AANBEVELINGEN TER BESCHERMING TEGEN DENIAL-OF-SERVICE-AANVALLEN

WWW.GOVCERT.NL

POSTADRES
Postbus 84011
2508 AA Den Haag
BEZOEKADRES
Wilhelmina van Pruisenweg
104
2595 AN Den Haag
TELEFOON
070 888 75 55
FAX
070 888 75 50
E-MAIL
info@govcert.nl

Auteur(s) : GOVCERT.NL
1.2
Den Haag : 20.11.2006

GOV  CERT.NL

GOVCERT.NL

1 INLEIDING

Het verstoren van diensten en systemen die in contact staan met het Internet is een bijna dagelijkse gebeurtenis. Een van de meest bekendste manieren om diensten en systemen te verstoren, is de zogenaamde (Distributed) Denial-of-Service (DDoS) aanval.

In het verleden werden DDoS-aanvallen als een vorm van vandalisme uitgevoerd. Er was dus geen sprake van een duidelijk doel of gewin. Tegenwoordig worden DDoS-aanvallen misbruikt om een bepaald doel na te streven. Een dergelijk doel is bijvoorbeeld afpersing of protest tegen een organisatie of standpunt. Door deze omslag is de kans reëel dat DDoS-aanvallen in de toekomst zullen gaan plaatsvinden.

Om een Denial-of-Service-aanval te kunnen afslaan is het van belang dat een aantal zaken zijn geregeld. Dit document geeft een uitleg over DDoS-aanvallen en beschrijft een aantal adviezen die bruikbaar zijn om diensten en systemen te beschermen tegen een dergelijke aanval. De adviezen beschrijven maatregelen op het gebied van preventie, detectie en reactie.

Een Denial-of-Service-aanval kan dusdanig omvangrijk zijn zodat de maatregelen die zijn genomen om diensten en systemen te beschermen niet meer effectief zijn. Op dat moment is hulp van derden noodzakelijk. De rol van de provider is ten tijde van een DDoS-aanval daarom cruciaal. In dit document is een apart hoofdstuk gewijd aan de rol die de provider voor u kan betekenen.

Denial-of-Service-aanvallen kunnen op allerlei systemen of diensten plaatsvinden. In dit document gaan we uit van een website omdat de meeste DDoS-aanvallen op websites zijn gericht. De beschreven maatregelen zijn uiteraard ook bruikbaar voor andere diensten of systemen, zoals mail-servers of FTP-servers.

2 WAT IS EEN DENIAL-OF-SERVICE

Denial-of-Service-aanvallen zijn aanvallen op een systeem of dienst met als doel een systeem, dienst of netwerk zo te belasten dat deze uitgeschakeld wordt of niet meer beschikbaar is. Meestal geschiedt dit door excessief gebruik te maken van een op zich legitiem Internet Protocol, bijvoorbeeld het opzetten van een TCP-sessie.
Denial-of-Service kan worden geïnitieerd van een enkel systeem, maar ook van meerdere systemen tegelijkertijd. Denial-of-Service vanaf meerdere systemen wordt een Distributed-Denial-of-Service genoemd.
Bij een Denial-of-Service-aanval wordt vaak gebruik gemaakt van source IP-adressen die niet gerouteerd worden op het Internet of source IP-adressen van anderen. Dit wordt 'IP spoofing' genoemd. Kwaadwillenden gebruiken source IP-adressen om de identiteit te verbergen maar zeker ook om systemen op eenvoudige manier te overbelasten.

In het algemeen gelden de volgende eigenschappen voor een Denial-of-Service:

- Poging om een netwerk te overspoelen met dataverkeer, waarmee legitiem dataverkeer niet meer kan doorkomen.
- Poging om connecties tussen twee systemen te verbreken.
- Poging om een gebruiker geen toegang te geven tot een systeem.
- Poging om een service op een systeem te onderbreken.

Oneigenlijk gebruik van resources op een systeem kan ook leiden tot een Denial-of-Service. Een hacker kan bijvoorbeeld een FTP-server met publieke toegang misbruiken om illegale bestanden te plaatsen. Dit veroorzaakt netwerkverkeer, en onnodig gebruik van diskruimte.

Denial-of-Service komt in verschillende vormen voor, waarbij gebruik kan worden gemaakt van een drietal basiselementen:

1. Consumptie van schaarse, gelimiteerde resources, of flooding (dichtslibben van netwerkverbindingen).
2. Vernieling of beschadiging van configuraties.
3. Fysieke vernieling of beschadiging van systemen.

In dit document worden alleen maatregelen beschreven die betrekking hebben op de consumptie van schaarse, gelimiteerde resources, of flooding.

2.1 Consumptie van schaarse, gelimiteerde resources

Om te functioneren, maakt het systeem gebruik van resources zoals geheugen, diskruimte, CPU, netwerkbandbreedte etc. Een aanvaller kan misbruik maken van resources op een systeem. Het gevolg is dat het systeem niet meer kan beschikken over de resources, met het gevolg dat het systeem crasht of niet meer bereikbaar is. Dit document gaat met name in op deze manier van DoS-aanval.

Hieronder volgt een aantal vormen:

1. SYN-aanval
2. Smurf-aanval
3. Syslog-aanval
4. E-mailbombing

2.1.1 SYN-aanval ('SYN flood')

Een SYN-aanval maakt misbruik van het zogeheten 'three-way handshake'-mechanisme, dat gebruikt wordt bij het opzetten van TCP-sessies. Normaal gesproken komt een sessie tot stand door het versturen van een SYN-pakket van host A naar host B. Host B antwoordt met een SYN/ACK-pakket, waarna host A antwoordt met een ACK-pakket. Hiermee is de sessie tot stand gebracht.
Bij een SYN-aanval stuurt host A een grote hoeveelheid SYN-pakketten naar host B. In het SYN-pakket wordt een mogelijk gespoofed source IP-adres opgenomen dat niet bekend is op het Internet, of een IP-adres dat anders is dan het IP-adres van host A. Host B stuurt voor elk SYN-pakket een SYN/ACK terug naar het gespoofde IP-adres en reserveert geheugen op het systeem. Host B wacht vervolgens op de ACK pakketten, maar dat komt niet terug omdat het gespoofde adres niet bestaat of omdat het IP-adres SYN/ACK niet herkent. Bij een grote hoeveelheid SYN-pakketten kan dat ertoe leiden dat host B geen geheugen meer beschikbaar heeft voor andere actieve processen op het systeem, met het gevolg dat het systeem crasht. Ook kunnen legitieme TCP-sessies niet meer worden geïnitieerd.

