Nasjonal sikkerhetsmyndighet

Veiledning i DNS-filtrering (U-12)
Oppdatert 2017-12-08

DNS Response Policy Zone (RPZ)

Filtrering av DNS-forespørsler ved hjelp av svartelister.

Dette dokumentet gir veiledning i filtrering av Domain Name System (DNS)-forespørsler ved bruk av Response Policy Zone (RPZ)-svartelister. Målgruppen er personell som drifter ugraderte, men sensitive 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 814
1306 Sandvika
NORWAY

Sivil telefon/telefax
+47 6786 4000 / +47 6786 4009

Militær telefon/telefax
515 4000 / 515 4009

Internettadresse
nsm.stat.no
E-postadresse
post@nsm.stat.no

Innhold

1 Innledning

Dette dokumentet gir veiledning i filtrering av *Domain Name System* (DNS)-forespørsler ved bruk av *Response Policy Zone* (RPZ)-svartelister. Målgruppen er personell som drifter ugraderte, men sensitive systemer. De beskrevne tiltakene er ment å reflektere commercial best practice og bidrar til å filtrere uønsket trafikk over en tradisjonelt *åpen og lett tilgjengelig kommunikasjonskanal*. Tiltakene forutsetter ikke at man har en DNS-server fra før.

Det kan være hensiktsmessig å filtrere DNS-trafikk da typiske oppsett ikke begrenser (**a**) hvilke protokoller som går gjennom port 53 i brannmuren, (**b**) hvilke interne maskiner som får kommunisere direkte ut gjennom brannmuren på denne porten, eller (**c**) hvilke Internett-domener som interne maskiner får tilgang til. Dette er en risiko. Man kan løse (**a**)* og (**b**) ved å tvinge trafikken gjennom en intern rekursiv DNS-server (f eks RPZ) og iverksette brannmur-blokkering. Man løser (**c**) ved å innføre DNS-filtrering, f eks RPZ. RPZ kan også blokkere domener og IP-adresser som byttes ut i høyt tempo (f eks skadevare-kommunikasjon ved bruk av *botnet* [1]).

DNS-filtrering kan forhindre at:

- Ikke-kompromitterte interne maskiner oppretter kontakt med uønskede domener
- Kompromitterte interne maskiner «ringer hjem» til angriperen
- Ondsinnede aktører oppretter kontakt med virksomhetens servere f eks for å spamme dem

Når en virksomhet etablerer RPZ-basert DNS-filtrering, oppnår den i tillegg at:

- Filtreringen blir bedre fordi:
  - RPZ kan stoppe botnet-baserte omgåelser av IP-filtreringen (jf *fast flux*, Vedlegg H)
  - Filtrering kan skje på ulike nivåer i DNS-hierarkiet
- Loggingen blir bedre fordi:
  - Oppslag mot svartelistede domener blir identifisert og logget
  - Filtrering av alle typer klientutstyr blir logget, inkludert *unmanaged* utstyr
- Overføringen av svarte- og hvitelister blir bedre ved at den automatiseres

Av de nevnte årsakene, bør RPZ-filtrering ses på som en del av *grunnsikringen av IT-infrastrukturen*.

Berkeley Internet Name Domain (BIND)-implementasjonen av RPZ logger i nær-sanntid hvilke oppslag som har blitt filtrert, hvilke maskiner disse kom fra, samt hvorfor filtreringen fant sted. Disse loggene kan med fordel benyttes som inngangsverdier i virksomhetens prosess for hendelseshåndtering, f eks i arbeidet med å identifisere kompromitterte maskiner.

RPZ muliggjør et økosystem for automatisert overføring og deling av svarte- og hvitelister. En virksomhet med flere rekursive DNS RPZ-servere, vil kunne overføre og oppdatere svartelister raskt og effektivt. Samarbeidende virksomheter vil kunne automatisere utvekslingen av svartelister seg imellom. Det viktigste er imidlertid muligheten til å abonnere på svartelister fra en profesjonell aktør som håndterer alle aspekter rundt vedlikehold av slik informasjon.

Virksomheter som ikke er i stand til å nyttegjøre seg fordelene ved en lokal DNS RPZ-server (se Vedlegg F), kan videresende DNS-oppslagene til en ekstern tilbyder av filtrert DNS. Det finnes også brannmurer med begrenset støtte for DNS-filtrering, se nærmere omtale i Vedlegg D .

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

(*) Avgrensning *Deteksjon/motvirkning av DNS-tunnelering og skjulte kanaler (covert channels) kamuflert i DNS-protokollen, er utenfor scopet til denne veiledningen. Svartelisting kan likevel bidra ved å vanskeliggjøre noen slike aktiviteter.*

2 Oversikt

Dette kapitlet inneholder en kort oversikt over de påfølgende kapitlene i veiledningen.

Kapittel 3 *Om DNS Response Policy Zone* gir en kort innføring i DNS-filtrering ved å beskrive historisk bakgrunn, virkemåte og sammenligning av DNS RPZ med andre filtreringsteknologier.

Kapittel 4 *Anbefalte tiltak* omtaler innplassering av RPZ-servere i IT-arkitekturen, nødvendige modifikasjoner i virksomhetens brannmur, konfigurasjonsherding, sikker utveksling av svartelister og tillit (verifikasjon av funksjonaliteten og konfigurasjonen).

Vedlegg A oppsummerer veiledningen.

Vedlegg B presenterer sikkerhetstiltakene i sjekkliste-form.

Vedlegg C tar for seg RPZ-meldingsformatet, samt bruk av sikkerhetspolicy.

Vedlegg D sammenligner RPZ-filtrering med nullruting, brannmur-filtrering og web proxy.

Vedlegg E forklarer RPZ ved bruk av et konstruert eksempel (skadevareinfeksjon på klientmaskin).

Vedlegg F beskriver kort fordelene ved intern DNS-filtrering i stedet for ekstern.

Vedlegg G forklarer hvordan RPZ kan bekjempe botnet-baserte trusler.

Vedlegg H inneholder referanser.

Vedlegg I er dokumenthistorien.

3 Om DNS Response Policy Zone

Dette kapitlet gir en innføring i DNS RPZ ved å beskrive historisk bakgrunn, virkemåte, samt sammenligning med andre typer filtrering: nullruting, brannmur og web proxy.

Forutsetningen for å kunne benytte RPZ, er at man tar i bruk DNS-serverprogramvare som støtter svartelister og filtrering. I dette dokumentet forutsettes det at man innfører nyeste versjon av BIND, som i skrivende stund er den eneste DNS-serveren med fullverdig RPZ-støtte.

Det er krevende å beskytte seg mot botnet-basert omgåelse av IP-filtrering, men RPZ er effektiv mot denne trusselen. Se G.2 for nærmere omtale.

3.1 Historisk bakgrunn

Det historiske opphavet til RPZ kan spores tilbake til Vixie Enterprises' *Mail Abuse Prevention System* (MAPS) og *Real-time Blackhole List* (RBL) i 1997. Formålet var hovedsaklig å blokkere avsendere av epost-spam, og MAPS RBL fungerte som en *Border Gateway Protocol* (BGP)-distribuert svarteliste. BGP er en rutingprotokoll, og bruken av begrepet «blackhole» henviser til at ruterne som abonnerte på listen ville forkaste trafikken (nullruting [2]) i stedet for å videresende den. Listen ble raskt populær, og av praktiske grunner valgte man etter kort tid å distribuere den som en DNS sonefil.

