CENTRE FOR CYBERSECURITY BELGIUM

DDOS: PREVENTIE EN BESCHERMING

TECHNISCHE RICHTLIJN 2024

Belnet

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Datum: februari 2024
Versie: 2.1 NL
Auteur: Centrum voor Cybersecurity België (CCB) met de waardevolle input van Belnet

Het Centrum voor Cybersecurity België (CCB) is de nationale autoriteit voor cyberbeveiliging in België. Het CCB werd opgericht bij koninklijk besluit van 10 oktober 2014 en staat onder het gezag van de eerste minister.

Vanuit zijn wettelijke opdracht probeert het CCB organisaties te informeren en te adviseren over de bescherming tegen DDoS-aanvallen. Dit document dient als technische richtlijn, bijstand en advies in het licht van de Belgische verkiezingen van 2024 om DDoS-aanvallen te voorkomen en zich ertegen te beschermen.

SAMENVATTING

Deze richtlijn met betrekking tot preventie en bescherming van DDoS-aanvallen, is opgesteld met het oog op de Belgische verkiezingen in 2024. Op federaal niveau spelen verschillende stakeholders een belangrijke rol in het verkiezingsproces. Effectieve bescherming tegen DDoS-aanvallen vereist een gecoördineerde aanpak tussen deze stakeholders.

In dit document wordt eerst uitgelegd wat een DDoS-aanval is en worden de verschillende soorten DDoS-aanvallen, de impact en de redenen achter een DDoS-aanval beschreven. Hoofdstuk 2 reikt proactieve maatregelen aan om voorbereid te zijn op een DDoS-aanval en schetst oplossingen voor risicobeperking. Hoofdstuk 3 beschrijft hoe u moet reageren wanneer uw organisatie het slachtoffer is van een DDoS-aanval en beschrijft technische beperkingsmaatregelen. Het vierde en laatste hoofdstuk bestaat uit een checklist, waarbij het eerste deel een proactieve checklist bevat. In het tweede deel worden de stappen van de incidentrespons toegelicht zoals beschreven in hoofdstuk 3.

Deze richtlijn is adviserend van aard en helpt om voorbereid te zijn en te kunnen reageren wanneer er een DDoS-aanval plaatsvindt.

Dit document is tot stand gekomen dankzij de waardevolle input van Belnet.

Inhoudsopgave

Woordenlijst

ASN	Autonomous system number
Botnet	Een verzameling geconnecteerde apparaten, vaak binnen een IoT-netwerk, die geïnfecteerd raken en overgenomen worden door malware ten voordele van cybercriminelen
CCB	Centrum voor Cybersecurity Belgium
CDN	Content delivery network
CSIRT	Cyber security incident response team
C2-server	Command and Control server
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
Drupal	Content management software
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ISP	Internet Service Provider
NSM	Network Security Monitoring
OSI-model	Het Open Systems Interconnection (OSI)-model beschrijft de zeven lagen die computersystemen gebruiken om via een netwerk te communiceren
SIP	Session Initiation Protocol
SIEM	Security Information and Event Management system
SMTP	Simple Mail Transfer Protocol
SYN flood	Een type DDoS-aanval (denial of service) die tot doel heeft een server onbeschikbaar te maken voor legitiem verkeer door alle beschikbare serverbronnen op te gebruiken
TCP	Transmission Control Protocol
TTL	Time to Live
UDP	User Datagram Protocol
WAF	Web Application Firewall

1. Inleiding

1.1. ALGEMEEN

Een Denial of Service, of DoS, is een cyberaanval die tot doel heeft de beschikbaarheid van een bepaalde dienst te verstoren. Een DoS-aanval maakt gebruik van één computer en één internetverbinding. Als de aanval “gedistribueerd” is en meerdere computers en hun internetverbindingen gebruikt, gaat het over een DDoS, Distributed Denial of Service. Het is belangrijk om te benadrukken dat de computers die betrokken zijn bij een DDoS, hoewel ze “gedistribueerd” zijn, een gemeenschappelijk doel beogen en dat het gaat om een gecoördineerde aanval. Dit soort aanval kan een grote impact hebben op de activiteiten van organisaties en bedrijven.

