Nasjonal sikkerhetsmyndighet

IT-veiledning for ugradert nr 4 (U-04)
Oppdatert: 2014-03-10
UTKAST versjon 1.0.2

Grunnleggende tiltak for forebygging av DDoS

Beskrivelse av noen grunnleggende tiltak for å sikre ugraderte systemer mot distribuerte tjenestenektangrep.

Dette dokumentet gir uformell og uforpliktende veiledning i noen grunnleggende tiltak for sikring av IT-systemer mot DDoS-angrep («Distributed Denial of Service»). Målgruppen er personell som utvikler ugraderte systemer i offentlig forvaltning, primært departmenter og andre store sentrale etater. De beskrevne tiltakene er ment å utfylle *commercial best practice*. Dokumentet er ikke ment brukt ifm formell sikkerhetsgodkjenning av graderte systemer.

Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet er tverrsektoriell fag- og tilsynsmyndighet innenfor forebyggende sikkerhetstjeneste i Norge og forvalter lov om forebyggende sikkerhet av 20. mars 1998. Hensikten med forebyggende sikkerhet er å motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, primært spionasje, sabotasje og terrorhandlinger. Forebyggende sikkerhetstiltak skal ikke være mer inngripende enn strengt nødvendig, og skal bidra til et robust og sikkert samfunn.

Hensikt med veiledning

NSM sin veiledningsvirksomhet skal bygge kompetanse og øke sikkerhetsnivået i virksomhetene, gjennom økt motivasjon, evne og vilje til å gjennomføre sikkerhetstiltak. NSM gir jevnlig ut veiledninger til hjelp for implementering av de krav sikkerhetsloven stiller. NSM publiserer også veiledninger innen andre fagområder relatert til forebyggende sikkerhetsarbeid.

Postadresse
Postboks 816
1306 SANDVIKA

Sivil telefon/telefax
+47 67 86 40 00/+47 67 86 40 09
E-postadresse
post@nsm.stat.no

Militær telefon/telefaks
0515 4000/0515 4009

Internettadresse
www.nsm.stat.no

Innhold

1 Innledning

Dette dokumentet gir uformell og uforpliktende veiledning i noen grunnleggende tiltak for sikring av IT-systemer mot DDoS-angrep («Distributed Denial of Service»). Målgruppen er personell som utvikler ugraderte systemer i offentlig forvaltning, primært departmenter og andre store sentrale etater. De beskrevne tiltakene er ment å utfylle *commercial best practice*. Dokumentet er ikke ment brukt ifm formell sikkerhetsgodkjenning av graderte systemer.

Dokumentet peker på sikkerhetstiltak som skal herde IKT-infrastrukturen slik at den bedre kan tåle DDoS-angrep, samt fortsette tjenesteleveransene under slike krevende forhold. Tiltakene omfatter følgende områder:

- Ukonvensjonelle tjenestenekt-angrep
- Design av nettverk og tjenester
- Konfigurasjon av nettverk og tjenester
- Rutiner for drift og vedlikehold
- Forebyggende testing og verifikasjon

I forbindelse med innføring av disse tiltakene, anbefales utviklings- og driftsmiljø å vurdere om tiltakene har lokale fordeler eller ulemper som ikke er tatt høyde for i den generelle beskrivelsen. Det er også viktig at virksomhetene er bevisste sårbarhetene som aksepteres, bevisst eller ubevisst, når tiltak ikke iverksettes.

Kontaktpunkt for denne veiledningen er si@nsm.stat.no. Kommentarer og innspill mottas med takk.

2 Bakgrunn

DDoS («Distributed Denial of Service», eller distribuert tjenestenekt-angrep) er ikke-legitim overbelastning av en eller flere IKT-tjenester. Dette kan gjennomføres på ulike måter; eksempelvis ved overbelastning av en nettverksforbindelse, en ruter, en brannmur og/eller en server. Ofte vil et DDoS-angrep gå i flere faser, hvor hensikten hele tiden er å videreutvikle angrepet i takt med at offeret gjør tiltak for å stoppe det. Angriperen vil også forsøke å måle effekten av angrepet, og ta i bruk det som skal til for å kvele offeret effektivt.

2.1 Aktører og motivasjon

I skrivende stund, er den overveldende mengden DDoS-angrep økonomisk motivert. Firma som driver innen bank og finans er spesielt utsatt. Ethvert firma som tjener penger på kontinuerlig betjening av kunder på nettet, vil imidlertid kunne rammes. I slike situasjoner vil det oftest være forsøk på utpressing inne i bildet. Man har også sett eksempler på at et DDoS-angrep benyttes som røykteppe for å skjule forsøk på svindel-transaksjoner. Til slutt er det en liten andel angrep som er motivert av nettaktivisme (politisk, filosofisk, religiøst).