Een SYN-aanval is te herkennen aan de volgende technische eigenschappen:

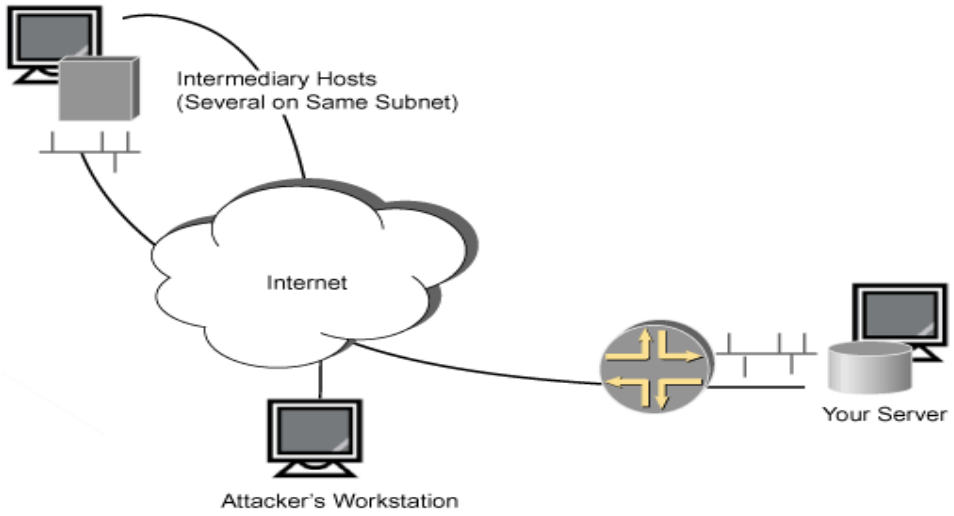
- Host B ontvangt een abnormale hoeveelheid SYN pakketten, afkomstig van één of meerdere IP-adressen
- Host B ervaart toename in hoeveelheid verkeer
- Gemiddelde pakketgrootte neemt af bij host B

2.1.2 Smurf-aanval

Bij een Smurf-aanval wordt gebruikt gemaakt van een principe dat 'directed broadcast' heet.

'Directed broadcast' houdt in dat een systeem een datapakket verstuurt naar het broadcast adres van een netwerk, dat een ander netwerk is dan waar het zendende systeem toe behoort. Het data pakket wordt als een unicast-pakket gerouteerd over een netwerk, totdat het pakket arriveert bij het lokale netwerk van het broadcast IP-adres. De router die het lokale netwerk, waar het subnet zich bevindt, verbindt met het Internet, zal het unicast-pakket omzetten in een broadcast.
Bij een Smurf-aanval wordt een ICMP (Internet Control Message Protocol) 'echo request' pakket verstuurd naar het broadcast IP-adres van een lokaal netwerk. De hacker gebruikt in dit ICMP-pakket een gespoofed source IP-adres of een hacker kraakt een systeem waarvan het source IP-adres wordt misbruikt. De router, die het lokale netwerk verbindt met het Internet, ontvangt de ICMP 'echo request'-pakketten. Alle hosts op het netwerk die in hetzelfde subnet behoren als het broadcast IP-adres, zullen een ICMP 'echo reply' terug geven naar het source IP-

adres. Het gevolg hiervan is dat het source IP-adres een overweldigende hoeveelheid verkeer krijgt toegestuurd wat vaak tot gevolg heeft dat de netwerkverbinding naar die specifieke host vol komt te zitten. Hierdoor is ander legitiem verkeer niet meer mogelijk. Op een netwerk van 254 hosts zal op 1 ICMP 'echo request' pakket 254 'echo reply'-pakketten terugkomen naar het source IP-adres van het ICMP-pakket.



Bovenstaande figuur dient ter verduidelijking van deze aanval:
Het werkstation van de aanvaller stuurt een ICMP 'echo request' naar het subnet, waar de 'Intermediary Hosts' bevinden. Deze ICMP 'echo request'-pakketten bevatten het source IP-adres van 'Your Server'. De 'Intermediary Hosts' versturen een ICMP 'echo reply' terug naar 'Your Server'. "Your Server' ontvangt een grote hoeveelheid ICMP-pakketten, met het gevolg dat de netwerkverbinding maximaal wordt benut. "Your Server' is hierdoor niet meer bereikbaar, of kan zelf geen verkeer meer genereren.

Een smurf-aanval is te herkennen aan de volgende technische eigenschappen:

- "Your Server' ontvangt een abnormale hoeveelheid ICMP-pakketten, afkomstig van een of meerdere IP-adressen
- 'Your Server' ervaart toename in hoeveelheid verkeer
- Gemiddelde pakketgrootte neemt af bij 'Your Server'
- Openstaande connecties van 'Your Server' worden onderbroken
- Router die 'Intermediary Hosts' verbindt met het Internet ontvangt ICMP 'echo request'-pakketten van een of meerdere hosts, die zich buiten het subnet van de 'Intermediary hosts' bevinden.

2.1.3 Syslog-aanval

Netwerk-aparatuur kan zo geconfigureerd worden dat gebeurtenissen, zoals hoge temperatuurscondities, configuratiewijzigingen, etc., rapporteren via Syslog. Wanneer er iets voorkomt dat gerapporteerd moet worden, wordt er over UDP-poort 514 een IP-boodschap verstuurd. Een andere IP-host, een Network Management Station (NMS) ontvangt, evalueert en indien noodzakelijk alarmeert personeel afhankelijk van de inhoud van de SYSLOG-boodschap. Het feit wil echter dat deze boodschappen gespoofed kunnen worden en zo vals alarm veroorzaken.

Technische herkenbaarheid:

- Toename van boodschappen over UDP-poort 514

2.1.4 E-mailbombing

E-mailbombing is een al wat ouder fenomeen dat momenteel niet erg populair meer is. Bij e-mailbombing wordt een mailserver (vaak één specifiek account op een server) overstroomd met e-mail berichten. Deze actie is gericht op het ontoegankelijk maken van e-mail voor een persoon of organisatie (hetgeen in zekere zin een Denial-of-Service-aanval is).
Een e-mailbomb kan ook een (onbedoeld) bijprodukt zijn van verstuurde spam. Indien spam wordt verstuurd met als afzendadres een geldig adres van een “andere partij”, dan worden alle foutmeldingen met betrekking tot de geadresseerden (mocht het geadresseerde adres niet bestaan of geen e-mail kunnen ontvangen bijvoorbeeld) teruggestuurd naar deze derde partij.

2.2 IP-spoofing

Spoofing is je voordoen als iemand anders. Bij een DDoS-aanval wordt vaak gebruikt gemaakt van IP-spoofing. IP-spoofing wil zeggen dat de aanvaller IP-pakketten verstuurt met een source IP-adres van andere systemen. Op deze manier kunnen resources op een systeem worden geblokkeerd en is de identiteit van de aanvaller lastig te achterhalen. Bij IP-spoofing worden de volgende IP-adressen gebruikt:

1. RFC1918 IP-adressen. Dit zijn IP-adressen die op private netwerken kunnen worden gebruikt.
2. IP-blokken die door IANA nog niet zijn uitgedeeld aan een LIR (Local Routing Registry), zoals bijvoorbeeld RIPE. Een overzicht van deze IP-blokken vindt u via:

   http://www.iana.org/assignments/ipv4-address-space

   IP-blokken die nog in bezit zijn van IANA zijn aangemerkt als ‘IANA - Reserved’. Deze IP-blokken kunnen worden misbruikt voor IP-spoofing.
3. IP-adressen die door een LIR of een provider niet nog niet zijn uitgedeeld. Providers beschikken vaak over grote IP-blokken waarvan nog niet alles is

uitgedeeld. De IP-adressen die nog niet in gebruik zijn, kunnen worden gebruikt voor IP-spoofing.