Helt fra den spede begynnelsen har det eksistert konkurrenter til MAPS RBL-listen, og antallet tilbydere har økt betydelig siden den gang [3][4].

DNS-filtrering har fått økt oppmerksomhet fordi den snur maktbalansen i kampen mot en kategori av digitale angrep: Botnet gir ikke lenger angriperen overtaket når DNS-filtrering (med gode svartelister) er iverksatt [5].

RPZ ble allment tilgjengelig med BIND versjon 9.8.1, sent i 2010.

3.2 Autoritativ og rekursiv DNS

Det er en viktig funksjonell distinksjon mellom en *autoritativ* og en *rekursiv* DNS-server. DNS-infrastrukturen er hierarkisk oppbygd, og det øverste nivået er *ROOT*. Autoritativ benyttes om alle DNS-servere som er «foreldre» til en DNS-sone. Det benyttes også om den DNS-serveren som er «siste stopp» på letingen etter en IP-adresse eller et domenenavn; «foreldre-sonen» til adressen.

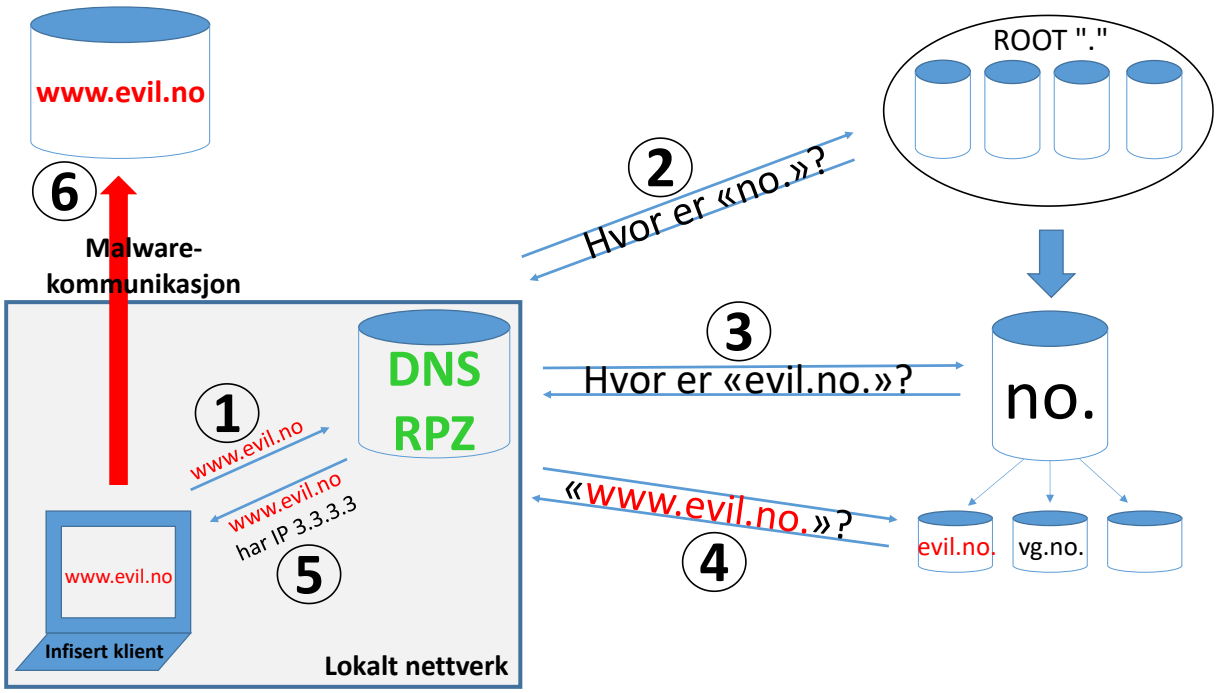
En rekursiv DNS-server (rDNS) gjør oppslag på vegne av DNS-klienter, samt mellomlagrer oppslagene (*caching*) for å tilby kortere responstid ved gjentatte oppslag. Hver gang den ikke har et oppdatert svar i mellomlageret, iverksetter den en prosess for å slå opp domenenavnet. Prosessen begynner på ROOT-nivået og fortsetter nedover i DNS-hierarkiet inntil den har funnet et autoritativt svar på spørsmålet.

RPZ-funksjonen tilbyr filtrering av rekursive DNS-oppslag, se Figur 1.

3.3 RPZ' virkemåte

RPZ innebærer ingen endringer i den ordinære DNS-trafikken, verken i DNS-protokollen eller DNS-programvaren. RPZ er en tilleggsfunksjonalitet som gjør en *rekursiv* DNS-server istand til å filtrere DNS-kommunikasjonen. En slik filtrerende rekursiv DNS-server (heretter kalt *RPZ-server*), benytter også DNS-meldingsformatet på en ny måte for å abonnere på og utveksle svarte- og hvitelister.

Figur 1 viser en infisert klient som forsøker å slå opp domenet www.evil.no for å kommunisere med bakmennenes infrastruktur. DNS-oppslaget er representert ved de første fem trinnene, og utføres av virksomhetens rekursive DNS-server. Dersom domenet, IP-adressen til domenet, navnetjeneren til domenet eller sistnevntes IP-adresse er svartelistet, vil RPZ-funksjonen bryte inn og erstatte svaret med noe annet.



Figur 1 DNS RPZ konfigureres som ny rekursiv DNS-server for å filtrere uønskede domener og navnetjenere.

RPZ-serveren oppfører seg som en ordinær rekursiv DNS-server inntil den støter på en svartelistet ressurs, for deretter å gi et forhåndsdefinert svar [5][6][7][8] f eks:

- Fortsett som om ingenting har skjedd (kun logging)
- En feil har oppstått (generell feilmelding)
- Blankt svar (den forespurte ressursen eksisterer ikke)
- Omdirigering til en annen adresse (f eks intern webserver med informasjon)

Hvilken av disse responsene som blir sendt, avhenger av valgt *policy action*. Når en svarteliste defineres, er det obligatorisk å angi en policy action for hver oppføring. Dette kan imidlertid overstyres for hele listen. Overstyring tillater f eks at man omdirigerer brukerne til virksomhetens interne webserver, hvor man får utfyllende informasjon om hva som har skjedd. Overstyring på listenivå gir mening i forbindelse med abonnement på eksternt produserte svartelister.

Meldingsformatet til RPZ er ordinære DNS-sonefiler med et nytt sett *Resource Records* (RR). I RPZ fungerer sonefiler som svartelister, og hver RR er en listeoppføring [3]. I hver RR er det definert et domenenavn som skal hvite- eller svartelistes, i tillegg til en *policy trigger* og en policy action [6].

Mer informasjon om policy triggers og policy actions finnes i Vedlegg C .

3.3.1 Overføring av RPZ-lister vha DNS

RPZ benytter **DNS-protokollen** til overføring av svartelister i form av sonefiler. Som ved overføring av andre typer sonefiler til slaver, vil hele sonen overføres den første gangen (**AXFR** [9]). Deretter varsler svarteliste-leverandøren kundens RPZ-server ved bruk av DNS NOTIFY-meldinger. En NOTIFY-melding medfører at kundens RPZ-server ber om inkrementelle endringer (**IXFR** [10]) som har kommet til etter den sist mottatte sonefilen (basert på serienummeret).

Konseptet med push-varsling ved endringer medfører distribusjon i nær-sanntid [8]. Inkrementelle endringer reduserer overføringstiden, behandlingstiden ved mottak, samt sparer båndbredde. Dette blir viktigere ved store datamengder; RPZ-sonefiler kan inneholde mer enn en million oppføringer [6] og endres ofte i høyt tempo.