2.1.1 Eksempel: Trusselbrev

I noen tilfeller kan virksomheten oppleve å få tilsendt et trusselbrev hvor man presses til å overføre et beløp til en bankkonto innen en viss tidsfrist for å unnslippe et DDoS-angrep etter dette tidspunktet. Se ***Vedlegg B.1*** for mer informasjon om dette scenariet.

2.2 Begreper

En leverandør som selger Internett-tilknytning, kalles ***ISP*** etter den engelske betegnelsen «*Internet Service Provider*». Man kan være tilknyttet en eller flere ISP'er avhengig av kravene til redundans og oppetid, og man kan av samme årsak ha en eller flere tilknytninger til hver enkelt ISP.

En angriper som ønsker å maksimere effekten av et anslag, vil basere seg på ikke-legitimt anskaffede ressurser som ikke kan spores tilbake til ham selv. Den vanligste «ressursen» er kompromitterte datamaskiner på Internett; organisert i et såkalt ***botnet***. Et annet ord for dette er *droner*.

De fleste angrepene vil bestå av IP-pakker som ikke enkelt kan spores tilbake til hvilken datamaskin de kom fra. Forklaringen på dette, er at angriperen kommanderer dronene til å forfalske sine avsender-adresser; såkalt «***IP address spoofing***». Dette gjør det vanskeligere for ISP'er å rydde opp og skille angrepstrafikken fra annen legitim trafikk. Den eneste måten å forhindre slik forfalskning, er å få alle verdens ISP'er til å innføre BCP38 («Best Current Practice» nummer 38; tilsvarer RFC2827), som pålegger filtrering av datapakker med forfalsket avsender-adresse. Dette er imidlertid frivillig.

3 Hvordan forebygge DDoS-angrep

NSM understreker at kunnskap om og kjennskap til egen IKT-infrastruktur er helt grunnleggende forutsetninger for å lykkes med forebyggende sikkerhet. I DDoS-konteksten er det tre hovedområder som er spesielt viktige: Sikkert design, sikker konfigurasjon og sikker drift og vedlikehold. I tillegg er det lurt å gjennomføre kontrollert testing og verifikasjon av tåleevnen til de eksponerte komponentene i IKT-infrastrukturen.

For å unngå forvirring knyttet til bruken av ordet «sikker», har forfatteren valgt å navngi delkapitlene i anførselstegn. *NSM betrakter ikke sikkerhet som en enten/eller-størrelse, men som en skala hvor man selv velger sikringsgrad i samsvar med verdien på ressursene som skal sikres.*

Når det gjelder outsourcing, er det viktig å huske at tredjeparter ikke nødvendigvis kjenner til spesielle forhold ved dine tjenester; eksempelvis kryss-avhengigheter. En tredjepart vil normalt heller ikke oppleve ulempen ved at dine tjenester fungerer dårlig eller faller ut. Det er derfor viktig at man har et bevisst og aktivt forhold til tredjepart, samt at man har innsikt i egen IKT-infrastruktur og normaltilstand. Kunnskap og gode, skriftlige avtaler er en forutsetning for å lykkes med et effektivt forsvar dersom krisen skulle inntreffe. Det er mulig å oppnå tilfredsstillende kvalitet ved outsourcing, men dette betinger at man selv besitter både bestillerkompetanse og IKT-infrastruktur-kompetanse.

3.1 Ukonvensjonell tjenestenekt

Før man går i gang med de tradisjonelle problemstillingene, kan det være greit å oppdatere seg på ukonvensjonelle angrepsmetoder som potensielt kan ha svært ødeleggende effekt uavhengig av andre tiltak.

3.1.1 DNS-utpressing

De siste årene har man sett en økning i utpressing som følge av ikke-legitim overtakelse av domenenavn. Når virksomheten har en forretningsmodell som er avhengig av et fungerende domenenavn, kan dette fort bli dyrt. Ved etablering av et domenenavn på Internett, kan man velge «*DNS domain lock*» eller «*registrar lock*», som innebærer at «*registration authority*» er forpliktet til å gjøre en personlig forespørsel til en bestemt kontaktperson i ens egen virksomhet før domenenavnet overføres eller endres på. Dette kan spare en for mye hodebry, og i beste fall et betydelig pengebeløp. Vær obs på at det kan by på problemer dersom en hendelse inntreffer og kontaktpersonen har sluttet i firmaet.