4. IP-adressen die geen IP-pakketten hebben gestuurd.
   Het gaat hier om actieve- of inactieve IP-adressen van systemen die initieel geen IP-pakketten hebben gestuurd naar het aangevallen systeem.

3 PREVENTIE

Om systemen en diensten te beschermen tegen DDoS-aanvallen is het noodzakelijk om een aantal preventieve maatregelen te nemen. Deze maatregelen moeten ervoor zorgen dat:

1. Het mogelijk is om snel en tijdig te kunnen reageren
2. De impact van een DDoS-aanval kan worden beperkt
3. Een aanval kan worden gedetecteerd en vastgelegd voor een eventuele strafrechtelijke vervolging

De meeste maatregelen kunt u zelf uitvoeren, maar een aantal maatregelen kunt u door anderen laten uitvoeren. Zo is het mogelijk om werkafspraken te maken met uw (hosting-)provider. Een provider kan namelijk hulp bieden bij het detecteren en blokkeren van een DDoS-aanval. De meeste providers beschikken over krachtige routers of oplossingen die hulp kunnen bieden bij een DDoS-aanval. Hieronder volgen een aantal adviezen over preventieve maatregelen die u of de provider kunt nemen.

3.1 Anti-spoofing mechanismen

Het is onmogelijk om alle IP-spoofing tegen te gaan. Daarom is het noodzakelijk om de kans op IP-spoofing zoveel mogelijk te verkleinen. Via een aantal anti-spoofing mechanismen is het mogelijk om RFC1918 IP-adressen en IP-blokken die door IANA nog niet zijn uitgedeeld aan een LIR te blokkeren (Zie paragraaf 2.2 IP-spoofing).

3.1.1 Unicast Reverse-Path Forwarding (uRPF)

Routers hebben de mogelijkheid om IP-spoofing tegen te gaan met behulp van Unicast Reverse-Path Forwarding (uRPF). Routers weten aan de hand van de routeringstabel hoe IP-blokken kunnen worden bereikt. Om dataverkeer te routeren naar een IP-adres, moet de router bepalen via welke interface het verkeer moet worden gestuurd. Dat betekent dat de router ook kan bepalen dat het inkomende verkeer op een interface alleen afkomstig kan zijn van het IP-blok dat via de interface bereikbaar is. URPF controleert op een interface of een IP-pakket afkomstig is van een source IP-adres die volgens de routeringstabel bereikbaar is via de betreffende interface. Deze manier van anti-spoofing is zeer effectief in een netwerk met statische routes. Wanneer een dynamisch routeringsprotocol (bijvoorbeeld OSPF of BGP) in het netwerk wordt gebruikt, kan vanwege asymmetrische routering problemen optreden. In een netwerk met een dynamisch routeringsprotocol kan wel 'loose uRPF' worden gebruikt. Bij deze variant van uRPF wordt alleen gecontroleerd of een IP-pakket die een router ontvangt afkomstig is van een IP-adres die in de routeringstabel voorkomt. Er wordt dus niet gekeken op welke interface het IP-pakket is ontvangen. Netwerk-providers kunnen deze manier van filtering toepassen in hun netwerk of op uw internet-verbinding. Het is daarom raadzaam om dit eens na te vragen bij uw netwerk- of hosting-provider.

3.1.2 Bogon list

Zo is er een zogenaamde 'bogon list' van IP-blokken die nog niet door IANA zijn uitgegeven. IP-blokken die op deze lijst staan vermeld kunnen met behulp van routers en firewalls worden geblokkeerd. Deze lijst wordt actief bijgehouden en is op allerlei manieren op te vragen. Meer informatie vindt u via:

http://www.cymru.com/Bogons/

3.1.3 Access Control List (ACL)

Een Access Control List (ACL) wordt gebruikt om dataverkeer te reguleren. Met behulp van een ACL kan een source of destination IP-adres en/of protocol worden toegestaan of worden geblokkeerd. Zo is het mogelijk om een ACL te maken waarmee al het IP-verkeer dat afkomstig is van IP-adressen uit de hiervoor genoemde 'Bogon list' te blokkeren. Een ACL is niet altijd de beste oplossing. Wanneer de grote DDoS-aanval wordt uitgevoerd waarbij zeer veel verschillende source IP-adressen worden gebruikt, kan een ACL een te grote belasting zijn voor een router. Elk eerste IP-pakket dat afkomstig is van een source IP-adres moet met behulp van de ACL worden gecontroleerd. Wanneer de ACL zeer groot is, is het controleren een zeer intensieve handeling voor de router. Netwerk- en hostingproviders kunnen u in dergelijke situatie helpen. Zij beschikken over krachtige routers die op andere manieren het verkeer kunnen blokkeren.

3.2 Firewalls

Een firewall biedt vaak een goede eerste stap als maatregel tegen een DDoS-aanval. Firewalls zijn over het algemeen goed in staat om op IP-niveau, netwerkverkeer te filteren. Tegenwoordig zijn firewalls ook steeds vaker in staat om op de applicatie-laag bepaalde filtering toe te passen waardoor voor bepaalde protocollen zoals HTTP, FTP en SMTP er al kan worden gekeken of het verkeer dat wordt bekeken, voldoet aan de daarvoor beschreven RFCs. Echter, DDoS-aanvallen kunnen worden uitgevoerd met legitiem netwerkverkeer waardoor de firewall niet zal herkennen dat er een aanval wordt uitgevoerd.

Soms is het middels bepaalde settings wel mogelijk om de firewall te 'vertellen' wat normaal gedrag is van een bepaalde verkeersstroom (bijvoorbeeld het maximaal aantal connecties vanaf 1 specifiek adres). Hierdoor is het in sommige omstandigheden mogelijk een DDoS-aanval te herkennen en mogelijk tegen te houden. Controle op applicatieniveau van dataverkeer kost echter wel veel capaciteit van het filteringsysteem en kan indien de aanval zeer groot is, het firewallsysteem laten crashen. Feitelijk is de DDoS-aanval in zo'n geval geslaagd aangezien er geen verkeer meer mogelijk is.

3.3 Hardening systemen

Om de prestaties van uw systemen te verbeteren ten tijde van een DDoS-aanval is het mogelijk om de TCP-/IP-stack te configureren. Dit geldt met name voor systemen die een dienst of service (bijvoorbeeld een webserver) aanbieden of voor firewalls. Om de TCP/IP-stack te configureren is wel een grondige kennis van het besturingssysteem een vereiste. Wijzigingen in de TCP/IP-stack worden op kernelniveau doorgevoerd en hebben daarom een grote impact op het functioneren van uw systeem. Het is daarom ook raadzaam om alle wijzigingen in een testomgeving te onderzoeken.