RPZ (og nullruting) støtter push-varsling og overføring av inkrementelle endringer. Alternativet er intervall-baserte løsninger (f eks brannmurer), som må laste ned og prosessere alle oppføringene hver gang. Sistnevnte kan medføre at svartelistene er utdaterte store deler av tiden (les om botnet i G.2).

For informasjon om *sikker* overføring av RPZ-lister, se kapittel 4.8.

3.4 Sammenligning av RPZ, nullruting, brannmur og web proxy

De ulike filtreringsteknologiene DNS RPZ, nullruting [2], brannmurfiltrering og web proxy har ulike styrker og begrensninger. Et av de sterkeste argumentene for RPZ-filtrering, er motstandskraften mot fast flux («botnet-DNS» som omgår IP-filtrering). Leseren henvises til Vedlegg D og Vedlegg G for utfyllende beskrivelse.

Vedlegg D svarer blant annet på følgende spørsmål:

- Er RPZ-filtrering tilstrekkelig, eller behøver jeg andre typer filtrering i tillegg?
- Er det mulig å omgå RPZ-filtreringen?
- Finnes det situasjoner hvor det er bedre å blokkere domenenavn enn IP-adresser?
- Hvorfor er det ikke tilstrekkelig å laste ned en svarteliste innimellom?

Tabell 1 gir en kortfattet sammenligning av de nevnte filtrerings-teknologiene. Det er tatt utgangspunkt i RPZ for å illustrere ulikhetene mellom ulike typer filtrering.

X betyr *ikke-oppfylt*, **X** betyr *delvis-oppfylt*, √ betyr *oppfylt*.

Funksjonalitet	DNS RPZ	Nullruting	Brannmur	Web proxy
Filtrere HTTP-trafikk på URL/URI	X	X	√	√
Filtrere på IP/subnett direkte	X	√	√	X
Filtrere på IP/subnett via DNS	√	X	X	X
Filtrere DNS-trafikk på domenenavn	√	X	X	X
Filtrere navnetjenere under DNS-rekursering (SOA/NS)	√	X	X	X
Hurtig distribusjon av svartelister	push/sekunder	push/sekunder	pull/intervall (min/timer)	pull/intervall (min/timer)
Filtrere IPv6-adresser fra svartelister	√ (kun DNS)	√ (kun IP)	X	X

Tabell 1 Ulike filtreringsmuligheter i DNS RPZ, nullruting, brannmurfiltrering og web proxy.

Vedlegg D gir en nærmere forklaring på disse ulikhetene.

4 Anbefalte tiltak

Ved oppsett av en DNS-server er det viktig å herde både operativsystemet (OS-et) og DNS-tjenesten, i tillegg til spesifikk RPZ-herding. Både OS og generell DNS-herding er utenfor scopet til denne veiledningen. For generell DNS-herding, henvises leseren til «ISC Knowledge Base: Best Practices for those running Recursive Servers» [11].

Dette kapitlet tar for seg det RPZ-spesifikke oppsettet, samt hvordan det kan herdes.

Push-varsler er en grunnleggende forutsetning for kontinuerlig oppdaterte svartelister. Dette krever at RPZ-serverne kan nås via offentlige IP-adresser, eller at man i samarbeid med leverandøren etablerer en VPN-forbindelse som løser dette problemet.

4.1 Ikke benytt autoritative DNS-servere som RPZ-servere

Beste praksis er å unngå sammenblanding av rekursiv og autoritativ rolle i en og samme DNS-server (*mixed mode*), med mindre det er snakk om intranett-domener [11]. *Delegering* fra RPZ-server til intranett-DNS er et alternativ dersom man ikke har Windows-klienter med Active Directory.

En RPZ-server må kunne nås utenfra via en offentlig IP-adresse for å ta imot push-varsler fra svarteliste-leverandøren. Benytter man RPZ-serveren autoritativt til intranett-domener, bør man forsikre seg om at intranett-domenene ikke gjøres tilgjengelige utenfra. Se også kapittel 4.5.

4.2 Benytt flere RPZ-servere for redundans

RPZ filtrerer DNS, som er en tilstandsløs (*stateless*) protokoll. Redundant oppsett krever derfor ingen synkronisering, og kan for eksempel gjøres slik:

- Konfigurer DHCP-serveren til å gi ut flere RPZ-adresser (se kapittel 4.4.2) eller
- Konfigurer IP-nivå arbitrering mellom klientmaskinene og RPZ-serverne

I oppsett uten intranett-DNS, kan **DHCP-serverne dele ut RPZ-adresser**. Man fyller simpelthen inn RPZ-servernes IP-adresser i DHCP-feltene for DNS-servere. En annen løsning er **IP-nivå arbitrering,** som innebærer at man benytter en annen nettverkskomponent (f eks ruter eller brannmur) til å fordele DNS-forespørslene mellom flere RPZ-servere.

Intranett med Windows Active Directory krever et annet oppsett; se kapittel 4.4.3 om *DNS forwarding* og 4.10.1 om logging.

4.3 Plasser RPZ-serverne ytterst mot Internett

RPZ blir virksomhetens nye rekurserende DNS-servere, og må derfor ha «siste ord» i forbindelse med alle utgående DNS-oppslag.

Dersom man har autoritative DNS-servere internt (f eks Active Directory), se kapittel 4.4.3 om *DNS forwarding* og 4.10.1 om logging.

4.4 Bruk RPZ-serverne til alle DNS-oppslag mot Internett

Omdiriger DNS-trafikken fra interne maskiner til RPZ-serverne. Har man gjennomført tiltakene i dette kapitlet i stigende rekkefølge, er BIND ikke konfigurert til å filtrere. Før man går videre, lønner det seg å verifisere at RPZ-serverne fungerer som ufiltrert rekursiv DNS.

4.4.1 Aktiver rekursiv DNS i BIND

Dette gjøres i named.conf.

4.4.2 Konfigurer DHCP-serveren til å sende klientene til RPZ-serverne

DHCP-servere benyttes ofte til å spesifisere hvilke DNS-servere klientmaskinene skal benytte. I et slikt oppsett bør man bytte ut de eksisterende DNS-adressene med RPZ-serverne, bortsett fra i scenariet omtalt i kapittel 4.4.3. Hensikten er å omdirigere den eksisterende DNS-trafikken til RPZ-serverne.

Det er viktig at man *fjerner* andre DNS-oppføringer enn RPZ-serverne i DHCP-konfigurasjonen for å sikre konsistent RPZ-filtrering*.

***(*) Obs** Vi har observert at moderne operativsystemer sender DNS-forespørsler i parallell til flere DNS-servere. Dette gjøres sannsynligvis for å korte ned ventetiden for applikasjonene. Dersom DHCP-oppsettet inneholder både RPZ-servere og ufiltrerte DNS-servere (f eks nettleverandørens), vil RPZ-filtreringen bli uforutsigbar og miste mye av sin verdi.*

4.4.3 Intranett? – DNS delegering eller DNS forwarding

Dersom man har intranett *uten* Microsoft Active Directory-DNS, er DNS-delegering fra RPZ-serverne til intranett-DNS et godt alternativ. I såfall konfigurerer man overordnet delegering av intranett-domenene til intranett-DNS på RPZ-serverne.

