



CENTER FOR
CYBERSIKKERHED

Vejledning

Beskyt mod DDoS-angreb

Indhold

Indledning	3
Overordnede anbefalinger.....	4
Læsevejledning	5
Fra DoS til DDoS	6
Forebyg og forsink DDoS-angreb	7
1. Undgå single point of failure	7
2. Indtænk internetudbydere	7
3. Anvend specialiseret udstyr	8
4. Brug de rigtige komponenter rigtigt	8
5. Husk Jeres DNS-servere	9
Håndter DDoS-angreb	11
1. Følg en DDoS-drejemåte	11
2. Håndter angrebet tidligt	11
3. Få ekstern hjælp	12
Referencer	13



Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

1. udgave april 2020. Revideret oktober 2022

Forsideillustration: pinkeyes/Shutterstock

Indledning

Enhver organisation, der er synlig og tilgængelig på internettet, er et potentielt mål for DDoS-angreb. Det er derfor vigtigt, at enhver organisation – stor som lille – tager de rette forholdsregler for at beskytte sig mod denne type af cyberangreb.

DDoS

DDoS står for Distributed Denial of Service og er et overbelastningsangreb.

Hackere udnytter kompromitterede computere til at generere usædvanligt store mængder datatrafik mod en hjemmeside (webserver) eller et netværk, så hjemmesiden eller netværket overbelastes.

Imens angrebet står på, er hjemmesiden eller netværket utilgængelig for legitim trafik.

Udsættes en organisation for DDoS-angreb kan det øjeblikkeligt forstyrre produktion og services. Angrebene er altid tidsbegrænsede og ophører typisk inden for 24 timer, men kan stadig medføre længerevarende konsekvenser på omdømme og økonomi.

Denne vejledning bidrager til at reducere risikoen for og ved DDoS-angreb ved at komme med en række anbefalinger til, hvordan man kan forebygge og forsinke angreb, samt til hvordan et angreb kan håndteres.

Vejledningen henvender sig først og fremmest til organisationens IT-ledelse, IT-driftsafdeling og IT-driftsleverandører. Det er hensigten, at anbefalingerne kan indgå i organisationens løbende arbejde med at forbedre eksisterende sikkerhedspraksis. Da mange organisationer i dag har outsourcet hele eller dele af IT-driften, kan vejledningen også bruges i dialogen med leverandørerne for at sikre, at disse har styr på de nødvendige foranstaltninger mod DDoS-angreb.

Overordnede anbefalinger

På de følgende sider opstilles og uddybes Center for Cybersikkerheds anbefalinger, som kan hjælpe organisationer med at reducere risikoen for og ved DDoS-angreb. Anbefalingerne i denne vejledning er generelle og kan bruges af de fleste organisationer, men skal ikke opfattes som en udtømmende liste. For mere organisationsspecifikke anbefalinger kan man kontakte it-sikkerhedsfirmaer.

Hvis en organisation i sin risikovurdering vurderer, at DDoS-angreb skal håndteres, anbefaler Center for Cybersikkerhed, at man:

- Opdaterer komponenter, herunder firewall, routere, switche, servere, applikationer og IoT-enheder, til seneste patch level. Det kan fjerne sårbarheder, der potentielt kan udnyttes af DDoS-angreb.
- Indgår aftaler om passende DDoS-beskyttelse med organisationens internetleverandører eller med de eksterne udbydere som hoster organisationens internetvendte tjenester.
- Implementerer dedikerede foranstaltninger der er specifikt designet til DDoS-beskyttelse. Dette kan både være i form af separate anti-DDoS-komponenter, der tilføjes i egen it-infrastruktur, eller som cloud-service.
- Er bekendt med og benytter mulige DDoS-sikkerhedsforanstaltninger i eksisterende netværksudstyr og software, der håndterer trafik fra internettet.
- Monitorerer sine netværk og applikationer, dels for hurtigt at kunne opdage et angreb, dels for at have et opdateret normalbillede af båndbredde (tilgængeligt og brugt). Det gælder særligt, hvis dele af den eksisterende DDoS-beskyttelse ikke er automatiseret men skal iværksættes manuelt ved angreb. Sørg for at monitoreringen ikke unødvendigt belaster netværkskapaciteten.
- Alternativt indgår aftaler om beskyttelse med en leverandør, der har specialiseret sig i at imødegå DDoS-angreb mod deres kunders infrastruktur.
- Sørger for at beredskabsplanen indeholder de rette kontakter til internetleverandører (ISP) og andre eksterne leverandører.

