CENTRE FOR
CYBER SECURITY
BELGIUM

Hoe je organisatie beschermen tegen een DDoS-aanval?

Adviezen om kleine en middelgrote organisaties te beschermen tegen DDoS-aanvallen

Publicatie – 05/05/2021

Een **Distributed Denial of Service** (DDoS)-aanval is een cyberaanval met als doel **het normale verkeer van een bepaalde dienst verstoren**. In organisaties en bedrijven kan dit een grote impact hebben op de werking. Het is dus van groot belang beschermd te zijn tegen DDoS aanvallen.

Deze aanbevelingen zijn opgemaakt door het **Centrum voor Cybersecurity België (CCB)**.

Het Centrum voor Cybersecurity België (CCB) is de nationale autoriteit voor cyberveiligheid in België. Het CCB is opgericht bij Koninklijk Besluit van 10 oktober 2014 en staat onder het gezag van de Eerste Minister. Vanuit de wettelijke opdracht tracht het organisaties te informeren en te adviseren inzake bescherming tegen DDoS-aanvallen.

Een Distributed Denial of Service (DDoS)-aanval is een cyberaanval met als doel het normale verkeer van een bepaalde dienst verstoren. Een mogelijks geval is dat de beschikbaarheid van een bepaalde dienst niet meer gegarandeerd kan worden. Deze dienst is dus gedurende een bepaalde tijd onbereikbaar, maar het gaat niet over een inbraak of het stelen van data. Er zijn verschillende types DDoS-aanvallen en deze variëren van complexiteit. Het fenomeen attack-as-a-service, waarbij non-technici cyberaanvallen kunnen 'bestellen' op het darkweb, wint ook bij DDoS aan populariteit.

Dit document is bedoeld als gids voor IT-verantwoordelijken in kleine en middelgrote organisaties en bedrijven om hen te informeren en adviseren over mogelijke beschermingsmaatregelen tegen een DDoS aanval. Hieronder wordt er gefocust op DDoS-aanvallen tegen het netwerk van een kleine en middelgrote organisatie, niet tegen een specifiek platform, website of andere online dienst. Het document heeft niet de ambitie om DDoS aanvallen te stoppen, maar tracht een organisatie voor te bereiden op en meer weerbaar te maken tegen DDoS-aanvallen. Deze gids bestaat uit acties die je als IT-verantwoordelijke van een kleine en middelgrote organisatie zelf kan nemen. De overzichtsfiche op het einde geeft een mooie samenvatting. We raden aan om dit overzicht af te drukken, in te vullen en ergens centraal op te hangen, zodat het actief kan worden gebruikt tijdens een DDoS aanval.

CENTRE FOR
CYBER SECURITY BELGIUM
Under the authority of the Prime Minister
Rue de la Loi, 16 - Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

CENTRE FOR CYBER SECURITY BELGIUM

Hoe kan ik mijn organisatie beschermen tegen DDoS aanvallen?

Voorbereiding

Ken je netwerk

Om je voor te bereiden op een cyberaanval is het belangrijk om je netwerk te kennen en te documenteren. Hoe ben je verbonden met het internet? Is dit rechtstreeks met de Internet Service Provider (kortweg ISP, bijvoorbeeld Telenet of Proximus) of via andere organisaties? Wie is jouw ISP en welk soort contract heb je? Welke diensten zijn verbonden met je netwerk?

We raden aan om een zo volledig mogelijke inventaris te maken van onder meer netwerktypologieën, externe en interne IP-adressen. Externe IP-adressen kunnen eenvoudig worden opgevraagd via https://whatismyipaddress.com/. Heel vaak is deze documentatie essentieel tijdens een aanval. Zorg er dus voor dat je deze kan opvragen tijdens de cyberaanval.

Incident response procedure

Een incident response procedure beschrijft wat er dient te gebeuren bij een cyberaanval. Essentieel tijdens een DDoS-aanval is een out-of-band communicatiekanaal hebben. Hiermee wordt een communicatiemiddel bedoeld waarvoor het netwerk niet nodig is. Enkele voorbeelden zijn: telefoon, WhatsApp, 4G, etc. Spreek ook duidelijk op voorhand af welke groep met welke middel gaat communiceren. Belangrijk is om offline (uitgeprint) een contactlijst te hebben van de mensen die die je kunnen helpen of die je moet informeren. Dit kan zowel intern (management, medewerkers, IT-dienst) als extern (ISP, security-expert, klanten) zijn.