Dersom man ikke har mulighet til å omdirigere DHCP-klientene til den rekursive RPZ-serveren direkte, f eks grunnet bindinger til en Active Directory-domenekontroller, finnes det en annen løsning. Konfigurer i stedet de eksisterende DNS-serverne til å videresende alle Internett-forespørsler til RPZ-serverne (såkalt *DNS forwarding*). Av samme årsak som i kapittel 4.4.2, er det viktig at man *fjerner* forwarding til andre eksterne DNS-servere fra domenekontrollerne.

DNS forwarding krever også et *spesielt oppsett for logging*. Se kapittel 4.10.1 for mer om dette.

4.4.4 Endre statiske DNS-oppføringer til å peke på RPZ-serverne

Dersom IT-infrastrukturen blir kompromittert, kan RPZ-filtrering bidra til å hindre den uønskede kommunikasjonen utad og logge forsøkene på slik kommunikasjon. Det er derfor god praksis å sende DNS-oppslagene fra servere og andre infrastruktur-komponenter gjennom RPZ-filtrering.

- Gjør først en vurdering av om sikkerhetssoner, ytelse eller andre forhold gjør det nødvendig å opprette separate RPZ-servere for disse DNS-oppslagene.
- Omkonfigurer DNS-innstillingene på servere og infrastruktur-komponenter slik at de peker på de rette RPZ-serverne.

I de fleste tilfeller er det best å tildele infrastruktur-komponenter statiske IP-adresser og dermed statiske DNS-servere. Dersom man benytter DHCP til infrastruktur-komponenter, er det enkelt å legge inn RPZ-servernes adresser som DNS-servere, og fjerne IP-adresser til andre DNS-servere.

4.5 Blokker og logg DNS-trafikken i brannmuren

For å hindre skadevare og feilkonfigurerte DNS-klienter i å omgå RPZ-mekanismene, er det nødvendig å konfigurere regelsettet i brannmuren. Det er også viktig at kun svarteliste-leverandørens RPZ-servere kan nå RPZ-serveren utenfra; jf problematikken rundt *open resolver*, *DNS amplification*- og *cache poisoning*-angrep [11][12].

4.5.1 Blokker DNS-klienter og tillat rDNS og RPZ

Når man skal blokkere DNS-trafikken i brannmuren, er det viktig å ta høyde for port 53 i alle kombinasjoner av TCP og UDP over IPv4 og IPv6. Vær også oppmerksom på tunnelering av IPv6 over IPv4, f eks Teredo.

Har man en brannmur som støtter identifikasjon og filtrering av DNS på utradisjonelle porter, kan dette bidra ytterligere til å hindre skadevare i å kommunisere. Et godt prinsipp er hvitelisting, hvor man kun åpner for den datatrafikken man ønsker og blokkerer resten (*default block*).

Brannmuren bør filtrere DNS-trafikken slik:

- Kun RPZ-serverne får kommunisere ut mot Internett
- Returtrafikk til RPZ-serverne tillates (krever *stateful inspection*)
- DNS NOTIFY-meldinger fra svarteliste-leverandør tillates inn til RPZ-serverne

Merk at den eneste aktive innkommende pakketrafikken RPZ-serveren skal motta fra Internett, er DNS NOTIFY-meldinger fra svarteliste-leverandøren. Slike meldinger indikerer at svartelisten er oppdatert. Deretter overføres selve svartelistene som returtrafikk ved at RPZ-serveren igangsetter nedlasting.

I større virksomheter er det et alternativ å organisere RPZ-arkitekturen todelt; en «ytre» del til mottak (og intern redistribusjon) av svartelister fra leverandør, og en «indre» del til filtrering nærmere endeutstyret. I slike tilfeller er det kun de «ytre» RPZ-serverne som behøver offentlig IP-adresse for innkommende DNS NOTIFY-meldinger. De resterende «indre» RPZ-serverne må fremdeles kunne nås med DNS NOTIFY-meldinger, men kun fra de «ytre» RPZ-serverne.

4.5.2 Logg forsøk på omgåelse av RPZ-serverne

Interne maskiner som forsøker å kontakte eksterne IP-adresser på DNS-porten, bør både blokkeres og logges. Dette kan være feilkonfigurerte klienter og visse spesielle tjenester, men over tid sannsynligvis innslag av kompromitterte maskiner og skadevare.

Det hender at bærbare enheter og laptoper tester Internett-forbindelsen (Captive Portal-deteksjon) ved å sende ut vilkårlige DNS-forespørsler. Disse kan være rettet mot hardkodede DNS-adresser. I tillegg forekommer det arbitrære DNS-forespørsler til andre åpne DNS-servere selv om maskinen er konfigurert med interne DNS-servere.

4.6 Herde RPZ-konfigurasjonen

Dette delkapitlet lister opp tiltak for å herde RPZ-konfigurasjonen. Tiltakene har til felles at de implementeres i named.conf (eller under-filer hvis named.conf er brutt opp; f eks named.conf.options).

For å herde RPZ, gjør slik:

Id	Tiltak	Konfig-referanse
1	Deaktiver RPZ-soneoverføring på RPZ-serverne (unntak: slave-rpz internt)	allow-transfer { none; };
2	Unngå DNS-lekkasje av RPZ-serverne (se note nedenfor)	
	a) SOA: Benytt "NS <ns.sone.utenfor>" i autoritative RPZ-soner	
	b) SOA: Omdøp RPZ-soner til nøytrale navn som «sone10.minbedrift.no», i motsetning til «rpz.minbedrift.no» eller «blacklist.minbedrift.no».	
	c) Servernavn: Navngi RPZ-serverne nøytralt dersom de legges inn i autoritativ DNS, f eks dns1 og dns2	
3	Deaktiver spørringer mot RPZ-sonene [6]	allow-query { none; };
4	Deaktiver unødvendige authority-data i DNS-responsene	minimal-responses yes;
5	Ikke definer subdomener eller andre RR i autoritative RPZ-soner (bryter best practice og lekker soneinformasjon til sluttbrukerne)	
6	Omdiriger utenfor, ikke inn i RPZ-soner eller subdomener av disse (policy action)	response-policy { zone "sone10.minbedrift.no" policy cname webserver.minbedrift.no.; };

Tabell 2 Herdetiltak for RPZ.

Om tiltak 2. For å motvirke at skadevare kartlegger sikkerhetstiltakene i virksomheten[1], bør man gi RPZ-serverne navn som ikke indikerer at de filtrerer. Nøytrale navn som dns1 og dns2 anbefales, eventuelt kan man la være å legge dem inn i intern DNS. I SOA record-en for RPZ-soner har det vært vanlig å benytte «NS localhost.», men dette er et avvik som stikker seg ut. Benytt i stedet en navneserver *utenfor* RPZ-sonen, for eksempel «NS dns14.minbedrift.no.».

Om tiltak 5 og 6. Subdomener av RPZ-soner skaper problemer ved at RPZ-serveren utleverer sone-informasjon i DNS-responsen. For eksempel, hvis sone10.minbedrift.no er lokal autoritativ RPZ-sone, *unngå* subdomener på formen ~~webserver.sone10.minbedrift.no~~. Bruk istedet webserver.minbedrift.no (f eks ved omdirigering til walled garden). Disse tiltakene motvirker informasjonslekkasje ved å obfuskere at RPZ-filtreringen finner sted. Slike lekkasjer kan forekomme i feilsituasjoner, eller ved valg av policy action som lekker soneinformasjon.

4.7 Etabler hvite- og svartelisting

Verdien til RPZ-filtreringen avhenger av svarte- og hvitelistene man benytter. Det første man bør gjøre, er å *opprette en intern hviteliste*. Deretter må man *identifisere de aktuelle svartelistene*, *teste oppsettet* og *aktivere policy actions*.