Læsevejledning

Denne vejledning er opdelt i to hovedafsnit, som kan indgå i organisationens risikohåndtering. Første afsnit har fokus på at forebygge og forsinke DDoS-angreb, mens andet afsnit har fokus på at håndtere et DDoS-angreb. Formålet med vejledningen er at beskrive de foranstaltninger, som imødegår DDoS-angreb over en bred kam, og begrænser sig derfor ikke til én bestemt angrebstype.

Hensigtsmæssig imødegåelse af DDoS-angreb bygger på alle de anbefalinger, der nævnes i denne vejledning. Ingen afsnit eller anbefalinger i denne vejledning bør derfor stå alene.

Visse af anbefalingerne vil benytte fagudtryk, som ikke nødvendigvis er uddybet. Dette bør man som læser være opmærksom på.

God læselyst.

Fra DoS til DDoS

Overbelastningsangreb har eksisteret næsten lige så længe, som internettet. I begyndelsen var det muligt at overbelaste en server ved at sende mange gentagne forespørgsler fra blot én computer (et DoS-angreb). Den samlede volumen ved den slags angreb er relativt lille og er sjældent en udfordring for en servers kapacitet i dag.

Metoden udviklede sig hurtigt til at inkludere flere tusinde kompromitterede computere. Fra et centralt sted bliver de styret til at sende store mængder datatrafik mod ét mål (et DDoS-angreb).

DDoS-angrebstyper

Volumen-angreb overbelaster kapaciteten (båndbredden) på internetforbindelsen.

Protokol-angreb overbelaster kapaciteten på en firewall, router eller anden netværkskomponent.

Applikations-angreb udnytter svagheder i programmerne på en netværkskomponent, eksempelvis en webserver.

Denne metode er også den mest udbredte i dag, blandt andet hjulpet godt på vej af udbredelsen af sårbare IoT-enheder, der let kan udnyttes i store botnets. Et botnet er et netværk af computere, routere, smartphones, og andre internetforbundne enheder, som indeholder applikationer eller malware, der gør det muligt at fjernstyre enhederne, således de kan indgå i et koordineret DDoS-angreb.

Der findes mange varianter af DDoS-angreb, eksempelvis er der en DDoS-teknik kaldet *"DNS Amplification"*. Her udnytter en angriber kompromitterede enheder til at sende forfalskede forespørgsler til en række DNS-servere, som i god tro returnerer forespørgslen til offerets IP-adresse. Datapakkerne, der returneres, er generelt mange gange større end forespørgslerne, og angrebet "forstærkes" derfor via DNS-serverne. Offerets system overvældes og overbelastes.

Fremgangsmåden for DDoS-angreb er grundlæggende den samme, men gennem årene er særligt antallet og størrelsen af de kraftigste angreb steget støt drevet af et stadig hurtigere internet og et øget antal internetforbundne enheder, der kan misbruges til at genere DDoS-trafik. I nogle tilfælde kombinerer angriberne endda de forskellige angrebstyper for at maksimere effekten. Det er derfor vigtigt, at organisationer holder sig opdateret inden for udviklingen og tilpasser sin risikostyring herefter.

Læs mere om DDoS-truslen og den generelle cybertrussel på www.cfcs.dk.

Forebyg og forsink DDoS-angreb

1. Undgå single point of failure

Alle internetvendte tjenester kan blive ramt af et DDoS-angreb. Man bør derfor have et konsolideret overblik over organisationens tilgængelige tjenester og de konsekvenser, det vil have for organisationen, hvis et DDoS-angreb medfører, at deres funktion påvirkes eller sættes ud af drift.

I sin vurdering bør man også overveje om der er specifikke trusselsaktører, der kan have en særlig interesse i og kapacitet til, at udføre et DDoS-angreb mod organisationen.

Geografisk fordeling af servere på forskellige netværk vil besværliggøre effekten af DDoS-angreb, da de typisk er koncentreret mod få mål. Derfor **anbefaler CFCS** at man overvejer at:

- Indbygge redundans i it-infrastrukturen.
- Installere "load balancers", som fordeler datatrafikken jævnt mellem organisationens internetvendte serverne.
- Opbevare data på flere servere på forskellige geografiske lokationer og på forskellige netværk via et Content Distribution Network (CDN).
- Benytte separate internetforbindelser til henholdsvis administrative services og web-services, så et DDoS-angreb mod den ene service ikke påvirker begge services samtidigt.
- Udarbejde en procedure, der sikrer, at test udføres jævnligt, når der sker væsentlige ændringer i netværkstopologien eller forud for forventede spidsbelastninger af forretningens tjenester.