Om uw prestaties van uw systeem te verbeteren kunt u de volgende wijzigingen doorvoeren in de TCP/IP-stack:

1. Vergroten van de 'TCP window size'. Deze parameter zorgt voor een meer efficiënte transport van grote hoeveelheden data. De aanpassing van deze parameter heeft wel een effect op andere processen. Een vergroting van de 'TCP window size' leidt tot meer geheugengebruik voor een TCP-sessie. Dat betekent dat er minder geheugen vrijkomt voor andere processen. Een grondige kennis van het systeem is dus een vereiste om de juiste waarde voor de parameter 'TCP window size' in te stellen. Een te grote of te kleine waarde van deze parameter kan zelfs het resultaat van een Denial-of-Service-aanval alleen maar bevorderen.
2. Vergroten van buffers voor:
    - Half open sockets (SYN ontvangen, SYN|ACK verzonden)
    - Volledig geopende sockets die op een 'accept()' wachten van de applicatie
3. Verlaag de time-out waarde van de TIME_WAIT-status.
   Vaak blijven sockets te lang in de TIME_WAIT-status staan, omdat de cliëntapplicaties de TCP-sessies niet correct afsluiten. Kwaadwillenden kunnen hiermee ook een Denial-of-Service veroorzaken. Verlaag daarom de time-out waarden van de TIME_WAIT–status naar bijvoorbeeld 60 seconden. Maar deze is sterk afhankelijk van uw besturingssysteem en de applicaties die worden gebruikt.

3.4 Aandacht voor de (netwerk)omgeving

'Een ketting is zo sterk als de zwakste schakel'. Deze uitdrukking geldt ook voor het beveiligen van systemen en specifiek voor het wapenen tegen een DDoS-aanval. Wanneer uw systemen optimaal beveiligd zijn, maar de (netwerk)omgeving is niet beveiligd, bestaat er nog steeds een risico voor een geslaagde DDoS-aanval. Kwaadwillenden kunnen namelijk de niet-beveiligde systemen aanvallen en vervolgens de internetverbinding dusdanig overbelasten zodat uw systemen ook niet meer bereikbaar zijn.
Zorg er dus voor dat alle systemen op het netwerk optimaal zijn beveiligd. Indien uw systemen bij een hosting-provider zijn ondergebracht, is het raadzaam om na te gaan hoe de hosting-provider zijn netwerk heeft ingericht. Systemen van andere klanten van de hosting-provider kunnen ook een risico vormen voor uw syste-

men. Het is natuurlijk ondoenlijk om hier een risicoanalyse van te maken, maar het is zeker iets waar u rekening mee dient te houden.

3.5 Afspraken met (hosting) providers

Aangezien het doel van een DDoS-aanval is om uw systemen onbereikbaar te maken, is de hulp van een provider noodzakelijk. Provider betekent in deze context de netwerk-provider die uw systemen internet-conectiviteit biedt. Indien uw systemen bij een hosting-provider zijn ondergebracht, dan wordt de hosting-provider bedoeld.
De meeste providers bieden de mogelijkheid om werkafspraken te maken. In dergelijke afspraken kunnen een aantal zaken worden vastgelegd om een DDoS-aanval snel tegen te gaan. Om een DDoS-aanval tegen te gaan zijn krachtige systemen nodig. De meeste providers beschikken vaak over krachtige routers die hulp kunnen bieden om een DDoS-aanval te kunnen blokkeren. In hoofdstuk 6 ‘De rol van de provider’ wordt een nadere toelichting gegeven over wat een provider voor u kan betekenen.

4 DETECTIE

Naast de preventieve maatregelen is het noodzakelijk om een DDoS-aanval te kunnen signaleren. Zoals eerder is uitgelegd gelden de volgende eigenschappen voor een Denial-of-Service-aanval:

- Poging om een netwerk te overspoelen met dataverkeer, waarmee legitiem dataverkeer niet meer kan doorkomen.
- Poging om connecties tussen twee systemen te verbreken.
- Poging om een gebruiker geen toegang te geven tot een systeem.
- Poging om een service op een systeem te onderbreken.

Dit hoofdstuk gaat wat dieper in de aspecten om de eigenschappen van een DDoS-aanval te kunnen herkennen.

4.1 Vastleggen van basisgedrag

Om een DDoS-aanval te kunnen waarnemen, is het ten eerste noodzakelijk dat er een basisgedrag is geformuleerd van de systemen en netwerkomgeving. Dit basisgedrag is het vastleggen van het gemiddelde bezoek en benutting van uw systemen en netwerk.
Het basisgedrag is een verzameling van gegevens die een beeld geven van uw systemen in een normale situatie. Gegevens die nodig zijn om het basisgedrag van uw systemen vast te leggen:

1. Het gemiddelde gebruik van de bandbreedte van de internet-verbinding
2. De gemiddelde pakketgrootte van het dataverkeer
3. Het gemiddelde gebruik van geheugen
4. Het gemiddelde gebruik van processoren
5. Het gemiddelde van lees- en schrijfacties op een harde schijf
6. Het gemiddelde van het aantal bezoekers/gebruikers

Deze gegevens dienen als basis om afwijkingen te kunnen herkennen. Periodiek moet het basisgedrag opnieuw worden vastgelegd zodat er rekening wordt gehouden met eventuele groei van het gebruik.
Wanneer uw systemen zijn ondergebracht bij een hosting-provider, is het niet altijd mogelijk om te beschikken over alle gegevens. Het is daarom raadzaam om na te gaan of uw hosting-provider kan helpen om inzicht te geven in bepaalde gegevens, zoals bijvoorbeeld het gebruik van bandbreedte of gemiddelde pakketgrootte.

4.2 Loggegevens en monitoring

De meeste besturingssystemen hebben de mogelijkheid om te loggen wat voor activiteiten op een systeem plaatsvinden en op welk tijdstip dat is gebeurd. Deze loggegevens zijn essentieel om het gedrag van een systeem te kunnen monitoren. Loggegevens spelen daarom ook een grote rol bij de vastlegging van een Denial-of-Service-aanval die op een systeem plaatsvindt.