Dersom man ønsker å ha strengere filtrering av f eks interne servere, kan man etablere *policy-basert filtrering* i BIND. F eks kan man stenge ned interne serveres kommunikasjon med domener eller DNS-tilbydere man er usikker på.

4.7.1 Opprett hviteliste

Det vil alltid være en viss risiko for *feilaktig svartelisting* (falske positiver), og dette kan ramme virksomheten på flere måter:

- Egne eller samarbeidspartneres servere blir feilaktig svartelistet
- En delt MTA (mailserver) svartelistes, og man forkaster viktig epost fra en legitim forbindelse
- En *registrars* navnetjenere blokkeres ifm et botnet, og man rammes indirekte som kunde
- En *shared host* svartelistes, og tilgangen til et viktig ikke-kompromittert nettsted blokkeres
- Et nettsted infiserer besøkende, men man ønsker å kommunisere med det likevel

Risikoen ved hvitelisting er at interne maskiner blir infisert fordi man ignorerer svartelistingen av reelt skadelige domener og IP-adresser. Det er viktig å vurdere risikoen og konsekvensene ved skadevareinfeksjon opp mot behovet for kommunikasjon før man hvitelister et domene eller en IP-adresse.

NSM anbefaler at man:

- Tar utgangspunkt i interne og forretningskritiske domener og IP-adresser
- Minimerer antallet hvitelistede domener og IP-adresser
- Risikovurderer hver enkelt oppføring
- Ved behov etablerer «usikre klienter» i egne sikkerhetssoner for spesielle anvendelser

Den siste anbefalingen kan være fordelaktig dersom virksomheten har forskere eller andre brukere med behov for å besøke nettsider som blokkeres av ulike årsaker. Detaljert beskrivelse følger.

4.7.1.1 Konfigurasjon av hvitelister

Huskeliste for konfigurasjon av hvitelister:

- Hvitelisten må plasseres før svartelistene for å ta presedens
- Har man tillit til alle domener på en DNS-server, vurder å hviteliste hele serveren
- Man kan unnta visse maskiner fra RPZ-filtrering med «rpz-client-ip.»

[1] Når en klient mottar et filtrert svar fra RPZ-serveren, presenteres den med en «autoritativ løgn». I dette svaret vil det, avhengig av valgt policy action, ligge en SOA record, en CNAME record, en A record, eller lignende. Dersom RPZ SOA-sonen er navngitt «rpz.minbedrift.no», er dette synlig i visse typer filtrerte svar; for eksempel NXDOMAIN og NODATA.

Har man egne navnetjenere og ønsker å hviteliste alle domener på disse, kan det være enklere å hviteliste selve navnetjenerne. Har man en dedikert «usikker sone» som ansatte kan benytte til forskning eller lignende, kan disse IP-adressene unntas fra RPZ-filtrering ved bruk av CLIENT-IP («rpz-client-ip.»).

Tips *For push-varsling og delta-overføring til interne slave-RPZ-servere, konfigurer «notify yes;», «also-notify {<slaveA-ip>; <slaveB-ip>;};» og «ixfr-from-differences yes;».*

Det lønner seg å automatisere oppdateringen av interne slave-RPZ-servere på denne måten. For å integritetsbeskytte denne kommunikasjonen, benytt TSIG[13] som omtalt i kapittel 4.8.

4.7.2 Abonner på lister

Verdien til RPZ-filtreringen er basert på kvaliteten på listene, og dårlige lister kan medføre en *falsk trygghetsfølelse*.

Man bør legge til grunn en risikovurdering for å finne det rette nivået på filtreringen.

4.7.2.1 Kriterier ved valg av svarteliste-leverandør

Når man skal vurdere leverandører av svartelister, bør man for eksempel se på:

- **Falske positiver:** Andelen feilaktig svartelistede, legitime adresser
- **Hurtighet:** Hvor raskt skadelige adresser blir identifisert og svartelistet
- **Kriteriene for svartelisting** (f eks «alvorlighetsgrad» før oppføring finner sted)
- **Kriteriene for fjerning** fra listen og eventuelle gebyrer
- **Behandlingstid** ved fjerning fra listen
- Prosess for **oppfølging av feilaktige henvendelser**

Gode leverandører har få falske positiver, er raske til å identifisere skadelige adresser, har gode kriterier for hvilket innhold som forårsaker svartelisting, har automatisert verifikasjon av renvaskede adresser og kort behandlingstid. I tillegg har de gode nettsider og epost-adresser for tilbakemelding dersom man har blitt feilaktig oppført på svartelisten.

Dersom leverandøren tar høye gebyrer eller har lang ventetid for å fjerne svartelistede adresser, kan det være vanskelig for små aktører å komme seg av listen. Dette rammer egne brukere ved at det tar lengre tid før de får tilgang til feilaktig oppførte og renvaskede adresser.

Ondsinnede aktører har i noen tilfeller utnyttet det at leverandøren ikke verifiserer henvendelser om feilaktig svartelisting til å gjennomføre et nytt angrep eller en ny masseutsendelse av epost-spam. De beste leverandørene har derfor kvalitetssikret prosessen for oppfølging av slike henvendelser.

I henhold til liste på dnsrpz.info, tilbyr følgende leverandører RPZ-svartelister: DissectCyber, FarsightSecurity, InfoBlox, SpamHaus, SURBL, SWITCH, ThreatStop.

4.7.2.2 Typer svartelister

De vanligste typene svartelister inkluderer:

- **Bogon:** Ubrukte IP-adresser som kan misbrukes på Internett
- **Malware:** Adresser som serverer skadevare
- **Botnet kommando og kontroll:** Datamaskiner som er i et botnet
- **Legit-abused:** Legitime nettsider som har blitt kompromittert og serverer skadevare
- **Epost spam:** Adresser som har sendt ut epost-spam tidligere
- **Konsoliderte lister** som hevder at de «tar alt»

Definisjonen av svartelister varierer noe mellom leverandørene. Man bør gjøre en vurdering på hvilke lister som passer med behovet. Det kan være lurt å bruke flere typer svartelister i begynnelsen og redusere ved behov, eventuelt kombinert med en testperiode med logging-modus hvis man er bekymret for falske positiver (se kapittel 4.7.3.1).

Legit-abused innebærer at en legitim nettside blir kompromittert og serverer skadevare. Blokkering av slike domener medfører risiko for henvendelser fra et stort antall frustrerte brukere. Av den grunn lønner det seg å omdirigere brukerne til en intern nettside med informasjon om blokkeringen (såkalt *walled garden*).

Epost spam-blokkering med RPZ blir ikke omtalt i detalj i denne veiledningen, men prinsippet er som følger. For å benytte RPZ til filtrering av epost-spam, må epost-serveren støtte *Forward Confirmed Reverse DNS* (FCrDNS). Dette får epost-serveren til å spørre RPZ-serveren om å slå opp domenenavnet (*forward*) og IP-adressen (*reverse*) ved innkommende epost. FCrDNS gir RPZ-serveren anledning til å blokkere eposten ved å sende et usant svar til epost-serveren dersom domenet, IP-adressen eller en av DNS-serverne ifm rekurseringen er svartelistet.