Spreek goed af met je ISP wat zij kunnen doen in het geval van een DDoS-aanval. Dit kan bijvoorbeeld geo-blocking, verandering van publiek IP, packet scrubbing, etc. zijn. Bekijk zeker de bestaande contracten met je ISP, Cloud- en Hostingprovider op DDoS bescherming.

Checklist

De checklist is opgedeeld in twee delen. Het eerste deel zijn basisvoorbereidingen die aangeraden worden voor alle organisaties. Het tweede deel zijn meer geavanceerde voorbereidingen en meer technisch van aard.

- ☐ Splits het netwerk op volgens toepassing, activiteit of functie (administratieve diensten, productiesystemen, publieke website, externe gebruikers, externe diensten, interne gebruikers, interne bedrijfsdata, …). Zowel voor het bedrijfsnetwerk als clouddiensten.
- ☐ Installeer een netwerk firewall en pas de nodige regels toe op de internettoegang (“network-based”).
- ☐ Zorg dat ook op interne systemen, zoals servers en workstations een firewall actief is (“host-based”).
- ☐ Schakel ongebruikte diensten uit of filter deze uit het netwerk.
- ☐ Zorg voor automatische beveiligingsupdates van besturingssystemen, programma’s en routers.
- ☐ Wijzig het standaard wachtwoord op uw internetrouter en andere systemen
- ☐ Gebruik waar mogelijk diensten in de Cloud, bijvoorbeeld websites, maildiensten of andere online platformen zijn erg kwetsbaar als je lokaal op een server gaat hosten. Clouddiensten zijn door hun brede beschikbaarheid beter beveiligd.

CENTRE FOR
CYBER SECURITY BELGIUM
Under the authority of the Prime Minister
Rue de la Loi, 16 - Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

- ☐ Schakel tweestapsverificatie (2FA) in waar mogelijk. Schakel dit zeker in voor administrator accounts en voor gebruikers met extra of gevoelige privileges die speciale taken moeten uitvoeren, die gewone gebruikers niet hebben. Voor meer informatie zie: https://www.safeonweb.be/index.php/nl/gebruik-tweestapsverificatie

Geavanceerd:

- ☐ Doe regelmatig een netwerk scan: wat is bereikbaar via het internet?
- ☐ Filter functionaliteit actief op internetrouter of firewall.
- ☐ Valideer het gebruik van private IP-ranges: valideer of je netwerk gebruik maakt van geldige interne IP-adressering die globaal bepaald zijn (voorbeeld van conforme ranges: 192.168.0.0/24 172.16.0.0/16 en 10.0.0.0/8).
- ☐ Voorkom IP-spoofing (misbruik van IP addressen): dit kan door Unicast Reverse Path Forwarding (uRPF).
  Voor meer informatie zie:
  https://www.juniper.net/documentation/en_US/junos/topics/concept/unicast-rpf-understanding.html#:~:text=A%20unicast%20reverse%2Dpath%2Dforwarding,and%20checks%20the%20incoming%20interface.
- ☐ Laat enkel gekende en betrouwbare netwerk verkeer door: standaard alles blokkeren (standaard “deny all”) maak gebruik van allow-lijsten om enkel dit verkeer door te laten.
- ☐ Harden je router zo veel als mogelijk door volgende zaken uit te schakelen: IP-directe broadcast - HTTP configuraties - ICMP ping - IP source routing.

Identificatie

Probeer zoveel mogelijk informatie te verzamelen over de aanval. Om de impact van de DDoS te bepalen is het belangrijk om een lijst te maken van de getroffen systemen. Dit kan gebeuren op basis van klachten van gebruikers. Zorg zeker ook voor **technische validatie.** Welke applicatie-, systeem- of netwerkcomponent heeft er een hoge belasting en consumeert veel bandbreedte?