Systeem- en applicatiegegevens worden meestal alleen naar log-bestanden op het systeem weggeschreven. Wanneer kwaadwillenden op een systeem inbreken, zullen zij direct hun sporen of handelingen willen verbergen. Daarom worden vaak de log-bestanden verwijderd of dusdanig verminkt zodat deze niet meer leesbaar zijn. Bij aanvallen op afstand kunnen ook vele opzettelijke handelingen worden uitgevoerd die gelogd worden naar de log-bestanden. Dergelijke loggegevens maken analyse van logbestanden erg lastig en tijdrovend, maar dienen ook als afleiding voor de daadwerkelijke aanvalspoging.
Om de loggegevens als bewijslast te kunnen gebruiken is het belangrijk om een goede log-strategie te ontwikkelen. De belangrijkste elementen bij het opzetten van een log-strategie zijn:

- Integriteit waarborgen van loggegevens
- Correlatie en monitoring
- Synchronisatie van datum en tijd

4.2.1 Integriteit waarborgen van loggegevens

Het eerste element bij het opzetten van een log-strategie is het waarborgen van de integriteit van de loggegevens. De integriteit van loggegevens kunnen het beste worden behouden wanneer de loggegevens op een andere server worden bewaard. Een andere mogelijkheid is om de loggegevens op een opslagmedium te bewaren. Echter, het bewaren van loggegevens op een opslagmedium maakt het lastig om goede en snelle analyses te maken.
Loggegevens kunnen via het syslog-protocol op een eenvoudige manier worden weggeschreven naar een syslog-server. Daarnaast kunnen de loggegevens nog steeds worden opgeslagen naar log-bestanden op het systeem. Verminking van de loggegevens is nog steeds mogelijk omdat de loggegevens die de syslog-server ontvangt meestal niet worden gefilterd. Daarom dient de syslog-server volledig afgeschermd te zijn zodat kwaadwillenden niet de mogelijkheid hebben om de loggegevens te kunnen vernietigen. Wanneer de log-bestanden niet vernietigd kunnen worden, zijn de sporen en handelingen die voor de verminking van de loggegevens hebben plaatsgevonden nog steeds intact en bewaard.
Ook is het mogelijk om de authenticiteit van de loggegevens te behouden door encryptie te gebruiken bij het versturen van de loggegevens naar de syslog-server. Encryptie is geen standaardonderdeel van het syslog-protocol. Daarom is het gebruik van encryptie bij het syslog-protocol afhankelijk per besturingssysteem. Microsoft Windows kan bijvoorbeeld geen encryptie gebruiken bij het syslog-protocol.

4.2.2 Correlatie en monitoring

Wanneer een DDoS-aanval wordt uitgevoerd op een systeem, is het belangrijk dat er een snelle en goede analyse van de aanval kan worden gemaakt. Om een goede analyse te kunnen maken, dient het eerder beschreven basisgedrag als referentiekader te worden gebruikt. Als de loggegevens van systemen worden bewaard op een syslog-server, is het makkelijker om een analyse te maken. Immers alle gegevens staan op een centrale plaats. Daardoor is het mogelijk om loggegevens van diverse systemen of applicaties te kunnen correleren. Er zijn diverse programma's die de analyse van loggegevens eenvoudiger kunnen maken.

Een ander voordeel van een centrale opslagplaats van loggegevens is de mogelijkheid om activiteit te kunnen monitoren. Systeembeheerders kunnen door middel van een monitoringsprogramma direct worden ingelicht wanneer DDoS-aanval wordt uitgevoerd. Een monitoringsprogramma kan dus ook bijdragen aan een snelle detectie van een Denial-of-Service.

4.2.3 Synchronisatie van datum en tijd

Om de handelingen op een of meerdere systemen te correleren is het belangrijk dat de handelingen in een logische tijdsvolgorde kunnen worden gezet. Daarom moeten de systeemtijd van een systeem gesynchroniseerd zijn. Wanneer meerdere systemen worden gebruikt, dient de systeemtijd van alle systemen gelijk te zijn. Een systeem kan zelfstandig een systeemtijd handhaven. Het nadeel is dat de systeemtijd dan niet centraal gesynchroniseerd is zodat afwijkingen in systeemtijden kunnen optreden. Tijd kan via het NTP(Network Time Protocol)-protocol centraal worden beheerd voor alle systemen. Alle systemen worden dan via een NTP-server van dezelfde systeemtijd voorzien. Er zijn op het Internet diverse NTP-servers de tijd van systemen kan synchroniseren

4.3 Indicaties van een DDoS-aanval

DDoS-aanvallen komen in verschillende vormen voor. Hieronder volgen een aantal indicaties die mogelijk kunnen duiden op een Denial-of-Service-aanval. Als uitgangspunt is het eerder beschreven basisgedrag genomen.

1. Het gemiddelde gebruik van de bandbreedte van de internet-verbinding neemt toe
2. De gemiddelde pakketgrootte van het dataverkeer neemt af
3. Het gemiddelde gebruik van geheugen neemt toe
4. Het gemiddelde gebruik van processoren neemt toe
5. Het gemiddelde van lees- en schrijfacties op disken neemt toe
6. Het gemiddelde van het aantal bezoekers/gebruikers neemt toe
7. Het gemiddelde van het aantal ontvangen SYN-pakketten neemt toe

De bovenstaande indicaties hoeven niet alleen op het aangevallen systeem of dienst op te treden. Ook andere systemen die bij de DDoS-aanval betrokken zijn, kunnen indicaties opleveren. Zo is vaak het gebruik van de processor op een router een goede indicator voor een DDoS-aanval. Bij de meeste routers wordt de processor benut om het eerste IP-pakket van een datastroom te indentificeren.

Vervolgens wordt elk IP-pakket herkend die bij deze datastroom hoort. Dat betekent dat niet elk IP-pakket uit deze datastroom wordt verwerkt door de processor van de router. Dit zorgt dus voor een efficiënt gebruik van de processor. In paragraaf 4.7 'Netflow' wordt verder ingegaan op deze techniek.Bij de meeste DDoS-aanvallen worden grote hoeveelheden datastromen tegelijkertijd gegenereerd richting het aangevallen systeem of dienst. De processor van de router wordt daardoor zwaarder belast omdat het eerste IP-pakket van vele datastromen moet worden geidentificeerd. De belasting van de processor is dus een goede indicator om een Denial-of-Service-aanval te kunnen herkennen.

4.4 Firewalls

Een DDoS-aanval is moeilijk te herkennen op een firewall. De firewall logt vaak alleen netwerkverkeer dat wordt tegen gehouden, niet het verkeer dat is toegestaan. Een DDoS-aanval heeft echter vaak als eigenschap dat het legitiem verkeer is, alleen dan heel erg veel. De meeste firewalls zijn niet in staat dit patroon te herkennen. Er zijn firewalls die de mogelijkheid hebben om aan te geven hoeveel connecties er maximaal mogen worden gemaakt vanaf 1 IP-adres. Dit zou een methodiek kunnen zijn om een DDoS-aanval te herkennen op de firewall, maar blijft erg beperkt.

Indien de aanval plaatsvindt naar niet standaard protocolpoorten, en de firewall logt het verkeer dat naar deze poorten wordt gestopt, dan zou aan de hand van de firewall logging kunnen worden geconcludeerd dat er een aanval wordt uitgevoerd.