4.7.2.3 Hvite- og svartelistenes rekkefølge avgjør prioritet

BIND tillater at man benytter inntil *32 lister samtidig* [14][6], hvor rekkefølgen avgjør utfallet av filtreringen. Har man en hvitelisting og en svartelisting av det samme domenenavnet, er prinsippet at det første treffet blir gjeldende. BIND gjennomgår listene i den rekkefølgen de er spesifisert i konfigurasjonen.

4.7.3 Etabler policy action

I RPZ-svartelister defineres en *policy trigger* og en *policy action* per oppføring (RR). I de fleste tilfellene lønner det seg å overstyre med policy action på listenivå. Se Vedlegg C for mer om dette.

Man bør teste oppsettet ved å konfigurere «logging-modus» før man iverksetter filtrering.

4.7.3.1 Begynn med logging-modus

RPZ støtter «logging-modus». Det anbefales at man benytter dette inntil man er sikker på at filtreringen fungerer som den skal. Logging-modus konfigureres ved å sette «policy disabled»:

- `response-policy { zone "sone10.example.com" policy disabled; };`

Denne konfigurasjonen medfører at RPZ-serveren oppfører seg som «rpz-passthru», men med utvidet logging av treff i svartelisten.

4.7.3.2 Iverksett filtrering

Når oppsettet fungerer som det skal, bytter man ut «disabled» med ønsket handling. For å unngå lekkasje av RPZ-soneinformasjon og for å øke brukervennligheten, anbefaler NSM at man benytter omdirigering:

- Omdiriger filtrerte adresser til en intern webserver («*walled garden*»; se C.1).
- `response-policy { zone "sone10.example.com" policy cname minwebserver.minbedrift.no.; };`

Se Vedlegg C for mer om sone-lekkasjer og policy actions.

4.7.4 Vurder policy-basert filtrering

I noen tilfeller kan man ønske å differensiere filtreringen mellom nettverkssegmenter, f eks:

- Strengere filtrering for interne servere enn klientmaskiner
- Mindre streng filtrering for dedikerte «usikre klientmaskiner»

Er målsettingen kun å unnta visse IP-adresser fra RPZ-filtrering, benytt «rpz-client-ip» istedet.

Man oppnår policy-basert filtrering ved å aktivere ulike svartelister for ulike segmenter. I BIND gjøres dette ved å benytte «*view clause*» og definere «*match-clients { <ip-subnett>; };*» og relevante «*zones*» innenfor hvert view [15].

4.8 Beskytt RPZ-soner og NOTIFY-meldinger med TSIG

Abonnement på svartelister innebærer et tillitsforhold til leverandøren, fordi man blindt aksepterer nye oppføringer fortløpende. Derfor bør man integritetsbeskytte dataoverføringen slik at ikke uvedkommende kan tilføre falske oppføringer.

TSIG (Transaction Signature [13]), en symmetrisk hemmelig nøkkel, er den best egnede mekanismen for dette. Det anbefales at man benytter TSIG til å beskytte:

- RPZ-soneoverføringer
- DNS NOTIFY-meldinger

Dette gjelder både mellom ekstern leverandør og RPZ-serveren, og mellom interne RPZ-servere.

Ønsker man i tillegg konfidensialitetsbeskyttelse av RPZ-soner under overføring, må man be leverandøren om å tilby en kryptert forbindelse (f eks IPsec VPN).

Noen RPZ-leverandører krever TSIG-signering av DNS NOTIFY-meldinger for å unngå at kundenes RPZ-servere manipuleres til å angripe leverandørens RPZ-servere. Angrepsmetoden er forfalskede DNS NOTIFY-meldinger som ser ut til å komme fra RPZ-leverandøren.

4.9 Verifiser at RPZ-loggingen er aktivert

RPZ tilbyr logging av både meldinger om RPZ-tjenesten og meldinger om gjennomførte filtreringer. Hva som logges bestemmes av innstillingen *severity*. Det beste er å spesifisere ønsket loggnivå – for eksempel:

```
logging {
      channel bind-rpz {
            file "/var/log/bind-rpz";
            severity info; };
      category rpz { bind-rpz; };
};
```

Meldinger om RPZ-tjenesten kan blant annet indikere feil ifm TSIG eller innlastingen av sonefiler. Meldinger om utført filtrering gir blant annet informasjon om klientmaskinens IP-adresse og hvilken svarteliste (sonefil) som utløste filtreringen.

4.10 Send RPZ-logger til sentralt loggverktøy

RPZ-loggene inneholder potensielt svært verdifull informasjon, som indikasjoner på kompromittering. Dette inkluderer unmanaged-utstyr. Man bør derfor:

- Benytte eksisterende mekanismer for innsending av loggmeldinger, f eks syslog-ng
- Merke RPZ-meldinger med en hensiktsmessig merkelapp (f eks «RPZ»)
- Definere hensiktsmessig varsling (*alerting*), f eks dersom en IP-adresse overstiger et visst antall blokkeringer per time

Dersom virksomheten har et sentralt loggverktøy som støtter varsling og vekting av loggmeldinger, kan man varsle basert på sammensatte kriterier. For eksempel:

- Totalt antall klientfiltreringer den siste perioden
- Toppliste over mest filtrerte klienter
- Filtreringer utenom normal arbeidstid
- Toppliste for alvorlige filtreringskategorier (svarteliste-kategori)

Se [U-11 ELK] for eksempel på hvordan man setter opp DNS- og RPZ-logging med «The Elastic Stack».

4.10.1 Logging for intranett-DNS, NAT eller proxy-server

Dersom klientmaskinene befinner seg på et intranett med dedikert intranett-DNS og forwarding til RPZ-serverne, vil intranett-DNS maskere bort klientenes IP-adresser. Det samme gjelder dersom klientmaskinene befinner seg bak en adresseoversetter (NAT) eller en proxy-server.

Dette reduserer verdien av RPZ-løsningen, fordi man mister muligheten til å identifisere hvilke klienter som blokkeres av RPZ.

Løsningen for **intranett-DNS**, er at disse serverne logger og sender inn samtlige DNS-forespørsler til sentralt loggverktøy. Videre bør man konfigurere det sentrale loggverktøyet til å korrelere loggene fra intranett-DNS og RPZ.

Dersom man benytter **NAT** internt i virksomheten, bør man undersøke muligheten for å plassere RPZ-servere på innsiden av hver NAT, og konfigurere port forwarding slik at RPZ-serverne kan oppdatere svartelistene. En annen løsning er å flytte adresseoversettingen ut til en ytre perimeter, slik at alle klientenes IP-adresser er synlige for RPZ-serverne.

For **proxy-servere**, kan det enkleste være å bytte til transparent modus slik at klientenes IP-adresser ikke blir maskert. En annen mulighet er å plassere RPZ-servere på innsiden av hver proxy og la klientmaskinene slå opp domenenavnene selv. I såfall må man konfigurere port forwarding slik at RPZ-serverne kan oppdatere svartelistene.

4.11 Verifiser utvalgte RPZ-funksjoner

Gjør følgende for å verifisere at RPZ-serverne fungerer som tiltenkt:

- Benytt innebygde BIND-verktøy for syntakssjekking av konfigurasjon og sonefiler
- Gjennomfør omstart av BIND og se etter feilmeldinger i loggfilen
    - Se etter feil ifm innlasting av sonefiler
        - Eksempel: "zone ... loading from master file ... failed ..."
    - Se etter feil ifm konfigurasjonen; herunder TSIG
        - Eksempel: "named[...] exiting (due to fatal error)"

De innebygde BIND-verktøyene for syntakssjekking benyttes slik:

- named-checkconf </etc/bind/named.conf>
    - Visse filer, f eks rndc.key og bind.keys, må sjekkes eksplisitt.
- named-checkzone <zonename> <filename>

Konfigurasjonsfilen til BIND er named.conf. I en del tilfeller er filen oppdelt i delmengder som importeres i hovedfilen, f eks named.conf.local og named.conf.options. Det er viktig at man verifiserer *alle* disse filene.