Mitigatie

Een zeer belangrijke partner bij het mitigeren van DDoS is de ISP (Internet Service Provider). Contacteer de ISP dus zo snel mogelijk, als je zeker bent dat het om een DDoS aanval gaat. Indien je dit wenst, kan er ook beroep worden gedaan op een cybersecurity expert. Geo-blocking op ISP-niveau of in meer geavanceerde firewalls kan de DDoS-aanval mitigeren. Hetzelfde geldt voor een verandering van publiek IP. Dit kan door de ISP gebeuren, maar in het geval van dynamische IP’s kan dit door de internet router 15-30 minuten uit te schakelen.
Indien er schade is, raden wij aan om een klacht in te dienen bij jouw lokaal politiekantoor.

Herstelling

Zodra de DDoS-aanval gestopt is, kunnen de uitgeschakelde diensten opnieuw opgestart worden. Nadien kan je verifiëren of alles normaal werkt. Indien alles naar behoren werkt, communiceer dit naar de gebruikers.

CENTRE FOR
CYBER SECURITY BELGIUM
Under the authority of the Prime Minister
Rue de la Loi, 16 - Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

Evaluatie

Evalueer wat vlot en wat minder vlot is verlopen. Probeer de werkpunten om te zetten in concrete acties in de voorbereidende fase.

Onderstaande vragen kunnen hierbij als leidraad dienen:

- Welke voorbereidende stappen zijn nodig om sneller of effectiever te reageren?
- Waren de nodige communicatie kanalen (intern en extern) beschikbaar?
- Waren de communicatiekanalen (intern en extern) bekend en gebruikt?
- Welke verdedigingsmechanismen verwacht je om dit type DDoS-aanval te voorkomen?
- Hoe werd het incident veroorzaakt en ben je in staat om sneller te reageren?
- Welke stappen heb je ondernomen om dit incident in te dammen en is de impact tot een minimum beperkt?
- Welke stappen heb je ondernomen om herhaling te vermijden?
- Wat waren de belangrijkste blokkeringspunten tijdens het incident?
- Welke externe en interne relaties kunnen helpen bij toekomstige incidenten?

CENTRE FOR
CYBER SECURITY BELGIUM
Under the authority of the Prime Minister
Rue de la Loi, 16 – Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

Meer informatie

Centrum voor Cybersecurity België:
https://ccb.belgium.be/nl

Cyberguide:
https://cyberguide.ccb.belgium.be/nl

Verschillende types DDoS-aanvallen:
https://www.enisa.europa.eu/publications/info-notes/dns-ddos-attack-protections

Filmpje over DDoS :
https://www.youtube.com/watch?v=E6t_jrk3LUs

Disclaimer

Dit document werd opgesteld door het Centrum voor Cybersecurity België (CCB). Deze federale overheidsinstelling werd opgericht bij het koninklijk besluit van 10 oktober 2014 en staat onder het gezag van de Eerste Minister.

Het CCB wijst alle aansprakelijkheid in verband met de inhoud van dit document af.

De vermelde informatie:

- is louter algemeen van aard en heeft niet tot doel alle specifieke situaties te behandelen;
- is niet noodzakelijk op alle vlakken volledig, nauwkeurig of up-to-date.

Het CCB stelt alles in het werk om ervoor te zorgen dat de inhoud van dit advies zo actueel, toegankelijk, accuraat en volledig mogelijk is op moment van publicatie. Bij wijziging, wordt zo nodig een nieuwe versie gepubliceerd.

Deze nota bevat links naar websites die door derden zijn gepubliceerd en die niet onder het beheer van het CCB vallen. Deze informatie kan ook te allen tijde veranderen.

Het CCB kan niet aansprakelijk worden gesteld voor schade die voortvloeit uit het gebruik van die informatie. Voorts kunnen geen rechten worden ontleend aan informatie verstrekt door derden.