Er zijn verschillende soorten DDoS-aanvallen, die uitgebreid worden toegelicht in 1.4. Soorten DDoS-aanvallen.

1.2. REDENEN VOOR DDOS-AANVALLEN

Een DDoS-aanval kan om verschillende redenen plaatsvinden: chantage, ideologische of haatgerelateerde aanvallen, concurrentie, politiek, elektronisch protest, rookgordijn, peilingen, experimenten, hacktivisme, prestige/uitdaging of afpersing. Hacktivisten hebben zich bijvoorbeeld gericht op verkiezingswebsites met voornamelijk DDoS-aanvallen, waarbij aanzienlijke hoeveelheden verkeer naar de servers worden gestuurd in een poging om legitieme gebruikers de toegang tot websites te ontzeggen. Deze aanvallen zijn vaak politiek gemotiveerd en zijn bedoeld om het democratische proces te verstoren, chaos te veroorzaken of te protesteren tegen politieke beslissingen.

De grootste hacktivistische dreiging op het gebied van DDoS-aanvallen is momenteel het DDoSia-project dat begin 2022 werd gelanceerd. Dit DDoS-project is gerelateerd aan een nationalistische Russische hacktivistengroep en lanceert veel aanvallen tegen Oekraïense en NAVO-gerelateerde landen en diensten.

1.3. BRON VAN DDoS-AANVALLEN

De meeste DDoS-aanvallen worden uitgevoerd via een botnet.

Deze botnets worden meestal voor een paar uur "ingehuurd" om de aanval uit te voeren, vergelijkbaar met "DDoS as a service". De eigenaars van de botnets zijn meestal niet dezelfde personen die de aanval uitvoeren. Een botnet bestaat uit een groot aantal computers die geïnfecteerd zijn met een vorm van malware. De malware heeft een agent component die de eigenlijke aanval uitvoert. De meeste malware heeft verschillende functies, waar DDoS er vaak maar één van is. De agent die draait op het geïnfecteerde apparaat, krijgt zijn van een C2-server (Command and Control server). Deze C2 stuurt de verschillende agents en vertelt ze wat ze moeten doen. Eigenaars van geïnfecteerde apparaten zijn zich er meestal niet van bewust dat hun apparaten geïnfecteerd zijn en bijdragen aan een DDoS-aanval. Het is belangrijk om te benadrukken dat bijna iedereen een DDoS-aanval kan uitvoeren.

Er zijn genoeg tools en middelen (botnets) beschikbaar. Iedereen met beperkte vaardigheden maar met voldoende vastberadenheid (of geld - hoewel botnets niet zo duur zijn) kan een DDoS-aanval uitvoeren.

1.4. SOORTEN DDoS-AANVALLEN

Over het algemeen kunnen de meest voorkomende vormen van DDoS-aanvallen in drie categorieën worden ingedeeld:

1. **Volumetrisch**: deze DDoS-aanvalsmethode verstoort het normaal verkeer naar een dienstdoor de netwerklaag ervan te overstelpen met een vloedgolf aan frauduleus verkeer vanuit talrijke bronnen. Dit resulteert in een verstoorde of volledig onbeschikbare service voor legitieme gebruikers. Dit type DDOS aanval wordt vaak een layer 3-aanval genoemd. Voorbeelden hiervan zijn reflective/amplification attacks (UDP flood) en ICMP (Internet Control Message Protocol) flood.

2. **Protocol**: de protocolgebaseerde DDoS-aanval maakt gebruik van zwakke punten in internetcommunicatieprotocollen om kwetsbaarheden in organisaties uit te buiten. Protocollen zoals TCP (Transmission Control Protocol) en ICMP kunnen worden gebruikt om protocolgebaseerde DDoS-aanvallen uit te voeren. Meestal brengt een DDoS op protocolniveau veel verbindingen tot stand zonder ze volledig op te starten (bv.: SYN flood) om het aantal verbindingen dat de server aankan uit te putten. Aangezien de belangrijkste vector voor dit type aanval SYN Flood (TCP) is, wordt deze aanval vaak een layer 4-DDoS-aanval genoemd.