Verifiser named.conf og importerte filer:

- Sjekk at BIND-prosessen benytter korrekt konfigurasjonsfil (named.conf) ved oppstart
- Sjekk at policy action «disabled» (testmodus) ikke forekommer
- Sjekk at passthru-rpz (hvitelisting) kun benyttes hvor det skal
- Sjekk at konfigurasjonen er konsistent med herdingen i kapittel 4.6
- Sjekk at konfigurasjonen er konsistent med sjekklisten i Vedlegg B

Vedlegg A Oppsummering

RPZ filtrerer DNS-trafikken, som er utgangspunktet for de fleste typer legitim Internett-trafikk. RPZ-filtrering er et verdifullt tillegg til web proxy, nullruting og brannmur-filtrering ved at den blokkerer forsøk på å benytte DNS til omgåelse av IP-filtreringen. Dette er et kjent problem i forbindelse med skadevare og botnet.

Skadevare benytter blant annet DNS til å omgå IP-filtrering (botnet – *fast flux*). Av den grunn er DNS-filtrering viktig for å filtrere skadevare-kommunikasjon. Skadevare som kommuniserer med hardkodede IP-adresser, må blokkeres på andre måter (f eks nullruting).

Til slutt er det viktig å huske at RPZ-filtreringen ikke er bedre enn kvaliteten på svartelistene. Gode svartelister forutsetter at leverandøren jobber raskt med å identifisere nye trusler, men uten å gå på kompromiss med kvaliteten på svartelistene.

Forutsatt at RPZ-serveren holdes herdet og oppdatert, kan RPZ-filtrering gi en potensielt svært kostnadseffektiv perimeterbeskyttelse av alle typer datautstyr, inkludert besøkendes bærbare enheter og annet utstyr som ikke er underlagt virksomhetens sentraliserte flåtestyring.

Vedlegg B Sjekkliste for DNS RPZ-herding

Denne sjekklisten er basert på de anbefalte tiltakene i kapittel 4.

- ☐ 4.1 Ikke benytt autoritative DNS-servere som RPZ-servere (utover intranett-domener)
- ☐ 4.2 Benytt flere RPZ-servere for redundans
- ☐ 4.3 Plasser RPZ-serverne ytterst mot Internett
- ☐ 4.4 Bruk RPZ-serverne til alle DNS-oppslag mot Internett
  - 4.4.1 Aktiver rekursiv DNS i BIND
  - 4.4.2 Konfigurer DHCP-serveren med kun RPZ-servere
  - 4.4.3 Konfigurer intranett DNS-servere med forwarding til kun RPZ-serverne
  - 4.4.4 Endre statiske DNS-oppføringer til å peke på RPZ-serverne
- ☐ 4.5 Blokker og logg DNS-trafikken i brannmuren
  - 4.5.1 Blokker DNS-klienter og tillat rDNS og RPZ
  - 4.5.2 Logg forsøk på omgåelse av RPZ-serverne
- ☐ 4.6 Herde RPZ-konfigurasjonen
- ☐ 4.7 Etabler hvite- og svartelisting
  - 4.7.1 Opprett hviteliste
  - 4.7.2 Abonner på lister
  - 4.7.3 Etabler policy action – begynn med testmodus og gå over til omdirigering
  - 4.7.4 Vurder policy-basert filtrering
- ☐ 4.8 Beskytt RPZ-soner og NOTIFY-meldinger med TSIG-signering
- ☐ 4.9 Verifiser at RPZ-loggingen er aktivert
- ☐ 4.10 Send RPZ-logger til sentralt loggverktøy
  - 4.10.1 Tiltak for intranett-DNS, NAT eller proxy-server
- ☐ 4.11 Verifiser utvalgte RPZ-funksjoner

Vedlegg C Om RPZ-meldingsformatet, policy triggers og actions

Meldingsformatet til RPZ er ordinære DNS-sonefiler med et nytt sett *Resource Records* (RR). Hver sonefil er en liste, og hver RR er en listeoppføring [3]. En RR inneholder et domenenavn som skal hvite- eller svartelistes, samt en *policy trigger* og en *policy action* [6]. Sistnevnte kan overstyres på listenivå.

Følgende policy triggers er tilgjengelige:

- QNAME: Domenenavnet som etterspørres av klientmaskinen (før rekursering)
- CLIENT-IP (rpz-client-ip): Klientmaskinens IP-adresse
- IP (rpz-ip): IP-adresse i DNS-responsen (ifm rekursering)
- NSDNAME (rpz-nsdname): Domenenavn til navnetjener (ifm rekursering)
- NS-IP (rpz-nsip): IP-adresse til navnetjener (ifm rekursering)

Følgende policy actions er tilgjengelige:

- NXDOMAIN (.): Domenenavnet som etterspørres eksisterer ikke
- NODATA (*.): Domenenavnet eksisterer, men svaret er tomt
- PASSTHRU (rpz-passthru): Unntak fra svartelistingen (hvitelisting)
- TCP-ONLY (rpz-tcp-only): Tvinger bruk av TCP; gjerne ifm triggeren CLIENT-IP
- DROP (rpz-drop): Unnlater å svare, som medfører timeout for klienten
- Local-Data (diverse): Muliggjør omdirigering til lokale ressurser

For NXDOMAIN og NODATA, returneres SOA Resource Record til klientmaskinen. Man gir sluttbrukeren informasjon om RPZ-sonen som forårsaket blokkeringen, f eks «rpz-liste-tyskland.minbedrift.no» med konfigurerte verdier (TTL, serienummer, osv). Eventuell skadevare, og dermed eksterne trusselaktører, bør ikke motta slik informasjon; se kapittel 4.6 for mer om dette.

C.1 Om omdirigering til walled garden

Anbefalt policy action er omdirigering til en «*walled garden*»; det vil si en intern webserver med informasjon om hva som har skjedd og hvorfor. En slik nettside kan også inneholde kontaktinformasjonen til brukerstøtte og et skjema man kan fylle ut dersom man mener at blokkeringen er urettmessig.

Vedlegg D Sammenligning av RPZ med nullruting, brannmur og web proxy

Denne veiledningen har introdusert leseren for RPZ. Det finnes flere løsninger for filtrering, f eks nullruting [2], brannmurer og web proxy. I dette vedlegget gjøres en sammenligning av de nevnte teknologiene.

Vedlegget besvarer spørsmål som:

1. Filtrerer RPZ alle tjenester og protokoller, eller er det mulig å omgå RPZ-filtreringen?
2. Er det tilstrekkelig med RPZ-basert IP-filtrering? Bør man supplere med ruter/brannmur?
3. Kan en web proxy med gode svartelister erstatte RPZ-filtrering?
4. Hvor raskt blir svartelister utdatert, og hvor ofte bør de lastes ned?
5. Finnes det angrepsmetoder som omgår IP-filtrering ved å misbruke DNS?
6. Hvis man blokkerer IP-adressen til en webserver for å blokkere ett domenenavn, hvor mange ikke-relaterte domener risikerer man å blokkere (gjennomsnittlig)?
7. Hvorfor er det fordelaktig at RPZ-blokkerte domener ikke genererer kommunikasjon med trusselaktørens DNS-servere?
8. Hvorfor er det ikke lurt å filtrere DNS-rekursererens utgående DNS-trafikk med en ruter/brannmur på utsiden?
9. Støtter alle brannmurer IPv6-adresser ifm svartelisting?