4.5 Intrusion Detection Systeem (IDS)

Omdat een firewall vaak niet goed in staat is om op applicatieniveau filtering toe te passen en de meeste aanvallen worden uitgevoerd naar diensten die door de firewall moeten worden doorgelaten, is er de zogenaamde IDS bedacht. Een Intrusion Detection Systeem (IDS) is in staat om te controleren of de inhoud van een netwerkpakket aan bepaalde voorwaarden voldoet. Hierdoor is een IDS in staat om van toegestane legitieme verkeersstromen te bepalen wat 'normaal' is en wat een aanval zou kunnen zijn. Een voorbeeld hiervan is verkeer dat naar een web-server wordt toegestaan. Normaliter is dit verkeer dat gebruik maakt van TCP port 80 en wordt dit verkeer door de firewall toegestaan. Echter, kwetsbaarheden in de web-server-software maken het mogelijk om over TCP poort 80 een aanval naar de webserver uit te voeren. Een IDS is in staat om zo'n aanval te herkennen, omdat een IDS 'kijkt' in het verkeer om te zien of het gewoon web-server verkeer is of een aanval. Hiervoor dient het IDS-systeem wel van de kwetsbaarheden op de hoogte te zijn om dit ook te kunnen herkennen.

Een IDS is niet gemaakt om DDoS-aanvallen te herkennen maar meer om bekende aanvallen naar kwetsbaarheden in software te herkennen. De techniek die hiervoor wordt gebruikt stelt het systeem wel in staat om een DDoS-aanval te herkennen. Dit kan omdat een DDoS-aanval vaak aan bepaalde patronen voldoet waardoor het mogelijk is het IDS-systeem te 'leren' hoe een DDoS-aanval er uit

ziet. Aangezien er vele DDoS-aanvalstechnieken zijn, zal het tijd en inspanning kosten om een IDS van de benodigde regels te voorzien en bij te houden.

4.6 Intrusion Prevention Systeem (IPS)

Voor Intrusion Prevention Systemen (IPS) gelden dezelfde opmerkingen als die beschreven staan voor IDS. Het verschil is alleen dat IPS-systemen in staat zijn om verkeersstromen te stoppen. Dit kan hetzij door het systeem zelf worden gedaan indien het verkeer door het IPS-systeem heen gaat (IPS in bridgemodus) ofwel door het IPS-systeem regels te laten plaatsen in een firewall of Access Control Lists (ACL) te laten plaatsen in routers.

Een IPS is niet gemaakt om DDoS-aanvallen te herkennen maar meer om bekende aanvallen naar kwetsbaarheden in software te herkennen. De techniek die hiervoor wordt gebruikt stelt het systeem echter wel in staat om een DDoS-aanval te herkennen. Dit kan omdat een DDoS-aanval vaak aan bepaalde patronen voldoet waardoor het mogelijk is het IPS-systeem te ‘leren’ hoe een DDoS-aanval er uit ziet. Aangezien er vele DDoS-aanvalstechnieken zijn, zal het tijd en inspanning kosten om een IPS van de benodigde regels te voorzien.

Een IPS is dus een IDS met als extra mogelijkheid verkeer te stoppen. Als preventie middel is een IPS dus in principe goed geschikt voor het tegengaan van DDoS-aanvallen. Hierbij moet wel worden opgemerkt dat zowel een IDS als een IPS te maken kunnen krijgen met zogenaamde ‘False Positives’. Meldingen dat een aanval wordt herkend terwijl het legitiem verkeer is dat niet mag worden tegengehouden. In het geval van een IDS is een ‘False Positive’ niet erg, maar een IPS zou zo geconfigureerd kunnen staan dat bij herkenning het verkeer wordt tegengehouden. Als dit niet terecht blijkt te zijn, is het IPS-systeem op dat moment zelf onderdeel van de DDoS-aanval. Tevens kan een aanvaller indien hij weet heeft van de aanwezigheid van het IPS-systeem, misbruik maken van deze situatie, en de IPS misbruiken voor zijn aanval.

4.7 Netflow

‘Flow-based accounting’ , ook wel Netflow genoemd, is een aanvulling op het proces dat de route van een IP-pakket bepaalt (ook wel ‘route-lookup’ genoemd). Netflow is een toepassing die op routers kan worden gebruikt. Wanneer het eerste IP-pakket van een datastroom binnenkomt op een router, wordt een hash-waarde berekend aan de hand van diverse velden uit de IP-header en/of TCP-header. De hash-waarde wordt vervolgens vergeleken met een zogenaamde ‘flow cache’. Als de hash-waarde nog niet in de ‘flow cache’ voorkomt, wordt een route-lookup gedaan en vervolgens wordt het IP-pakket verzonden naar zijn bestemming. Nadat het IP-pakket is verzonden wordt een zogenaamde ‘flow’ in de ‘flow cache’ geregistreerd. Voor elk IP-pakket dat binnenkomt op de router wordt de hash-waarde

berekend en vervolgens vergeleken met de ‘flow cache’. Als een zelfde hash-waarde wordt geconstateerd in de ‘flow cache’, wordt het pakket geteld in de statistiek van de betreffende flow. Tevens wordt er geen route-lookup gedaan, maar wordt het IP-pakket via hetzelfde pad verzonden, als dat het eerste IP-pakket is gestuurd.

Netflow levert voor routers een aanzienlijke prestatieverbetering op. Maar Netflow is ook een zeer effectieve manier om een DDoS-aanval te kunnen signaleren. Routers kunnen de Netflow-gegevens transporteren naar een centrale opslagplaats. Diverse applicaties kunnen de opgeslagen Netflow-data interpreteren. Er zijn zelfs specifieke applicaties die kunnen monitoren op Denial-of-Service-aanvallen.
Netflow heeft ook een schaduwzijde, vanwege de grote hoeveelheid data die gegenereerd wordt. Er is veel diskcapaciteit nodig om de opgeslagen data op te vangen. Tevens moeten de routers de Netflow-data transporteren. Deze data moet het liefst via een aparte managementinterface worden gestuurd naar de centrale opslagplaats. Wanneer de Netflow-data via bijvoorbeeld een internet-verbinding verstuurt, kan de grote hoeveelheid Netflow-data ten tijde van een DDoS-aanval de internet-verbinding overbelasten. Daarmee wordt dus meegeholpen aan een Denial-of-Service.

Netflow kan niet op iedere router worden gebruikt. De meeste netwerk-providers gebruiken Netflow in hun netwerk voor strategische doeleinden, maar ook voor beveiligingsdoeleinden. Wanneer u niet over krachtige routers beschikt die met Netflow kunnen omgaan, is het raadzaam om na te gaan of uw netwerk-provider hulp kan bieden. Vele netwerk-providers hebben mechanismen die aan de hand van Netflow-data een Denial-of-Service-aanval kunnen signaleren. Netwerk-providers zijn vaak bereid om op operationeel niveau afspraken te maken over het bieden van hulp bij een DDoS-aanval. Zo is het mogelijk om bijvoorbeeld bij speciale evenementen een afspraak te maken over hulp in geval van problemen.

5 REACTIE

De maatregelen die bij de hoofdstukken ‘Preventie’ en ‘Detectie’ zijn beschreven dienen om snel en adequaat te kunnen handelen ten tijde van een DDoS-aanval. Deze maatregelen moeten dus uw reactie op een DDoS-aanval ondersteunen. Maar hoe kunt u het beste reageren op een Denial-of-Service-aanval ? Dit hoofdstuk beschrijft een aantal opties om een DDoS-aanval te stoppen. Naast een aantal technische opties wordt ook het nut van procedures beschreven.