CENTRE FOR
CYBER SECURITY BELGIUM
Under the authority of the Prime Minister
Rue de la Loi, 16 - Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

Voorbereiding

NETWERK

Internet toegang:
rechtstreeks/via anderen, namelijk ……

ISP: ……

Contract: ……

IP's: ……

Diensten op netwerk: ……

INCIDENT RESPONS PROCEDURE

Out of band communicatie + contactgegevens

Intern:

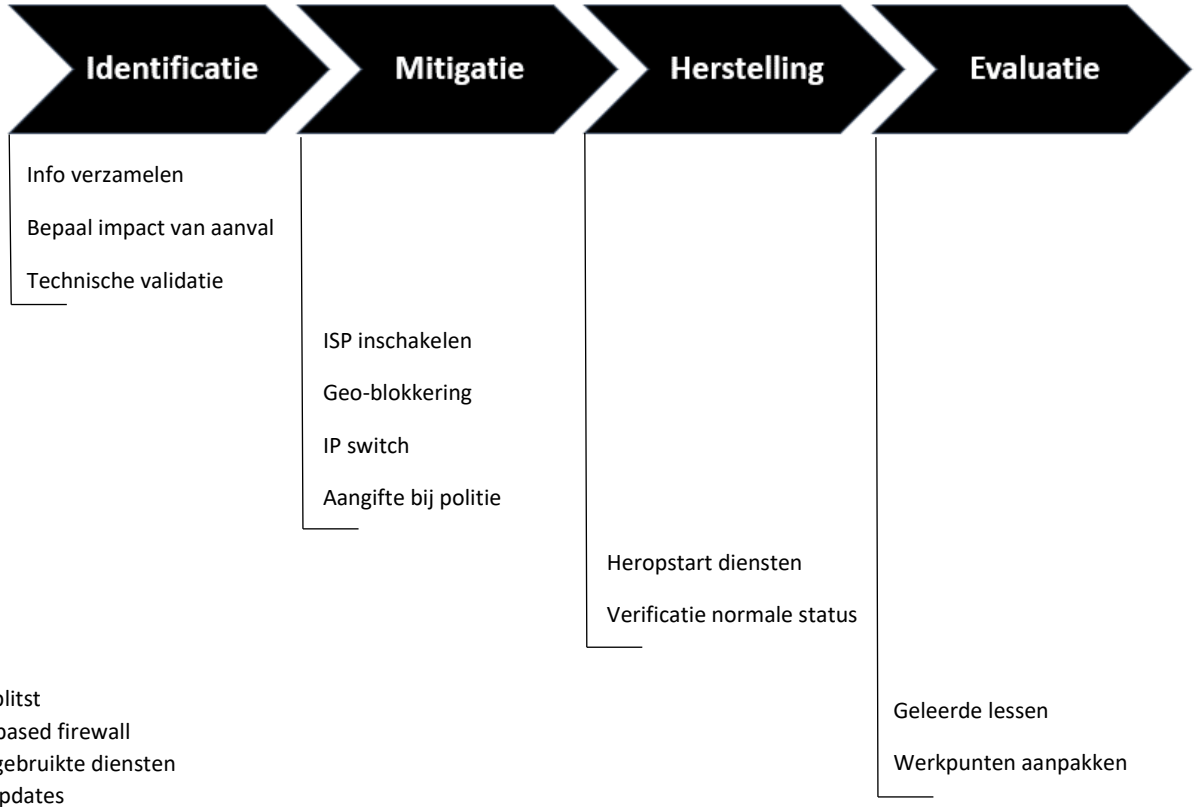
- Management: ……
- IT-dienst: ……
- Medewerkers: ……

Extern:

- ISP: ……
- Security-expert: ……
- Klanten: ……

Afspraken met ISP's

- Geo-blocking/switch van publiek IP/packet scrubbing/andere ……



Checklist voorbereiding

- ☐ Netwerk opgesplitst
- ☐ Netwerk + hostbased firewall
- ☐ De-activatie ongebruikte diensten
- ☐ Automatische updates
- ☐ Geen standaard wachtwoorden
- ☐ Diensten in Cloud
- ☐ 2FA waar mogelijk

Geavanceerd:

- ☐ Regelmatige netwerk scanning
- ☐ Filtering functionaliteit actief op router
- ☐ Private IP-ranges
- ☐ Voorkom IP spoofing
- ☐ Enkel gekende goede trafiek doorlaten
- ☐ Uitgeschakeld: IP-directe broadcast - HTTP configuraties - ICMP ping - IP source routing