3.1.2 Kapring av offentlige profiler

Det har også vært gjennomført vellykkede utpressingsforsøk ved at en angriper har tilegnet seg en epost-konto som benyttes til utstedelse av nytt passord ifm virksomhetens offentlige Twitter-profil. Ofte er forklaringen at epost-kontoen har hatt et svakt passord. Angriperen har deretter byttet epost-passordet, bedt om et nytt passord til Twitter-kontoen, og overtatt denne.

Moralen er at man bør ha ***sterke passord*** og ***gode rutiner for passordbytte*** for å motvirke slike kapringsforsøk. Dette gjelder selvsagt alle de digitale plattformene som virksomheten benytter i kommunikasjonen med omverdenen; ikke bare Twitter. En annen måte å tenke på, er at passordet er nøkkelen som sikrer verdiene, og dersom verdiene er høye, bør passordstyrken reflektere dette. Etter hvert som digitale plattformer kommer med ***flerfaktor-autentisering***, bør man vurdere fordelene og ulempene ved å ta dette i bruk for spesielt viktige profiler.

3.1.3 Oppskalering av virtuelle tjenester

Dersom man har inngått en avtale om dynamisk oppskalering av ens egne tjenester hos en leverandør av kommersielle skytjenester, kan man være sårbar for angrep som forårsaker finansiell drenering. En forbitret konkurrent vil kunne leie inn en angriper til å forårsake langvarig oppskalering av de virtuelle ressursene, med påfølgende finansiell baksmell. Det er derfor fornuftig å vurdere bruken av terskelverdier for dynamisk oppskalering opp mot risikoen for at legitime brukere opplever uakseptabel tjenestekvalitet. Eventuelt kan man avtale krav om varsling eller manuell intervensjon ved oppskalering over en viss grense.

3.1.4 Ikke-legitim BGP-overtakelse («BGP hijacking»)

BGP («Border Gateway Protocol») er protokollen som benyttes mellom ISP'er for å utveksle informasjon om hvor de ulike IP-adressene er tildelt, samt hvem de tilhører. I lys av de siste årenes hendelser, har man blitt klar over at det er mulig å jukse med eierskapet til IP-adressene. Det er meningen at man skal søke om å få tildelt IP-adresser før man tar dem i bruk, men fordi hele systemet er basert på tillit mellom ISP'ene, er det mulig å overta IP-adresser som er ubrukt eller som

tilhører en annen virksomhet. Det eneste man behøver å gjøre, er å etablere en ISP på en vilkårlig lokasjon, for så å koble seg til en annen ISP og hevde at man har fått tildelt et spesifikt IP-adresseområde.

Denne fremgangsmåten tillater en teknologisk kompetent aktør å gjennomføre et lavkostnads-angrep ved å kapre virksomhetens offentlige IP-adresser. I de fleste tilfeller vil man relativt raskt få assistanse til å gjenopprette eierskapet til IP-nettet sitt, men fordi rutingoppdateringer kan bruke noe tid på å oppnå global utbredelse, vil det være uforutsigbart når og hvor lenge ulike kunder opplever ustabilitet og nedetid.

3.2 «Sikkert design»

Det er en rekke tiltak man kan gjøre for å herde IKT-infrastrukturen i designfasen.

3.2.1 Oppskalering

Det er lett å tenke at det enkleste forsvar er å oppskalere ressursene slik at de er i stand til å håndtere enhver mengde med innkommende forespørsler. For sentralisert plassert, statisk innhold kan dette være en effektiv løsning; særlig dersom det kombineres med bufring (engelsk: «*caching*»). I de fleste tilfeller vil imidlertid tjenesteleveransene ha innslag av dynamisk generert innhold, og dette krever mer avanserte tiltak. Normalt vil man dimensjonere sine IKT-ressurser for spisslast, men DDoS-angrep har potensiale til å mangedoble belastningen fra normal spisslast. Uansett dimensjonering, er det en forutsetning at man både har kjennskap til egen IKT-infrastruktur, samt oversikt over interne og eksterne kryss-avhengigheter som tjenestene bygger på.

Dersom man har dårlig oversikt over hva som er normal spisslast, eller opplever at spisslasten svinger en god del, er det mulig å oppskalere IKT-infrastrukturen ytterligere. Dette kan oppnås ved en kombinasjon av kraftigere utstyr, parallell-prosessering (eks. server-cluster), økt båndbredde og aggregering/meshing[1] av nettverksforbindelser, samt generelle tiltak for å unngå at enkeltfeil skal ta ned en eller flere tjenester (unngå «*single points of failure*»). Nettverksutstyr kan settes opp med mekanismer for lastbalansering (engelsk: «*load balancing*») og høytilgjengelighet (engelsk: «*high availability*»), og ved behov kan man innføre et ekstra lag med servere mellom applikasjonsserverene og Internett-forbindelsen for å bedrive ytterligere avlastning og lastbalansering.