2. Indtænk internetudbyderne

Mange internetleverandører (ISP'er) tilbyder forskellige beskyttelsesmuligheder mod DDoS-angreb. Undersøg hvilke DDoS-sikringsforanstaltninger de stiller til rådighed, eller som kan tilkøbes. Her **anbefaler CFCS** at man eksempelvis laver en aftale med udbyderne om, at:

- Stille ekstra IP-adresser i et andet netværk til rådighed, som kan bruges, hvis de primære IP-adresser bliver blokeret.
- Stille ekstra separate internetadgange og separat netværksudstyr til rådighed, som kan bruges, hvis den primære internetadgang bliver blokeret.
- "Null route" datatrafik, så angrebet afvises, inden det rammer den tiltænkte server. Ved "null routing" ignorerer ISP'en alle indkomne datapakker til organisationen, så serveren ikke overbelastes, men stopper også al normal trafik.

- Omdirigere datatrafik til en "scrubber". En "scrubber", er et system, som løbende analyserer netværkstrafikken. Det kan afvise den ondsindede trafik fra DDoS-angrebet, men samtidig tillade normal trafik, så serveren stadig kan tilgås.
- Automitigere angreb, der automatisk bekæmper angreb med på forhånd aftalte teknikker, og som sikrer en lav reaktionstid.
- Man bør have en aftale, der sikrer, at ISP'en varsler, eller automatisk alarmerer organisationen, hvis dette iværksættes.

3. Anvend specialiseret udstyr

Mange sikkerhedsleverandører tilbyder udstyr, som er skræddersyet til at håndtere DDoS-angreb. Udstyret placeres foran firewalls og bruger mønstergenkendelse til at analysere den indgående datatrafik. Afviges der væsentligt fra normalmønstret begrænses, blokeres eller filtreres trafikken for at undgå overbelastning af det bagvedliggende netværk. Ved anskaffelse af den slags udstyr bør man:

- Sikre tilstrækkelig kapacitet i udstyret til at analysere datatrafikken. Udviklingen og stigningen i angrebsvolumen risikerer hurtigt at overskride det nyindkøbte udstyrs maksbelastning.
- Teste udstyret grundigt efter at det er sat i drift, både isoleret og i samspil med andre komponenter.
 - Opsættes og driftes udstyret i samarbejde med en leverandør, skal testning indtænkes i kontrakten.
 - Sårbarhedstest, som simulerer et DDoS-angreb, bør også overvejes.
- Overvej hvorvidt udstyret skal installeres lokalt, eller om det skal være cloud-baseret.

4. Brug de rigtige komponenter rigtigt

Meget netværksudstyr har indbygget funktionalitet til at beskytte sig mod DDoS-angreb. Der er en række basale forhold, som man kan benytte i sit eksisterende netværk. Det **anbefales**, at man:

- Opdaterer alle komponenter til nyeste patch level. Det kan løbende fjerne eventuelle sårbarheder, der gør udstyret mindre effektivt til at imødegå DDoS-angreb.
- Konfigurerer firewalls eller routere til at droppe indgående ICMP-datapakker, og, hvis man ikke selv drifter internet-tilgængelige DNS servere, standse DNS-besvarelser fra ydersiden af eget netværk ved at blokere UDP port 53.

- Kontrollerer og lukker egne netværk for SNMP-services. Er der et forretningsmæssigt behov for åbne SNMP-services, bør udstyrsspecifikke anbefalinger følges.
 - Som minimum bør SNMP-services netværksbegrænses til relevante administrations- og monitoreringsstationer og ligeledes rettighedsbegrænses.
 - Der kan benyttes en sårbarhedsscanner eller NMAP port scanning til at lokalisere åbne SNMP-services.
- Konfigurerer firewalls eller routere til at monitorere ufuldendte forbindelser og fjerne dem, når antallet overskrider en foruddefineret grænse.
- Aktiverer evt. indbygget DDoS-beskyttelse i webservere. Eksempelvis leveres flere moduler med muligheder, som beskytter applikationslaget mod at opretholde halvåbne forbindelser.
 - Husk også at optimere applikationer for ydelser og gennemfør ydelsestest.
- Monitorerer mønsteret i netværkstrafikken. Hvis trafikmønsteret ændres væsentligt, bør der udsendes en alarm til den sikkerhedsansvarlige. Alarmerne kan man efterfølgende bruge aktivt for at opdage DDoS-angreb.
- Overvejer muligheden for at indføre geo-filter på IP-adresser fra visse lande eller områder, hvis det vurderes, at de ikke har et forretningsmæssigt behov for adgang. Der kan også overvejes en mere restriktiv tilgang ved at udarbejde og implementere en whitelist, som kun tillader trafik fra kendte IP-adresser. Vær særlig opmærksom på:
 - At man ved denne tilgang også udelukker forbindelser fra udlandet samt evt. VPN-forbindelser, som kan have et legitimt behov for at tilgå serveren.
 - At søge råd i egen juridisk afdeling da der gælder særlig lovgivning på området for at indføre geo-filtre.