3. **Applicatie-aanval**: de applicatie-aanval staat ook bekend als layer 7-DDoS-aanval. Deze methode richt zich op de applicatielaag van de netwerkstack - dit is de laag die verantwoordelijk is voor de verwerking

van specifieke protocollen, zoals HTTP, SMTP (Simple Mail Transfer Protocol) of DNS. Aanvallen op applicatielagen vereisen over het algemeen de meeste kennis van de infrastructuur van het slachtoffer. Als ze correct worden uitgevoerd, heeft de aanvaller bovendien de minste middelen nodig. Meestal plaatsen DDoS-aanvallen op applicatieniveau willekeurige gegevens op een zoekformulier van een website om de database te belasten of vragen ze een willekeurig, niet-bestaand subdomein aan de DNS-server. Een voorbeeld van een applicatie-aanval is een HTTP slow post-aanval, waarbij een aanvaller opzettelijk heel langzaam aangekondigde gegevens verstuurt om de verbindingen open te houden en uiteindelijk de bronnen van de server uit te putten.

2. Proactieve maatregelen

In dit hoofdstuk worden een aantal proactieve, zowel technische als niet-technische maatregelen opgesomd, die genomen kunnen worden om de impact van een mogelijke DDoS-aanval te beperken.

2.1. KEN UW NETWERK

Het is belangrijk om uw netwerk te kennen. Weet over welke openbare diensten en netwerken u beschikt. Vergeet ook uw off-sitediensten (bv. cloud) niet. Als uw internetverbinding uitvalt, hebt u geen toegang tot deze diensten.

Het wordt aanbevolen om een volledige inventaris op te maken, inclusief netwerktypologieën en externe en interne IP-adressen. Deze documentatie is essentieel tijdens een aanval. Zorg ervoor dat u ook offline toegang hebt tot deze documentatie in geval van een cyberaanval.

Door regelmatig een off-netwerkscan uit te voeren om uw openbaar toegankelijke apparaten en diensten te inventariseren, kunt u in kaart brengen wat u aan het internet blootstelt. Zorg ervoor dat u een lijst hebt van eigenaren van diensten en een lijst van mensen die verantwoordelijk zijn (zowel technisch als niet-technisch) voor al uw blootgestelde bedrijfsmiddelen.

2.2. KEN UW TOEPASSINGEN

Het is belangrijk om kennis te hebben van uw toepassingen en de nodige mitigatiemaatregelen (risicobeperkingsmaatregelen) voor te bereiden. DDoS-aanvallen maken vaak gebruik van specifieke onderdelen van de toepassingen om de belasting op meerdere systemen te verhogen. Als u zich bewust bent van deze zwakke punten, kunt u specifieke mitigaties voorbereiden.

Op een website kunnen sommige pagina's de database zwaarder belasten (bv. een zoekformulier), waardoor ze een aantrekkelijk doelwit zijn. Dat zijn ook vaak de pagina's die niet effectief achter een cache kunnen worden geplaatst. Door ze te inventariseren en een procedure voor te bereiden om die pagina's uit te schakelen als ze het doelwit zijn, kunt u de DDoS-aanval beperken. Er kan ook een statische kopie van de site worden gemaakt als tijdelijke vervanging tijdens de aanval.

2.3. INCIDENT RESPONSE-PROCEDURE

Stel een incident response-plan op en hou dit plan up-to-date. Bij een DDoS-aanval is het belangrijk om snel en efficiënt te reageren.

Een incident response-procedure beschrijft wat er moet gebeuren in het geval van een cyberaanval. Bepaal een aantal operationele standaardprocedures in geval van een DDoS-aanval:

- Identificeer debedrijfsmiddelen van uw organisatie
- Implementeer een Business Continuity Plan/Disaster Recovery Plan
- Bepaal de bedrijfsprioriteiten voor herstel
- Documenteer hoe uw systemen werken en hou deze documentatie up-to-date
- Wijs verantwoordelijkheden en rollen toe aan mensen met de juiste vaardigheden
- Bereid een out-of-band communicatiekanaal voor
- Stel een lijst met contactpersonen op
- Doe een beroep op deskundigen inzake cyberincidentresponse
- Bereid een communicatiestrategie voor - voor meer informatie: https://atwork.safeonweb.be/recent-news-tips-and-warning/crisis-communication-event-cyber-attack

Specifiek voor DDoS-aanvallen is het cruciaal om bijzondere aandacht te besteden aan de volgende punten:

- Overleg vooraf met uw internetprovider (ISP): bespreek wat uw ISP kan implementeren om DDoS-aanvallen te voorkomen en wat de ISP kan ondernemen in het geval van een DDoS-aanval.Bijvoorbeeld: geo-blocking, publiek IP-adres wijzigen, packet scrubbing etc.