Man bør også vurdere å avlaste tyngre oppgaver til dedikert maskinvare; eksempelvis SSL/TLS offloading, TCP offloading og «web caching». Godt konfigurerte brannmurer kan også bidra til å redusere mengden angrepstrafikk som når frem til selve applikasjonsserveren; eksempelvis ved bruk av «web application firewalls». Et gjennomtenkt nettverksdesign kan også være et godt redskap i jobben med å luke ut suboptimale oppsett. Eksempelvis bør man unngå å benytte komponenter i roller som de ikke har ***maskinvareakselerasjon*** for å ta seg av. Et velkjent eksempel er at lag 3-svitsjer ikke har maskinvareakselerasjon for ruting, og derfor ikke bør bedrive rutingen foran kritiske tjenester.

[1] Forfatteren kjente ikke til noe godt norsk ord for «meshing»; men det kan forklares med «fullmasket nett eller garn». I denne konteksten innebærer det at alle noder har en forbindelse til alle noder på nettverket, eller tilnærmet alle noder, av hensyn til robusthet og båndbredde.

3.2.2 Overgang til dedikert infrastruktur

Dersom man har utplassert deler av egen IKT-infrastruktur (eksempelvis servere, datasentra) hos en tredjepart, er det vel verdt å undersøke hva slags IKT-infrastruktur denne betjenes av. Det er stor forskjell på fysisk og virtuell maskinvare; dette gjelder både på nettverkssiden og på server-siden.

En velkjent problemstilling er potensialet for negative ringvirkninger når man deler nettverks- eller serverinfrastruktur med andre kunder (engelsk: «*multi tenancy*»). Dersom en annen kunde kommer under angrep, kan dette dra med seg ens egen infrastruktur også. Selv om både en selv og den andre kunden skulle klare seg, kan det hende at leverandøren av nettverksforbindelsen opplever overbelastning og/eller krasj som tar med seg ens egen nettforbindelse. Dette gjelder spesielt ISP'ens ruter. Denne problemstillingen forventes å bli mer vanlig, etter som ISP'er i økende grad tar betalt for DDoS-beskyttelse, og dersom man ikke betaler for dette, kan man bli skadelidende også i de tilfeller hvor man ikke selv er under angrep (engelsk: «*collateral damage*»).

NSM anbefaler at man gjør undersøkelser for å avdekke de faktiske forholdene, for deretter å gjøre en samlet risikovurdering målt opp mot egne oppetidskrav. Relevante tiltak kan være å investere i DDoS-beskyttelse fra ISP'en, gå over fra delt til dedikert maskinvare, eller å bygge «The Castle»; jamfør neste delkapittel.

3.2.3 «The Castle» - analogien

Forfatteren tillater seg å benytte en analogi fra Middelalderen: Det er lettere å forsvare en klart definert, godt bevoktet borg enn å bedrive brannslukking over en stor, distribuert slagmark uten gode stillinger. Basert på denne tankegangen, er det enklere å beskytte et sentralisert datasenter hvor alle tjenestene er samlet under ett tak og med en godt beskyttet forbindelse mot Internett, enn å dimensjonere DDoS-beskyttelse av servere og tjenester spredt over en rekke forbindelser og lokasjoner med varierende båndbredde og maskinvarekapasitet.

3.2.3.1 Generelle prinsipper

Ut ifra dette har vi utledet følgende liste over anbefalinger:

1. Kartlegg den fysiske og logiske plasseringen av IKT-ressurser
2. Samle IKT-ressursene på så få steder som mulig (**1**)
3. Sammenkoble lokasjonene med høy, dedikert båndbredde som ikke benytter Internett direkte som bærer (eks. MPLS (**2**))
4. Skap ett felles grensesnitt mot Internett
5. Sikre dette grensesnittet helhetlig mot DDoS-angrep:
    a. Oppskalering (jamfør 3.2.1)
    b. Dedikert infrastruktur (jamfør 3.2.2)
    c. Vurder anskaffelse av «DDoS appliances»
    d. Vurder skybasert DDoS-beskyttelse (**3**)
6. Skill ut brukertrafikk fra datasenter-trafikk (**4**)

(1) Dette må ikke oppfattes som et argument imot redundans; tvert imot bør man styrke redundansen når man samler ressursene på få lokasjoner. Dersom man skal dimensjonere for ekstraordinære begivenheter som naturkatastrofer eller terroranslag, bør man i tillegg vurdere flere

geografisk atskilte lokasjoner med både redundans og autonomi på hver lokasjon (jamfør «*asynkron replikering*»).

