvallen te mitigeren en wat daar de gevolgen van kunnen zijn. Het kan bijvoorbeeld zijn dat uw hostingprovider *blackholing/null-routering* gebruikt tijdens een aanval. Hierbij wordt al het verkeer voor uw systeem gerouteerd naar een 'zwart gat' om de rest van hun infrastructuur te beschermen;
- welke maatregelen zijn genomen om uw diensten te beschermen tegen aanvallen op andere klanten van de leverancier. Als u bijvoorbeeld gebruikmaakt van gedeelde hostingmiddelen, kunnen aanvallen op andere klanten ook uw diensten negatief beïnvloeden;
- indien er sprake is van gedeelde infrastructuur: met welke andere (type) klanten deelt u de infrastructuur?
- welke anti-spoofingmechanismes worden gebruikt;[3]
- welke detectiemechanismes gebruikt worden om (D)DoS-aanvallen in een vroeg stadium te detecteren;
- welke afspraken er gemaakt zijn voor het installeren van beveiligingsupdates;
- hoe het met de systeem- en netwerkcapaciteit van uw onlinediensten gesteld is.

Advies 3: ga bij alle interne infrastructuur na welke maatregelen al genomen zijn en, pas technische maatregelen toe indien nodig

Het NCSC adviseert om meerdere overlappende maatregelen te treffen om de weerbaarheid van uw interne infrastructuur tegen (D)DoS-aanvallen te vergroten. Maak gebruik van het bij Advies 1 gemaakte overzicht om voor uw eigen infrastructuur vast te leggen welke maatregelen al getroffen zijn. Voor alle applicaties, servers of netwerkapparatuur waar er onvoldoende maatregelen zijn getroffen, informeer over de mogelijke technische maatregelen.

In de factsheet **Technische maatregelen voor de continuïteit van onlinediensten** vindt u een uitgebreide lijst van technische maatregelen.[4] Overweeg het treffen van maatregelen op deze lijst, indien deze nog niet getroffen zijn. Afhankelijk van de mate van uitbesteding van uw ICT kunnen sommige maatregelen niet worden toegepast zonder medewerking van derden.

Advies 4: bereid uw incidentrespons voor en denk na over failoverscenario's van onlinediensten

Maak een draaiboek voor tijdens een (D)DoS-aanval. Beschrijf hoe een aanval herkend wordt en wie welke stappen neemt. Wie houdt bijvoorbeeld de tijdlijn en kenmerken van de aanval bij? Wie verzamelt de nodige gegevens om aangifte te doen (zie

[3] Internetproviders kunnen filtering toepassen volgens bekende standaarden, zoals BCP38: http://www.bcp38.info/, om gespoofd verkeer tegen te houden.

[4] https://www.ncsc.nl/actueel/factsheets/factsheet-technische-maatregelen-voor-de-continuiteit-van-onlinediensten.html

kader)? Overweeg om een gespecialiseerd team[5] in te richten dat autonoom optreedt tijdens dit soort incidenten.

Denk na over backup- en failoverscenario's van onlinediensten. Maak afspraken met externe dienstverleners over responsmechanismes en eventuele extra dienstverlening. Een voorbeeld is een simpele website die klanten laat weten dat er aan het probleem gewerkt wordt.

Overweeg het opzetten van alternatieve communicatiepaden die gebruikt kunnen worden tijdens een aanval. Hiermee blijft u in contact met uw belangrijke systemen en organisaties.

Advies 5: instrueer de communicatieadviseur van uw organisatie

Bepaal een communicatiestrategie voor uitingen naar de eigen medewerkers, klanten, leveranciers, overheid en andere stakeholders. Communicatie over (D)DoS-bestendigheid kan juist leiden tot (D)DoS-aanvallen. Het is te laat om tijdens een crisis te bepalen hoe gecommuniceerd gaat worden. Zorg ook dat een communicatieadviseur op hoofdlijnen weet wat de gevolgen zijn van een (D)DoS-aanval. Wat wordt eraan gedaan? Hoe lang kan het gaan duren? Waar kan men terecht voor meer informatie? Communiceer daarbij vooral geen onzekerheden of onjuistheden.

Aangifte doen

Het uitvoeren van een (D)DoS-aanval is een strafbaar feit waar gevangenisstraf of een boete voor kan worden opgelegd. Het is belangrijk om aangifte bij de politie te doen. Ook als de dader niet te achterhalen is, helpt het doen van aangifte om een beter beeld te geven van de omvang van dit fenomeen.

Indien u ervoor kiest om aangifte te doen, neemt u dan via 0900-8844 contact op met uw lokaal wijkteam voor het maken van een afspraak. Vraag of er een digitaal expert aanwezig kan zijn tijdens de aangifteprocedure. Neem uit uw monitoringsysteem de basisgegevens mee.[6]

[5] Bijvoorbeeld een Security Operations Centre (SOC) of Computer Security Incident Response Team (CSIRT).
[6] Zie de factsheet 'Technische maatregelen voor continuïteit' van onlinediensten voor een lijst van basisgegevens: https://www.ncsc.nl/actueel/factsheets/factsheet-technische-maatregelen-voor-de-continuiteit-van-onlinediensten.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-2013-01 | versie 2.0 | 14 maart 2016