- Bereid Service Level Agreements (SLA's) met uw ISP voor in het geval van een DDoS, alsook SLA's voor DDoS-aanvallen op elk niveau van het netwerk.

- Controleer de bestaande contracten met uw ISP, Cloud en Hosting provider voor DDoS-bescherming en pas ze indien nodig aan.

- Zie nauwlettend toe op de belangrijkste infrastructuur om snel te achterhalen of er meer resources worden gebruikt of deze zelfs uitgeput raken, zodat er snel kan worden gereageerd. Bepaal de verantwoordelijkheden en rollen met betrekking tot deze monitoring.

- Zorg ervoor dat er een duidelijke baseline bestaat voor netwerkverkeer, zodat abnormaal of aanvalsverkeer makkelijker kan worden opgespoord.

- Onderzoek de mogelijkheid om uw infrastructuur op te schalen in het geval van een aanval, vooral voor diensten in de cloud (bv. Azure).

- Voer regelmatig stresstests uit om ervoor te zorgen dat de infrastructuur en mitigaties werken zoals verwacht.

- Bereid een out-of-band communicatiekanaal voor: een beveiligd communicatieplatform moet op een apart netwerk werken dat niet onderhevig is aan dergelijke aanvallen. Enkele voorbeelden: telefoon (onveilig), Signal, Threema etc. Bepaal vooraf ook duidelijk welke groep mensen met welke middelen gaan communiceren.

- Maak een offline contactlijst: het is belangrijk om over een offline (afgedrukte) contactlijst te beschikken van personen die u kunnen helpen of die u moet informeren. Dit kan zowel intern (management, werknemers, IT-dienst) als extern (ISP, beveiligingsexpert, klanten) zijn.

- Naast technische expertise moet er ook personeel beschikbaar zijn dat uitvoerende beslissingen kan nemen. Al deze rollen moeten worden opgenomen in een Business Continuity Plan/Disaster Recovery Plan.

- Hou een permanente dreigingslijst bij voor bekende botnets en kwaadaardige IP's, en blokkeer deze permanent of enkelwanneer dat nodig is.

- Verspreid de verschillende diensten over uw IP-omgeving om mogelijke neveneffecten te minimaliseren en mitigatie te vergemakkelijken. Voeg geen verschillende onafhankelijke diensten samen achter eenzelfde IP-adres.

- Gebruik nooit hetzelfde publieke IP voor diensten/toepassingen als hetgene dat gebruikt wordt voor de internettoegang voor de personen binnen uw organisatie.

3. Stappen voor incidentrespons bij een DDoS-aanval

Hoofdstuk 3 beschrijft hoe te reageren als uw organisatie het slachtoffer is van een DDoS-aanval. De mitigerende maatregelen die hieronder worden beschreven, zijn de minimale stappen die een organisatie moet volgen in het geval van een DDoS-aanval. Wees je ervan bewust dat er geen pasklare oplossing bestaat.

Het is belangrijk om een slachtoffer van een DDoS-aanval erop te wijzen dat dit proces technische expertise vereist, evenals toegang tot alle betrokken resources (firewall, applicaties, etc).

3.1. DE OMVANG VAN DE AANVAL VASTSTELLEN EN BEVESTIGEN

Wanneer u denkt dat er een DDoS-aanval aan de gang is, moet u eerst de onbeschikbaarheid van services nagaan (bv.: alleen onbeschikbaar voor een beperkt aantal mensen of voor iedereen).

Verzamel zoveel mogelijk informatie over de aanval. Om de impact van de DDoS te bepalen, is het belangrijk om de getroffen systemen in kaart te brengen. Dit kan bijvoorbeeld worden ingeschat op basis van klachten van gebruikers.