5.1 Procedures

Om tijdens een Denial-of-Service-aanval snel en adequaat te reageren, is het van belang om te handelen aan de hand van op voorhand afgesproken procedures. In deze procedures worden de verantwoordelijkheden vastgelegd en hoe de communicatiekanalen verlopen.
Op voorhand moet bekend zijn wie verantwoordelijk is voor het technisch beheer van de systemen. Tevens moet het duidelijk zijn welke manager ten tijde van een calamiteit een beslissing op managementniveau kan nemen.
Communicatie is met name van belang tussen management en technische medewerkers. Tijdens een DDoS-aanval moet er soms een beslissing worden genomen die impact kan hebben op bijvoorbeeld een dienstverlening. Management moet deze beslissing nemen en dit direct kunnen bevestigen aan een systeem- of netwerkbeheerder die een aanpassing op systemen kan doorvoeren. Op voorhand moet er dus ook bekend zijn wie er verantwoordelijk is voor het beheer van de systemen.
Wanneer uw systemen zijn ondergebracht bij een hosting-provider dienen er duidelijke afspraken te worden gemaakt over het handelen tijdens een DDoS-aanval. De provider zal de aanval moeten kunnen signaleren en vervolgens u zo snel mogelijk op de hoogte stellen. Spreek ook op voorhand af waar scheidslijn ligt tussen besluiten die u kunt nemen en besluiten die de hosting-provider zelfstandig neemt. Dit is van belang omdat u de eigenaar van het systeem bent, terwijl deze systemen in een netwerk staan die van de hosting-provider is.

5.2 Access Control List (ACL)

Zoals in paragraaf 3.1.3 ‘Access Control List (ACL)’ is beschreven, wordt een ACL gebruikt om dataverkeer te reguleren. Met behulp van een ACL kan een source of destination IP-adres en/of protocol worden toegestaan of worden geblokkeerd. Bij een DDoS-aanval zijn mechanismen nodig die een aanval moeten kunnen blokkeren zonder een te grote belasting voor een systeem te veroorzaken. Naarmate een ACL steeds groter wordt, wordt de belasting van het systeem ook steeds groter. Elk eerste IP-pakket dat afkomstig is van een source IP-adres moet met behulp van de ACL worden gecontroleerd. Er zijn betere oplossingen om een DDoS-

aanval te stoppen zoals 'NULL routing (zie paragraaf 5.3) of Quality-of-Service (zie paragraaf 5.4).
Netwerk- en hosting-providers kunnen u ook helpen om dataverkeer te blokkeren. Zij beschikken over krachtige routers die op andere manieren het verkeer kunnen blokkeren.

5.3 NULL-routing

'Null routing' betekent dat een IP-pakket wordt gerouteerd naar een destination IP-adres dat gerelateerd is met een zogenaamde NULL-interface. Een NULL-interface is een virtuele interface die nergens mee is verbonden en kan dataverkeer ontvangen of versturen. Oftewel, het IP-pakket verdwijnt. Dit wordt ook wel 'Black Hole Routing' genoemd. NULL-routing is een zeer effectieve manier van het blokkeren van een DDoS-aanval.
Ten tijde van een DDoS-aanval is het mogelijk om op een router de source IP-adressen die gebruikt worden voor de DDoS-aanval uit te voeren te routeren naar een NULL-interface. Uiteraard moet u natuurlijk wel zeker weten dat het source IP-adres misbruikt wordt voor de aanval en dat het mogelijk is om het IP-adres te blokkeren. Er is echter een probleem wanneer het source IP-adres op deze manier wordt gerouteerd naar het NULL-interface: het dataverkeer dat afkomstig van het source IP-adres bereikt nog steeds uw systemen. Alleen het dataverkeer dat uw systemen terugsturen wordt door de router naar het NULL-interface gerouteerd. Immers, de router routeert op basis van het destination IP-adres waardoor dus alleen het NULL-interface wordt gebruikt voor het dataverkeer naar het source IP-adres. Deze methode zal dus niet effectief zijn om de aanval te kunnen stoppen. NULL-routing moet daarom in combinatie met een ander mechanisme (bijvoorbeeld een anti-spoofing mechanisme) worden gebruikt zodat het mogelijk is om het verkeer dat afkomstig is van een verdacht source IP-adres te kunnen blokkeren. Unicast Reverse-Path Forwarding (uRPF, zie paragraaf 3.1.1) is een goed anti-spoofing mechanisme dat in combinatie met NULL-routing kan worden gebruikt. Dataverkeer dat afkomstig is van een verdacht source IP-adres, en dat wordt gerouteerd wordt naar een NULL-interface, zal worden weggegooid wanneer uRPF op de router gebruikt.
NULL-routing is ook zeer effectief in combinatie met een dynamisch routeringsprotocol zoals BGP (Border Gateway Protocol) of OSPF (Open Shortest Path First). De meeste netwerkproviders gebruiken deze combinatie vaak. Zij kunnen in geval van een calamiteit helpen om dataverkeer te routeren naar een NULL-interface.

5.4 Quality-of-Service (QoS)

Quality-of-Service (QoS) wordt normaal gesproken gebruikt om een bepaalde hoeveelheid bandbreedte te reserveren voor bijvoorbeeld bepaalde IP-adressen of een bepaald protocol. QoS wordt met name gebruikt om ervoor te zorgen dat audio- en videodatastromen voldoende bandbreedte hebben.
QoS kan ook worden gebruikt om een Denial-of-Service-aanval te blokkeren. Zo is het bijvoorbeeld mogelijk om een SYN-aanval tegen te gaan. Met QoS kunt u bepalen wat u met het dataverkeer wilt doen:

1. Blokkeren
2. Limiteren van de bandbreedte
3. Niets doen

De beslissing is afhankelijk van wat voor source IP-adressen worden gebruikt bij een DDoS-aanval. Bij paragraaf 2.2 'IP spoofing' vindt u een overzicht van wat voor IP-adressen bij een DDoS-aanval kunnen worden gebruikt.

1. RFC1918 IP-adressen. Dit zijn IP-adressen die op private netwerken kunnen worden gebruikt.

   QoS-oplossing:
   Aangezien deze IP-adressen niet via het Internet mogen worden gerouteerd, kunt u met behulp van QoS al het dataverkeer dat afkomstig van een dergelijk source IP-adres blokkeren.

2. IP-blokken die door IANA nog niet zijn uitgedeeld aan een LIR (Local Routing Registry), zoals bijvoorbeeld RIPE.

   QoS-oplossing:
   Aangezien deze IP-adressen nog niet via het Internet worden gerouteerd, kunt u met behulp van QoS al het dataverkeer dat afkomstig van een dergelijk source IP-adres blokkeren.