(2) ***MPLS*** («Multi Protocol Label Switching») er primært en ISP-teknologi. Når en ISP skal styre og prioritere trafikken i eget nett, er det en fordel å ha et abstraksjonslag under selve Internett-trafikken. MPLS er den mest brukte teknologien for dette. Som bedriftskunde kan man oppnå bedre nettverkssegmentering ved å emulere et stort lokalnett på tvers av lokasjoner ved hjelp av MPLS. Dermed får man kun ett sentralisert grensesnitt mot Internett, i motsetning til ett (eller flere) grensesnitt per lokasjon. Dette gjør det enklere å filtrere og beskytte mot DDoS-angrep, fordi all angrepstrafikken tvinges inn gjennom ett sentralt knutepunkt.

(3) Pass opp for snubletråder knyttet til skybaserte tjenester. Hvis man har SSL/TLS-basert sikkerhet på sine offentlige tjenester, må denne sikkerheten i utgangspunktet outsources til leverandøren av skytjenesten. Er denne lokalisert i utlandet, introduserer man ytterligere kompleksitet med hensyn på internasjonal avtalerett og jurisdiksjon (eksempelvis personvern, konkurs, «collateral damage» i forhold til kriminelle handlinger, osv.). Det finnes teknologiske tilnærminger som kan bøte på problemene, men man ender fort opp med å gjøre en avveining mellom tilgjengelighet, konfidensialitet og kompleksitet.

Ett alternativ er å innføre et ekstra lag med kryptering (såkalt tunnel-i-tunnel), hvor den ytre tunnelen går fra brukerens utstyr til skyleverandøren, og den indre tunnelen går ende til ende mellom sluttbrukerens applikasjon og ens egen applikasjonsserver. En slik løsning vil også ha begrensninger; primært det at den krever god klientautentisering på den ytre tunnelen for å unngå at en angriper får tilgang til den indre tunnelen på samme måte som legitime klienter. Mye av hensikten med å outsource DDoS-beskyttelsen til en skyleverandør er å unngå at angrepstrafikken når frem til ens egen IKT-infrastruktur. Dette alternativet vil derfor antakelig være best egnet til outsourcing av en VPN-forbindelse, hvor skyleverandøren står for terminering av denne, samt klientautentiseringen. Da vil datatrafikken mellom applikasjoner på klient- og serversiden være beskyttet av DDoS-beskyttelsen til VPN-forbindelsen, samtidig som konfidensialiteten ivaretas ende til ende ved hjelp av SSL/TLS på innsiden av VPN-tunnelen.

(4) Det er primært tre grunner for å skille brukertrafikk og datasenter-trafikk på nettverket. For det første er det unødvendig at de ansatte skal frarøves muligheten til å være produktive dersom datasenteret rammes av et DDoS-angrep. Dette løser man ved å ha en separat Internett-forbindelse for brukertrafikken. Man kan vurdere å ha tilfeldige IP-adresser på denne forbindelsen, i motsetning til et forutsigbart, statisk adresseområde. Ved DDoS-angrep på brukerforbindelsen, bytter man raskt IP-adressene på kun denne.

For det andre er det lettere å holde oversikten over nettverksdesignet dersom dette er ryddig og «renskåret». For det tredje er det en mulighet for at angriperen lykkes med å infisere ansatt-maskinene og bruker disse for å øke slagkraften i angrepet mot datasenteret. Dette er mulig fordi man ofte har en god del høyere båndbredde internt i virksomheten. Datasenteret bør med andre ord også beskyttes mot angrep fra interne datamaskiner.

3.2.3.2 «Tynne blodårer»

Dersom man overtar et historisk oppsett, vil det ofte finnes en rekke «tynne blodårer» som forsyner IKT-tjenestene med rådata. Med «tynne blodårer» menes forbindelser med lav båndbredde; gjerne plassert på geografisk adskilte lokasjoner. Det kan også være at man har kjøpt opp en liten leverandør av data til en større tjeneste uten å konsolidere ressursene på IKT-siden. Dersom slike ressurser benyttes som byggesteiner for kritiske tjenester, har man lite å gå på ved målrettede DDoS-angrep. Det er ikke sikkert at alle ressurser lar seg sentralisere; eksempelvis kan det være at en tredjepart ønsker å beholde sin ressurs i sine lokaler. I så fall kan man vurdere tidsstyrt replikering av slike data til en kraftigere, mer sentralisert ressurs i egen IKT-infrastruktur.