3.2. INZICHT IN DE AANVAL

Zodra de impact van de aanval in kaart gebracht is, is het belangrijk om te onderzoeken wat deze onbeschikbaarheid heeft veroorzaakt. Een goed begrip van hoe de aanval werkt is essentieel voor het implementeren van effectieve tegenmaatregelen.

- Indien beschikbaar kan een Security Information and Event Management-systeem (SIEM) of Network Security Monitoring (NSM) heel nuttig zijn om na te gaan wat er aan de hand is.
- Als er geen oplossing voor monitoring/logging beschikbaar is, bekijk dan rechtstreeks de logbestanden van netwerkapparatuur/applicaties.
- Als u een baseline van uw netwerkverkeer hebt, kunt u deze gebruiken om te achterhalen welke aanvalspatronen de aanvaller gebruikt. Voorbeelden hiervan zijn een aanzienlijke toename in aanvragen naar een webserver of (verhoogde) query's voor onbestaande domeinen (DNS).
- Bespreek met uw ISP hoe de situatie kan worden rechtgezet en zorg voor proactieve monitoring.

3.3. VRAAG ASSISTENTIE AAN UW ISP OF IMPLEMENTEER EEN ANTI-DDOS-OPLOSSING VAN DERDEN

- Neem zo snel mogelijk contact op met uw ISP of uw externe leverancier van anti-DDoS-oplossingen en geef de ISP zoveel mogelijk informatie over de aanval. De informatie moet op zijn minst de geviseerde IP's, het type DDoS (zie 1.4. Soorten DDoS-aanvallen) en de potentiële aanvalsvectoren omvatten.
- U kunt ook de impact en de gevolgen van de aanval meedelen, zodat uw ISP beter begrijpt wat er aan de hand is en welke oplossingen mogelijk zijn.
- U kunt ook de baseline van legitiem verkeer meedelen, zodat de ISP een idee heeft van de hoeveelheid verkeer die ze moeten blokkeren.
- Vraag om een communicatiekanaal te openen om de communicatie tijdens de aanval te vergemakkelijken. Aanvalsvectoren veranderen vaak tijdens de aanval om de mitigaties te omzeilen. Op die manier kunt u ook feedback geven over de genomen maatregelen. De ISP zal sneller kunnen reageren op te forse maatregelen die legitiem verkeer blokkeren of te zwakke maatregelen die te veel pakketten van de aanval toelaten.
- Hoewel ISP's waarschijnlijk niet in staat zijn om een L7-aanval te beperken als ze uw applicaties niet hosten of beheren, kunt u toch overwegen om hen erbij te betrekken, omdat ze sommige vectoren die tegelijkertijd worden gebruikt, kunnen beperken.
- Hou er rekening mee dat, hoewel de meeste ISP's een vorm van DDoS-bescherming aanbieden (intern of via een derde partij) die veel van de volumetrische layer 3- en 4-aanvallen kan beperken, de mitigatie nooit 100 procent is.

- Alleen als laatste redmiddel en als één specifiek IP (niet een perimeterapparaat) het doelwit is, en de bescherming niet voldoende is, kunt u overwegen om uw provider te vragen om dit IP tijdelijk te "blackholen". Dit heeft uiteraard als gevolg dat de dienst onbeschikbaar zal zijn, waardoor de aanval (deels) succesvol zal zijn, maar in ieder geval worden de gevolgen beperkt en blijft de organisatie tot op zekere hoogte operationeel.

3.4. STAPPEN DIE U ALS SLACHTOFFER KAN NEMEN

De onderstaande stappen gaan ervan uit dat de externe connectiviteit nog steeds beschikbaar is. Als de gateway of externe firewall volledig uitgebuit is door de aanval, neem dan contact op met de ISP.

Als u monitoring/logs beschikbaar hebt, onderzoek deze dan. Zo niet, kunt u een PCAP aan de externe kant van de firewall uitvoeren, of direct logs van applicaties/apparaten verzamelen.