5. Husk Jeres DNS-servere

Et succesfuldt DDoS-angreb mod en organisations DNS-tjeneste, kan forhindre adgang til alle organisationens internetvendte tjenester. Hvis navneforespørgsler ikke besvares, vil man eksempelvis kun kunne finde en hjemmeside eller mailserver, hvis man for ganske nyligt har tilgået den.

For at beskytte DNS-tjenesten, bør disse anbefalinger følges:

- Hold navneserverne opdaterede så nye sårbarheder, der potentielt kan udnyttes i DDoS-angreb fjernes.
- Konfigurer autoritative navneservere til ikke at tillade rekursive navneforespørgsler. De navneservere der skal svare på forespørgsler, bør ikke anvendes til at foretage navneopslag for andre domæner.

- Anvend flere eksterne navneservere, for at sikre tilgængelighed af navnetjenesten. Det kan være en fordel at lade eksterne leverandører, der er uafhængige af organisationens egen infrastruktur, drive nogle, eller alle, organisationens eksterne navneservere. Eksterne leverandører af navneservertjenester er ofte i stand til at tilbyde god beskyttelse mod DDoS-angreb, og har servere distribueret over flere netværk.
- Begræns antallet af tilladte forespørgsler fra samme IP-adresse, i et givent tidsrum.
- Konfigurer routere og firewalls til kun at acceptere netværkspakker fra IP-adresser, der er gyldige på det netværk, pakken kommer fra (IP-spoofing beskyttelse).
- Tillad ikke forespørgsler af typerne AXFR (zonetransfer) eller ANY (alle records).

Læs mere om beskyttelsen af DNS-servere og udførelse af ovenstående anbefalinger i vejledningen "*Sikker håndtering af domæner*" fra Center for Cybersikkerhed.

Håndter DDoS-angreb

1. Følg en DDoS-drejemodul

På grund af de øjeblikkelige forretningskonsekvenser kan det være særligt tidskritisk at håndtere et DDoS-angreb. Her er det en hjælp at følge en drejemodul, som sikrer en godkendt, ensartet og effektiv tilgang til at afværge angrebet og hurtigt returnere til normal drift.

Drejemodulen bør tilføjes til organisationens eksisterende hændelsehåndtering eller som bilag til beredskabsplanen. Ved udarbejdelse af drejemodulen, bør man:

- Udpege en indsatsleder, som er ansvarlig for, og har mandat til, at iværksætte mitigerende foranstaltninger i tilfælde af DDoS-angreb.
- Føre opdaterede kontaktoplysninger til relevante internetleverandører, eksterne leverandører og DDoS-sikkerhedsspecialister.
- Indskrive forudsætninger for at kunne udarbejde en hændelsesrapport af et evt. DDoS-angreb, herunder adgang til egne og leverandørers logs af netværkstrafik.
- Gøre sig overvejelser om frekvens af test og afprøvning af drejemodulen.

2. Håndter angrebet tidligt

Jo hurtigere et DDoS-angreb opdages, jo bedre er mulighederne for at stoppe det. Dette kræver, at man har et godt kendskab til organisationens datatrafik, har opsat relevant monitorering og automatisk modtager alarmer fra egne komponenter eller eksterne udbydere, hvis trafikmønsteret ændres væsentligt.