Basert på denne tankegangen anbefaler NSM følgende tiltak:

1. Kartlegg hvilke interne og eksterne kryssavhengigheter ens IKT-tjenester bygger på
2. Kartlegg båndbredden og oppetidsgarantien til nettverksforbindelsen til hver av dem
3. Vurder mulighetene for intern konsolidering (jamfør 3.2.3.1, punkt 3-5)
4. Minimer kryssavhengigheter utenfor egen kontroll:
    a. Diskuter kraftsamling av IKT-ressursene med tredjeparter (eksempelvis felles datasenter)
    b. Vurder tidsstyrt replikering fra tredjepart til egen infrastruktur for de ressursene som ikke lar seg konsolidere

3.3 «Sikker konfigurasjon»

Dette dokumentet er ikke laget i den hensikt å tilby en uttømmende liste over herding av enkeltkomponenter. Slik herding vil nødvendigvis måtte tilpasses det enkelte tilfellet. Det finnes også en del «*commercial best practice*»-guider til slikt bruk. Det er imidlertid noen momenter som gjelder DDoS-angrep spesifikt, og disse bør man ha i bakhodet.

3.3.1 DNS-herding

For det første er det viktig å betrakte DNS-tjenerne for ens eget domenenavn som kritiske. Disse vil ofte være blant de første målene for et DDoS-angrep, fordi de er hovedinngangen til domenet. Det er derfor viktig med flere DNS-tjenere, og det kan være lurt å spre dem over flere høyhastighets Internett-forbindelser. Dette kan man oppnå ved å leie sekundære tjenere hos en ISP eller annen tredjepart. Videre er det lurt å stenge ned muligheten for «Zone Transfer», fordi en sonefil kan benyttes som et kart over virksomhetens tjenester og servere. Til slutt bør man unngå å videreformidle eller forsterke angrep rettet mot andre DDoS-ofre; jamfør 3.3.3.

3.3.2 Software-prosessering i nettverksutstyr

Alt teknologisk utstyr har en avgrenset mengde ressurser og kapasitet. For å få best mulig utnyttelse av ressursene og lavest mulig strømforbruk og varmeutvikling, er det utviklet maskinvare optimalisert for vanlige ressurskrevende oppgaver. Eksempler på dette er FPGA'er og ASIC'er som er skreddersydd for TCP offloading, SSL/TLS-offloading og ruting. Dersom man ikke har et bevisst forhold til dette, kan man ende opp med sårbare enkeltkomponenter i IKT-infrastrukturen, eksempelvis:

- En svitsj som står for rutingen foran en kritisk tjeneste
- En ruter som lar seg utnytte til software-prosessering av TCP- eller IP-fragmenter
- En ruter, brannmur eller server som utnyttes ved fikling med IPv6-headere

3.3.3 "Magnification attacks" og "reflective attacks"

Ofte benyttes TCP-protokollen til leveranse av tjenester. Den er forbindelses-orientert; det vil si at den benytter en treveis-hilsen før den overfører datatrafikk. For tjenester som er bygd på IP direkte eller UDP, vil det være mulig å forfalske avsender-adressen og få tjenesten til å sende svaret tilbake til en annen mottaker; et offer man ønsker å angripe. Dersom svaret er mye større enn forespørselen, kalles dette et «magnification attack», og er en variant av «reflection attack», som benyttes for å skjule ens egen IP-adresse.

For å unngå denne typen angrep, er det viktig å opptre solidarisk med andre virksomheter. Dette innebærer å gjennomgå egne tjenester for å sikre at ikke disse kan benyttes som talerør for angrep. Man bør være spesielt obs på NTP («Network Time Protocol»), ICMP («Internet Control Message Protocol»), DNS og SNMP. Både NTP-servere og DNS-servere bør oppgraderes og konfigureres til ikke å svare på bestemte forespørsler. Rutere bør skrus til for å unngå at de videresender ICMP-meldinger til nettverks- og broadcast-adresser, samt unngå at de svarer med store ICMP-feilmeldinger utad. Dette kan også gjelde for brannmurer.

3.4 «Sikker drift og vedlikehold»

En stor og viktig del av DDoS-arbeidet i virksomheten omhandler ansvarsfordeling, tildeling av bestemte roller, samt øvelser som tar for seg de vanligste scenariene. Det er til stor hjelp dersom virksomheten har en IKT-organisasjon som er klart definert på forhånd. Dette delkapitlet er ikke skrevet med tanke på å beskrive hvordan en helhetlig IKT-organisasjonen skal være utformet, men er myntet på de spesifikke momentene som er relevante for DDoS-angrep.