3.4.1. INZCHT IN DE AANVAL

- Bepaal het doelwit van de aanval.
- Welke soorten resources zijn het doelwit van de aanvaller?
- Bepaal het type DDOS-aanval (op welke laag van de OSI-laag, layer 3-4 of tot en met 7).
- Voer een statistische analyse uit van de oorsprong van de aanval: zijn er bronnen of landen die opvallen? Zijn er ASN's die opvallen? Visualisaties/dashboards die gewoonlijk beschikbaar zijn in een NSM zijn hierbij erg nuttig.

3.4.2. ALGEMENE DDOS-MITIGATIES

Het is meestal een goed idee om het aanvalsverkeer snel te filteren, zodat uw netwerk wat ademruimte krijgt. Op dit punt kunt u zich waarschijnlijk beperken tot zeer restrictieve blokkering. De gezondheid van uw netwerk en applicaties, evenals de beschikbaarheid voor uw belangrijkste klanten zijn hier uw eerste zorg. Dit geeft u de tijd om dieper te graven en betere oplossingen te vinden op maat van de gebruikte aanvalsvector.

- Tijdelijke blokkering van aanvallende IP's: maak een (bij voorkeur aparte) zwarte lijst met de IP-adressen die (tijdelijk) de toegang moet worden ontzegd. Als het IP-adres dat het verzoek heeft verzonden op de zwarte lijst staat, onderschept het systeem de verbinding en weigert het de toegang. Deze weigering kan verschillende vormen aannemen, zoals het weergeven van een foutmelding, het doorsturen van de gebruiker naar een andere pagina of het verbreken van de verbinding zonder antwoord.

- Tijdelijke geoblocking/geofencing van specifieke IP-reeksen: blokkeer de toegang vanuit een hele geografische regio.

- ASN-blokkering: als het malwareverkeer afkomstig is van verschillende ASN's, blokkeert u deze ASN, of netwerkblokken daarvan.

- Load-balancing en upscaling: load-balancingtechnieken verdelen inkomend verkeer over meerdere servers of datacenters. Door de verkeersbelasting te spreiden, kan worden voorkomen dat een enkele server of resource verzadigd wordt door een DDoS-aanval. De mogelijkheid om de capaciteit van een service tijdelijk te verhogen tijdens een aanval kan de impact ervan beperken.

- Isoleren: als de aangevallen service op een server staat die ook andere services levert, verplaats de aangevallen service dan naar een apart systeem om de neveneffecten van de aanval te minimaliseren.

- Strip down: reduceer een service tot het absolute minimum.

- Remotely triggered black hole: alle verkeer naar een specifiek doel-IP omleiden naar een "null interface", waardoor kwaadaardig verkeer wordt verwijderd voordat het zijn bestemming bereikt.

- Geviseerde services en/of applicaties stoppen: deze maatregel blokkeert geen aanvallen, maar kan wel voorkomen dat de applicatie/service crasht of een ernstige storing ondervindt. Wees u er van bewust dat dit tot een aanzienlijk verlies van gegevens en services kan leiden.

3.4.3. SPECIFIEKE MITIGERENDE MAATREGELEN PER AANVALSVECTOR

In het geval van een DDoS-aanval: zoek naar specifieke protocol- (Layer3/Layer4) of applicatie- (Layer 7) patronen zoals:

Overzicht Layer 3 en Layer 4

Protocol	Aanvalsvector	Mitigerende maatregelen
UPD	Reflective/Amplification	• Kan worden geblokkeerd als dit verkeer niet wordt gebruikt/verwacht op het geviseerde systeem. • Anders een beroep doen op volumetrische/ DDoS-scrubbingtechnologieën.
TCP	SYN Flood	• Syn-cookie implementeren. • Time-outinstellingen bijstellen. • Hergebruik van oudste half-open TCP sessie.

Overzicht Laag 7

Toepassing	Aanvalsvector	Mitigerende maatregelen
DNS	NX Flood (Legitimate) request flood	• De DNS server cache beschermen tegen besmetting met NX- antwoorden. • DNS-query's weigeren op basis van een whitelist van (sub)domeinen. • Snelheidsbeperking per bron-IP.
HTTP/HTTPS	Low/slow Targeted URL flood	• Time-outinstellingen agressiever afstellen. • Agressievere snelheidsbeperking voor de meest geviseerde URL's. • Als de impact op de webserver groot is: overweeg om alle aanvragen naar de meest geviseerde URL's te weigeren (zodat ze niet meer beschikbaar zijn). • Indien beschikbaar: referrer URL bekijken.