Er man udsat for et angreb, bør man overveje, at:

- Aktivere en nødforside på organisationens hjemmeside, der fylder så lidt, som muligt.
 - Det kan med fordel overvejes at hoste nødsiden eksternt og adskilt fra egen infrastruktur, eksempelvis hos en cloudtjeneste.
 - Nødforsiden bør forklare at siden er midlertidigt utilgængelig.
- Øge kapaciteten på båndbredden af sin primære trafiklinje til det højest mulige. Visse organisationer disponerer over ekstra kapacitet for at håndtere perioder med en naturlig høj belastning. Selvom denne ekstra kapacitet ikke nødvendigvis rækker langt i et DDoS-angreb, kan det give et par minutters ekstra tid til at reagere i.
- Indstille *rate limiting* så kun den mængde trafik serveren kan håndtere accepteres.

- Nedsætte grænseværdien for, hvornår routere skal afvise halvåbne forbindelser.
- Begrænse responsraten af ICMP-pakker.
- Automitigering med en "scrubber", såfremt man har dedikeret anti-DDoS-udstyr til rådighed.

Er det en leverandør, som varetager driften af organisationens infrastruktur, bør man sikre sig, at denne har gjort sig samme ovenstående overvejelser. Dette bør være beskrevet i kontrakten mellem organisationen og leverandøren.

Man bør på forhånd også sikre sig, at leverandøren på eget initiativ iværksætter tiltagene inden for nogle aftalerammer, herunder varslings om håndteringen mv.

DDoS er også et værktøj, der benyttes til at distrahere organisationen fra trusselsaktørens faktiske mål. Derfor bør organisationen opretholde monitorering på alle systemer, selv under et angreb.

3. Få ekstern hjælp

Når man har iværksat de indledende foranstaltninger og købt sig lidt ekstra tid, bør man:

- Kontakte internetleverandøren. De vil muligvis først "null route" datatrafikken, som standser trafikken, inden det når den tiltænkte server. Dette vil dog have samme effekt som et DDoS-angreb, og trafikken bør i stedet, eller hurtigst muligt, sendes forbi en "scrubber", som afviser den ondsindede trafik fra DDoS-angrebet, men tillader normal trafik.
- Kontakte DDoS-sikkerhedsfirmaer. De har typisk stor kapacitet og erfaring med at håndtere DDoS-angreb hurtigt og kan om dirigere trafikken til egne servere, som kan klare belastningen.
 - Vær opmærksom på, at dette kræver en aftale på forhånd med sikkerhedsfirmaet. Er man i dialog om mulighederne med et sikkerhedsfirma, kan man med fordel tage udgangspunkt i anbefalingerne i denne vejledning.
- Efter angrebet er stoppet, og normaldriften er genoprettet, anbefales det at udarbejde en undersøgelsesrapport. Den kan benyttes til at afdække tekniske og organisatoriske svagheder, så man er bedre forberedt ved næste angreb. Her kan man med fordel benytte et eksternt firma.

En undersøgelse af DDoS-angrebet kan belyse de nærmere karakteristika ved angrebet, herunder metode og evt. oprindelse, samt afdække eventuelle tekniske og proceduremæssige svagheder i organisationens DDoS-forsvar som kan være væsentlig information til at imødegå lignende angreb i fremtiden.

- Indberet angrebet til relevante myndigheder via www.virk.dk.

Referencer

Vejledningen er blandt andet udarbejdet med inspiration fra:

Center for Cybersikkerhed (2022): *Domænesikkerhed*
<https://www.cfcs.dk/da/forebyggelse/vejledninger/domaner/>

Center for Cybersikkerhed (2017): *Trusselsvurdering: DDoS-angreb stiger i antal og størrelse*
<https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/arkiv/ddos-angreb/>

National Cyber Security Centre, NL (2016): *Protect your organisation against (D)DoS attacks*
<https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-continuity-of-online-services>

National Cyber Security Centre, UK (2020): *Denial of Service (DoS) guidance*
<https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection>

Center for Internet Security (2017): *Technical White Paper – Guide to DDoS Attacks*
<https://www.cisecurity.org/white-papers/technical-white-paper-guide-to-ddos-attacks/>

eSecurity Planet (2018): *How to Prevent DDoS Attacks*
<https://www.esecurityplanet.com/network-security/how-to-prevent-ddos-attacks.html>

eSecurity Planet (2022): *How to Stop DDoS Attacks: Prevention & Response*
<https://www.esecurityplanet.com/networks/how-to-stop-ddos-attacks-tips-for-fighting-ddos-attacks/>

Safetydetectives (2022): *What is a DDoS Attack and How to Prevent One in 2022*
<https://www.safetydetectives.com/blog/what-is-a-ddos-attack-and-how-to-prevent-one-in/>