3.4.1 Deteksjon

Deteksjon av et DDoS-angrep er enkelt dersom det er uforklarlig store mengder innkommende datatrafikk mot adresser, porter og tjenester som ikke er i bruk. Det kan være atskillig vanskeligere dersom trafikken ligner veldig på legitim trafikk. Man bør også være oppmerksom på at et angrep på høyere lag i OSI-modellen ikke nødvendigvis skiller seg ut i form av spisslast på nettverkslaget. Dette gjelder spesielt angrep mot dynamiske webtjenester hvor klienten tillates å gjøre anonyme eller forfalskede forespørsler som krever mye regnekraft på server-siden.

Dersom man har lite intern kompetanse på analysering av nettverkstrafikk for å skille mellom dette, kan det være lurt å ha klare avtaler om ekstern bistand på kort varsel ved behov. Leverandører av DDoS-beskyttelse vil ofte ha regelmessig erfaring med slike jobber. Dette kan forkorte problemløsningstiden betraktelig. Som oftest vil en viss prosentandel legitime kunder avvises når man innfører filtrering av angrepstrafikk, og det er her spisskompetanse virkelig kommer til nytte.

Et annet moment å ta stilling til, er når på døgnet man er avhengig av DDoS-beskyttelse. Er man avhengig av å tilby kritiske tjenester nattestid, bør man vurdere om man har intern kapasitet til å

bemanne en 24/7-tjeneste. Det er også mulig å overlate natten til en tredjepart; eksempelvis ved at tredjeparten detekterer og varsler om angrep; eventuelt håndterer eskalering i samarbeid med internt ansatte. Slike forhold bør være tydelig kontraktsfestet; det samme gjelder kostnader og sanksjonsmuligheter.

3.4.2 Reaksjon

Når man har detektert en hendelse, er det viktig med klare prosedyrer og gode rutiner for håndtering og eskalering. Dette forutsetter at mandat og myndighet er klargjort fra virksomhetens ledelse, samt at man er kjent med de økonomiske kostnadene knyttet til ulike former for eskalering. Det bør utpekes nøkkelpersoner med ansvar for ulike trinn ved eskalering (eks: «Hvem oppgraderer en driftshendelse til en sikkerhetshendelse?»). Har man inngått avtale med tredjepart[2] om bistand, bør man ha navn og kontaktinformasjon til denne. I tillegg krever ofte seriøse aktører at man oppgir en liste over internt ansatte som tillates å ta beslutninger om involvering av tredjepart. Man bør være oppmerksom på at slike lister ofte håndteres såpass strengt at selv ikke virksomhetens leder eller eier kan kreve eskalering uten å være oppført på listen.

3.4.2.1 Øvelser

For å sikre strømlinjeformet reaksjon, er det viktig å gjennomføre regelmessige øvelser. Dette er spesielt viktig ved rotasjon av personell; både internt og hos tredjepart. På den måten minimerer man forvirring og løse tråder i en akutt situasjon. Øvelser bør bestå av relevante og virkelighetsnære scenarier. Er man usikker, kan man konsultere en profesjonell aktør innen området.

3.4.3 Gjenoppretting

Når DDoS-angrepet er over, bør man så snart som mulig gjennomføre debrifing av involvert personell. Dette inkluderer evaluering av hendelsesforløpet, tilbakemeldinger på hva som gikk bra, forslag til forbedringer, osv. Kanskje er det nødvendig med nye forebyggende teknologiske tiltak – eksempelvis nytt design eller konfigurasjon. Kanskje finner man behov for presisering av roller og ansvar, tettere kontakt med tredjeparter eller utskiftning av utstyr som ikke holdt mål under press.

Det er også viktig å være oppmerksom på at DDoS-angrep kan benyttes som røykteppe for svindelforsøk; da spesielt i tilknytning til applikasjoner som direkte eller indirekte håndterer pengestrømmer. Det kan også være at noen har lyktes med å bryte seg inn i en eller flere webtjenester mens angrepet pågikk. Kanskje finner man kompromitterte klientmaskiner i virksomheten etter et DDoS-angrep fordi personellet med ansvar for deteksjon av innbruddsforsøk var opptatt med håndteringen av DDoS-angrepet.

[2] Man bør vurdere om man kan ha behov for bistand fra andre tredjeparter enn leverandøren av DDoS-beskyttelse. Kanskje trenger man bistand fra DDoS-kompetansen hos sin ISP (be om navn på kontaktperson), eller eksternt drifts- og utviklingsteam til applikasjonsservere, databaser eller nettverksinfrastruktur. Samarbeider man med andre virksomheter om en tjenesteleveranse, bør man ha informasjon om relevant kontaktperson hos denne.