3.4.4. ANDERE EVENTUELE MITIGERENDE MAATREGELEN

- Implementeer een anti-DDOS-apparaat dat DDoS-aanvallen kan beperken. Opgelet: dit is een dure oplossing. Als DDoS-aanvallen op uw omgeving veel voorkomen, kunnen deze kosten echter gerechtvaardigd zijn.

- Voor webtoepassingen: vervang dynamisch gegenereerde inhoud door statische inhoud. Het uitschakelen van dynamische inhoud zoals een zoekformulier, het gebruik van afbeeldingen van lage resolutie en het comprimeren van de CSS- en JavaScript-bestanden kan het totale dataverkeer van/naar de website verminderen.

- Verbeter de veerkracht door (permanent) een Content Delivery Network (CDN)-oplossing te implementeren.

- Overweeg verdere segmentatie in uw netwerk. Vermijd waar mogelijk het delen van infrastructuur.

- DNS-records: instellen van een hogere Time To Live (TTL) voor DNS-records. Een TTL van één dag (24 uur) kan de impact op andere services beperken als DNS-servers uitvallen. Hou er echter rekening mee dat een langere TTL ook gevolgen heeft bij het toepassen van wijzigingen.

- Voor webtoepassingen zoals websites: implementeer een Web Application Firewall (WAF) en Advanced Global CDN. De WAF controleert en blokkeert kwaadaardig verkeer van uw website/server op basis van een reeks regels. Deze detecteert/blokkeert bekende kwaadaardige IP-adressen, verdachte user agents en andere ongewone activiteiten, zoals herhaalde pogingen tot brute force-aanvallen op uw website. AGCDN voegt verdere bescherming toe tegen DDoS-aanvallen op uw website door te voorkomen dat een piek in aanvragen uw hoofdserver (origin server) bereikt, waardoor uw site onbeschikbaar zou kunnen worden. Veel CDN-aanbieders beheren de WAF zelf, als onderdeel van een betaalde service.

- Wanneer u Cloud resources gebruikt die toegankelijk zijn vanaf het openbare internet, overweeg dan om de DDoS-beschermingsmechanismen van de Cloud aanbieder te activeren.

3.5. BEWIJS VERZAMELEN

Ongeacht of u het incident in de post-incident fase rapporteert aan uw ISP, aan het nationale CSIRT, aan de gerechtelijke autoriteiten of aan een andere partner, zal u op de een of andere manier bewijsmateriaal moeten voorleggen. Bewijs kan bestaan uit NetFlow, netwerk en applicatie logbestanden. Idealiter zou u al deze elementen moeten kunnen voorleggen.

3.6. HERSTEL

De DDoS-aanval is voorbij wanneer uw netwerkverkeer terugkeert naar de eerder ingestelde baseline.

DDoS-aanvallen verlopen soms in golven.. Aanvallers kunnen meerdere DDOS-golven lanceren. U kunt dus denken dat de aanval voorbij is, de aandacht kan verslappen en de hackers kiezen dat moment om een nieuwe, krachtigere aanval te lanceren. Ze kunnen hun methode tussen de golven ook veranderen om te bepalen welke techniek de meeste impact heeft. Zodra de DDoS-aanval voorbij is, kunnen de uitgeschakelde services opnieuw worden opgestart.

Controleer daarna of alles normaal werkt. Zo ja, deel dit dan mee aan de gebruikers.

3.7. EVALUATIE

Zodra de aanval is afgehandeld, moeten alle betrokkenen samenkomen om lessen te trekken. Evalueer wat goed ging en wat minder goed ging. Voer regelmatig stresstests uit om ervoor te zorgen dat de infrastructuur en mitigaties werken zoals verwacht.

Evalueer de verbeterpunten en zet deze om in concrete actiepunten in de voorbereidingsfase. Pas de incidentprocedure aan voor de toekomst.