3. IP-adressen die door een LIR of een provider niet nog niet zijn uitgedeeld. Providers beschikken vaak over grote IP-blokken waarvan nog niet alles is uitgedeeld. De IP-adressen die nog niet in gebruik zijn, kunnen worden gebruikt voor IP-spoofing.

   QoS-oplossing:
   Aangezien deze IP-adressen nog niet via het Internet worden gerouteerd, kunt u met behulp van QoS al het dataverkeer dat afkomstig is van een dergelijk source IP-adres blokkeren. U kunt alleen maar aan de hand van het routeringsprotocol BGP (Border Gateway Protocol) duidelijk bepalen welk gedeelte van een IP-blok van een bepaalde provider nog niet in gebruik is. Wanneer u geen gebruik maakt van BGP is het raadzaam om het verkeer dat afkomstig is van een dergelijk source IP-adres door te laten of de bandbreedte te limiteren.

4. IP-adressen die geen IP-pakketten hebben gestuurd.

   QoS-oplossing:
   Afhankelijk van het source IP-adres is het mogelijk om op basis van QoS te kiezen voor het toelaten, limiteren of blokkeren van het dataverkeer. Als u bijvoorbeeld een web-server gebruikt voor het Nederlandse publiek en de server wordt aangevallen vanaf source IP-adressen uit het buitenland, en die op het Internet worden gerouteerd, is het mogelijk om op basis van QoS het verkeer te blokkeren.

6 DE ROL VAN DE PROVIDER

Zoals al vaker in dit document is aangegeven, is de rol van uw provider van groot belang bij een DDoS-aanval. Provider betekent in deze context de netwerk-provider die uw internetconnectie beheert, of de hosting-provider die een netwerk en eventueel uw systemen beheert. De rol van de provider wordt soms over het hoofd gezien of onderschat, maar de meeste providers kunnen u op de volgende gebieden helpen:

1. Met behulp van een goed anti-spoofing mechanisme wordt verkeer geblokkeerd dat afkomstig is van RFC1918 IP-adressen of van IP-adressen die door IANA nog niet zijn gealloceerd.
2. Met behulp van krachtige systemen, zoals bijvoorbeeld routers, kan op een effectieve manier een DDoS-aanval worden gestopt of beperkt.
3. Met behulp van een detectiemechanisme, zoals bijvoorbeeld Netflow, kan een DDoS-aanval worden gesignaleerd.
4. Providers hebben contacten met hun upstream-providers of andere netwerkrelaties zoals peers om een aanval in andere netwerken, dan het netwerk van uw provider, te blokkeren.

Bij de meeste providers is het mogelijk om op een operationeel niveau werkafspraken te maken over hoe te handelen ten tijde van een DDoS-aanval. Providers beschikken vaak over procedures om snel en adequaat te kunnen optreden. Dit is bijvoorbeeld erg nuttig wanneer u een groot evenement via het Internet organiseert. U kunt dan met uw provider afspraken maken voor bijvoorbeeld extra monitoring.

Zoals gezegd beschikken de meeste providers over middelen om u te helpen bij calamiteiten. Dat betekent dus dat niet alle providers die mogelijkheid hebben. Wanneer u een keuze moet maken voor een bepaalde (hosting-)provider, is het raadzaam om te overwegen of de provider ten tijde van calamiteiten kan helpen. Ga daarom altijd na of uw provider ondersteuning kan bieden om een DDoS-aanval te stoppen of te beperken.

7 CONCLUSIE

Denial-of-Service-aanvallen zijn een van de moeilijkste aanvallen om tegen te wapenen. Maar er zijn diverse manieren op gebied van preventie, detectie en reactie die hulp kunnen bieden om een DDoS-aanval te stoppen of te beperken.

Om ten tijde van een DDoS-aanval snel en adequaat te kunnen handelen, is het raadzaam om op voorhand goed na te denken over preventie, detectie en reactie. Daarbij is de rol van uw provider van zeer groot belang. Naast de vele technische oplossingen is het vastleggen van verantwoordelijkheden en het gebruik van procedures noodzakelijk.

Het is raadzaam om het kennisniveau op peil te houden ten aanzien van (nieuwe) aanvalstechnieken en technologieën die een DDoS-aanval kunnen voorkomen, herkennen of afslaan. Wanneer u inzicht heeft in deze trends kunt u als goed onderlegd gesprekspartner fungeren in contacten met uw provider.

DDoS-aanvallen kunnen een grote impact hebben op een dienstverlening of bedrijfsvoering. Het management van een organisatie moet daarvan bewust zijn. Adviseer daarom het management inhoudelijk over de maatregelen op het gebied van preventie, detectie en reactie. Op deze manier kunt u aantonen dat de maatregelen noodzakelijk zijn.

8 APPENDIX

1. Best Practices for Preventing DoS/Denial of Service Attacks [Microsoft]
   http://www.microsoft.com/technet/security/bestprac/dosatack.mspx

2. Distributed Denial of Service (DDoS) Attacks/tools [Dave Dittrich]
   http://staff.washington.edu/dittrich/misc/ddos/

3. Algemene informatie en praktische tips over loggegevens [Marcus Ranum]
   http://www.loganalysis.org/

4. Microsoft TCP/IP-stack configuren [Microsoft]
   http://www.microsoft.com/technet/itsolutions/network/deploy/depovg/tcpip2k.mspx#EAAA

5. Unix-varianten TCP/IP-stack configuren [Team Cymru & USENIX]
   http://www.cymru.com/Documents/ip-stack-tuning.html
   http://www.usenix.org/publications/library/proceedings/bsdcon02/full_papers/lemon/lemon_html/index.html

6. RFC 2827: Network Ingress Filtering [P. Ferguson]
   ftp://ftp.isi.edu/in-notes/rfc2267.txt

7. The Bogon List [Team Cymru]
   http://www.cymru.com/Bogons/

8. Black Hole Routing [Chris Morrow & Brian Gemberling]
   http://www.secsup.org/Tracking/

9. Denial of Service (DoS) Attack Resources [P. Ferguson]
   http://www.denialinfo.com/

10. Netflow HOW-TO:
    http://www.linuxgeek.org/netflow-howto.php

11. Overzicht van Netflow
    http://www.switch.ch/tf-tant/floma/software.html

12. Handleiding Cybercrime [GOVCERT.NL]
    http://www.govcert.nl/render.html?it=218

9 DISCLAIMER

GOVCERT.NL betracht grote zorgvuldigheid bij het samenstellen en onderhouden van de informatie. GOVCERT.NL is echter niet verantwoordelijk voor de volledigheid, juistheid en actualiteit van de informatie en aanvaardt geen aansprakelijkheid voor eventuele directe of indirecte schade als gevolg van de activiteiten die door een gebruiker worden ondernomen op basis van de informatie, adviezen en waarschuwingen die door middel van dit document wordt verstrekt. Indien er verwezen wordt naar externe bronnen staat GOVCERT.NL niet garant voor de juistheid en volledigheid van deze informatie. Gezien de technologische ontwikkelingen wordt niet gepretendeerd dat het document uitputtend is.