3.4.4 «Lessons learned»

NSM ønsker å understreke viktigheten av rutiner for evalueringer og tilbakemeldinger i tilknytning til alle de tre områdene deteksjon, reaksjon og gjenoppretting. På den måten sikrer man at virksomheten utvikler seg både med hensyn på personell og teknologi.

3.5 Testing og verifikasjon

Som et ledd i herdingen av egne IKT-tjenester, kan det være fornuftig å gjøre testing ved kontrollert overbelastning av tjenesten før den settes i produksjon. Da får man en viss idé om hvilken kapasitet den har, og ikke minst hvordan den oppfører seg i slike tilfeller. Er det meningen at tjenesten skal skalere opp dynamisk eksempelvis ved å starte opp flere virtuelle instanser, får man et inntrykk av hvilken brukeropplevelse man får idet oppskaleringen slår inn. Et annet moment er at man avdekker hvilke ledd i kjeden som er svakest. Dermed kan man bedre forstå hendelsesforløpet dersom man skulle havne i kryssilden for et faktisk DDoS-angrep. Dersom man har funksjonalitet for oppskalering av de interne tjenestene til en kommersiell nettsky (såkalt «*hybrid cloud*»), bør man kanskje sette et tak for hvor mye ekstra maskinvare som skal tillates brukt for å unngå en finansiell baksmell på neste faktura.

Oversvømming av egne IKT-tjenester bør gjennomføres både på komponent-nivå og basert på de relevante lagene i nettverksstakken (OSI-modellen).

4 Konklusjon

Vi har sett at det er nødvendig med en rekke tiltak for å stå godt rustet mot DDoS-angrep; både personellmessige og teknologiske tiltak. Det viktigste er å rydde opp i de store linjene i IKT-infrastrukturen før hendelsen inntreffer. Her kan man oppnå mye ved å ha et ryddig nettverksdesign med gode rutiner for drift og vedlikehold.

En viktig del av arbeidet med design av IKT-infrastrukturen, er å kartlegge kryssavhengigheter og svake forbindelser som man er avhengig av i tjenesteleveransene sine. En del komponenter lar seg oppskalere, og dette er med på å løfte maksgrensen for hvor mye spisslast man klarer å håndtere. Dersom de økonomiske tapene ved bortfall av tjenestene er store nok, bør man imidlertid også vurdere spesialisert utstyr og skybaserte tjenester for å kunne ta unna selv de kraftigste angrepene.

Når man har designet, skalert og herdet IKT-infrastrukturen hensiktsmessig, er den viktigste oppgaven å ha et klart bilde av hva som kan gå galt, samt å øve på reelle scenarier med relevant sikkerhetspersonell; både internt og eksternt. Dette inkluderer tildeling av roller og ansvar, utforming av klare retningslinjer for eskalering, samt innsamling og relevant distribusjon av kontaktinformasjonen til nøkkelpersoner hos tredjeparter.

Sikkerhet er ingen enten/eller-størrelse, men en skala hvor man velger sikringsgrad i samsvar med verdien på ressursene som skal sikres. I tillegg til teknologiske og personellmessige tiltak, er det beste forsvar kunnskap om og kjennskap til egen IKT-infrastruktur; inkludert hva som er normal bruk og spisslast.

Vedlegg A Dokumenthistorie

2014-02-14	Tiltakene samlet i ett veiledningsdokument.
2014-02-18	Dokumentet fremstilt for første revisjon.
2014-03-07	Første revisjon innlemmet. Noen utvidelser. Klargjort for publisering.
2014-03-10	Referanser og mindre justeringer.

Vedlegg B Fremgangsmåte ved spesifikke hendelser

B.1 Trusselbrev

I noen tilfeller kan virksomheten oppleve å få tilsendt et trusselbrev hvor man presses til å overføre et beløp til en bankkonto innen en viss tidsfrist for å unnslippe et DDoS-angrep etter dette tidspunktet.

Dersom man har bygget et solid vern mot slike angrep, kan dette være et godt tidspunkt å innføre ytterligere tiltak. Kanskje har man en avtale med et eksternt firma som skal hjelpe med å absorbere innkommende DDoS-angrep. Da er det mulig å gjøre denne tredjeparten oppmerksom på at man forventer et slikt angrep, og at denne autoriseres til å iverksette tiltak umiddelbart ved deteksjon av DDoS-angrep for et visst tidsrom fremover. Skulle man ønske å eskalere tiltakene ytterligere, kan man be tredjeparten om allerede nå å omdirigere all den innkommende Internett-trafikken gjennom seg selv, for på den måten å eliminere tidsforsinkelsen med omdirigering idet DDoS-angrepet tar til i styrke.