Dit omvat onder meer de volgende aspecten:

- Overweeg om back-end server-IP's die bekend zijn bij aanvallers te wijzigen.
- Bepaal de juiste bandbreedte voor uw internetverbinding: normale dagelijkse activiteiten zouden slechts ongeveer 50% van uw totale bandbreedte mogen verbruiken.
- Herzie uw architectuur op basis van de zwakke punten die tijdens de DDoS-aanval aan het licht zijn gekomen.

4. Checklist

De onderstaande checklist is opgedeeld in twee delen. Het eerste deel bestaat uit een proactieve checklist. Het tweede deel licht de stappen van incident response toe zoals beschreven in hoofdstuk 3.

4.1. PROACTIEVE CHECKLIST

☐ Weet welke netwerken, hosts en services blootgesteld zijn, werk uw inventaris regelmatig bij. Wees u bewust van mogelijke knelpunten:

- Evalueer het risico en het belang van blootgestelde bedrijfsmiddelen.
- Zorg voor een schriftelijke en goedgekeurde lijst van service-eigenaars.
- Zorg voor bijgewerkte netwerk- en servicediagrammen.
- Zorg voor out-of-band communicatiekanalen.
- Zorg voor offline of hardcopy's van lijsten met contactpersonen.

☐ Zorg ervoor dat uw ISP en nationale CSIRT uw organisatie en uw contactpunten kennen en vice versa.

☐ Weet precies wat uw ISP wel en niet kan doen tijdens een DDoS-aanval.

☐ Bereid SLA's voor met uw ISP in het geval van DDoS-aanvallen.

☐ Controleer uw firewallregels regelmatig.

☐ Zorg voor automatische beveiligingsupdates van besturingssystemen, programma's en routers.

☐ Gebruik waar mogelijk diensten in de Cloud. Websites, e-maildiensten of andere onlineplatforms zijn bijvoorbeeld erg kwetsbaar als u ze lokaal op een server host. Door hun omvang zijn clouddiensten vaak minder vatbaar voor DDoS-aanvallen.

☐ Stel een crisiscommunicatieplan op.

4.2. STAPPEN IN INCIDENTRESPONS

☐ Zorg voor interne capaciteit om op incidenten te reageren.

☐ Gebruik een goed geconfigureerde loadbalancer en maak gebruik van upscaling.

☐ Implementeer een reverse proxy.

☐ Implementeer een WAF en Advanced Global CDN.

☐ Controleer en versterk uw netwerkapparaten en pas best practices toe.

☐ Bereid een gestripte versie van uw services voor om te gebruiken in het geval van een aanval.

☐ Voor webtoepassingen: vervang dynamisch gegenereerde contacten door statische inhoud.

☐ Verbeter de veerkracht door een Content Delivery Network (CDN)-oplossing te implementeren.

☐ Overweeg het opsplitsen van de interne en openbare DNS-infrastructuur.

☐ DNS-records: instellen van een hogere Time To Live (TTL) voor DNS-records. Een TTL van één dag (24 uur) kan de impact op andere services beperken als DNS-servers bij een toekomstige aanval uitvallen.

☐ Voor webtoepassingen (bv. Drupal): implementeer een Web Application Firewall (WAF) en Advanced Global CDN.

☐ Overweeg om DDoS-bescherming van uw (cloud)providers te activeren/aan te vragen.

☐ Blokkeer kwaadaardige IP's tijdelijk.

☐ Stel tijdelijke geoblocking/geofencing van specifieke IP-reeksen in.

☐ ASN blokkeren: als het schadelijke verkeer afkomstig is van verschillende ASN's, blokkeer dan deze ASN, of netwerkblokken daarvan.

☐ Load-balancing en upscaling: load-balancingtechnieken verdelen inkomend verkeer over meerdere servers of datacenters. Door de overbelasting te spreiden, kan het voorkomen dat een enkele server of bron verzadigd wordt door een DDoS-aanval.

☐ Packet scrubbing: het verkeer dat bestemd is voor een bepaalde IP-adresreeks wordt omgeleid naar datacenters, waar het aanvalsverkeer wordt "gescrubd" of opgeschoond. Alleen schoon verkeer wordt dan doorgestuurd naar de doelbestemming.

☐ Stop geviseerde services en/of toepassingen.

☐ Remotely triggered black hole.