I følgende figur er det tatt utgangspunkt i RPZ for å illustrere ulikhetene mellom ulike typer filtrering. Kap-kolonnen angir hvilket delkapittel som omtaler funksjonaliteten.

X betyr *ikke-oppfylt*, **X** betyr *delvis-oppfylt*, √ betyr *oppfylt*.

Kap	Funksjonalitet	DNS RPZ	Nullruting	Brannmur	Web proxy
D.1	Filtrere HTTP-trafikk på URL/URI	X	X	√	√
D.1	Filtrere på IP/subnett direkte	X	√	√	X
D.1	Filtrere på IP/subnett via DNS	√	X	X	X
D.2	Filtrere DNS-trafikk på domenenavn	√	X	X	X
D.3	Filtrere navnetjenere under DNS-rekursering (SOA/NS)	√	X	X	X
D.4	Hurtig distribusjon av svartelister	push/sekunder	push/sekunder	pull/intervall (min/timer)	pull/intervall (min/timer)
D.5	Filtrere IPv6-adresser fra svartelister	√ (kun DNS)	√ (kun IP)	X	X

Tabell 3 Ulike filtreringsmuligheter i DNS RPZ, nullruting, brannmurfiltrering og web proxy.

De følgende delkapitlene ser nærmere på filtrerings-funksjonaliteten i de ulike teknologiene og gjør sammenligninger med RPZ.

D.1 Filtrere på IP/subnett direkte versus RPZ- og proxy-filtrering av IP-adresser

De første linjene i tabellen sammenligner IP-filtrering i RPZ-servere med tilsvarende funksjonalitet i rutere (nullruting), brannmurer og web proxies. Selv om alle disse teknologiene støtter filtrering av IP-adresser og -subnett, har de distinkte forskjeller:

- IP-filtreringen i RPZ gjelder kun IP-adresser direkte relatert til DNS-rekurseringen
- Nullruting og brannmur filtrerer all IP-trafikk uavhengig av applikasjonsprotokoller
- En web proxy filtrerer kun IP-adresser ifm webtrafikk, ikke andre protokoller

RPZ-filtreringen vil ha bredt nedslagsfelt fordi de fleste tjenester benytter DNS-oppslag, men det er mulig å omgå RPZ-filtreringen ved å unngå DNS-oppslag. Av den grunn kan ikke RPZ erstatte generell IP-filtrering. Det motsatte stemmer også: Nullruting og brannmurfiltrering har ikke fullstendig forståelse av DNS-protokollen, og dette gjør dem dårlig egnet til å erstatte RPZ-filtrering. Forskjellen blir tydeligst ifm avanserte angrep som beskrevet i kapittel D.2 og Vedlegg G .

En web proxy kan filtrere *forward queries* mot IP-adresser og domener, men treffer snevrere enn RPZ fordi den kun ser på webtrafikk. På den annen side filtrerer den også webtrafikk som ikke gjør DNS-oppslag. Den sistnevnte fordelen overlapper med nullruting og brannmurfiltrering.

Adresseoversetting (NAT) er et generelt problem i forbindelse med RPZ, fordi det i RPZ-loggene ser ut som om alle DNS-oppslagene kommer fra en enkelt IP-adresse. Dette kompliserer prosessen med å spore opp klientmaskinene som er ansvarlige for forbindelsen, f eks ved skadevareinfeksjon. Dersom klientene befinner seg bak en web proxy, bør man gjøre tiltak for å kompensere for dette. Man kan f eks plassere RPZ-serveren på innsiden av web proxyen (på klientenes IP-subnett), omgjøre web proxyen til transparent modus (deaktivere ruting/NAT) eller aktivere intens logging i web proxyen og korrelere RPZ- og proxy-loggene i et sentralt loggeverktøy.

I skrivende stund er det kun RPZ som tilbyr fullgod DNS-filtrering lokalt. Nullruting og brannmurfiltrering kan stoppe omgåelser av RPZ, og web proxy støtter høyere detaljnivå på webfiltrering (mapper og filer), men kompliserer sporingen av maskinene bak DNS-oppslagene når web proxy og RPZ benyttes samtidig.

RPZ har en begrensning i forbindelse med etablerte IP-forbindelser: DNS-oppslaget gjøres normalt kun i begynnelsen. Etablerte IP-forbindelser har normalt ikke behov for å gjøre et nytt DNS-oppslag, og derfor kan heller ikke RPZ filtrere etablerte IP-forbindelser. For å oppnå dette, må man benytte brannmur eller nullruting.

D.2 Filtrere DNS-trafikk på domenenavn: IP-filtreringens begrensninger og botnet

Når man konverterer domenenavn til IP-adresser som man filtrerer i stedet for domenenavnet, oppstår det et mulighetsrom for misbruk. DNS-filtrering er den eneste generiske filtreringsmekanismen som ikke har disse problemene. En web proxy har lignende funksjonalitet, men kun for webtrafikk. RPZ-filtrering håndterer alle typer trafikk som er avhengig av DNS-oppslag, inklusive skadevare.

Det fundamentale problemet med konvertering av domenenavn til IP-adresser som man filtrerer, er at man bytter ut primær informasjon med sekundær. Dette får uheldige utslag; spesielt når trusselaktøren benytter et botnet [1] for å rotere IP-adressene hurtig og unngå IP-basert filtrering.

Rutere (nullruting) og brannmurer støtter primært IP-basert filtrering, og må derfor slå opp svartelistede domenenavn til IP-adresser før de kan filtreres. Uavhengig av om oppslaget gjøres av svarteliste-distributøren eller den lokale brannmuren, opererer IP-filtreringen vanligvis under følgende begrensninger:

- IP-blokkering rammer shared hosting-nettsteder blindt
- Ufullstendig behandling av DNS-responsen
- For lav oppdateringsfrekvens på IP-konvertering av domenenavn
- Botnet gjør IP-blokkering lite effektivt

Løsningen på disse problemene, er å innføre DNS-filtrering som RPZ. For utfyllende beskrivelse av disse problemstillingene, se Vedlegg G .

D.3 Filtrere navnetjenere under DNS-rekursering

RPZ kan filtrere spesifikke DNS-servere på en skalerbar og effektiv måte. Dette delkapitlet forklarer hvordan RPZ' navnetjener-filtrering er bedre enn lignende funksjonalitet i ruter/brannmur.

Den primære fordelen med RPZ, er at også navnetjenere kan filtreres direkte uten konvertering til IP-adresser. Ruter/brannmur er ikke i stand til dette, og man støter på følgende forhold:

- Problemene ved IP-konvertering og -filtrering av domenenavn (se kapittel D.2)
- Filtreringen må finne sted mellom rDNS-serveren og Internett
- IP-filtrering på WAN-siden av en rDNS-server bryter med god kutyme og kan medføre ytelsestap for brukerapplikasjonene grunnet *DNS timeout*

Foruten de samme **problemene som oppstår ved IP-konvertering av domenenavn** beskrevet i kapittel D.2 , er det også et par andre forhold man bør være oppmerksom på.

Skal man filtrere navnetjenere på IP-nivå, må **filtreringen finne sted mellom DNS-serveren og Internett**. Navnetjenerne man ønsker å filtrere er en del av kommunikasjonen som DNS-serveren utfører på vegne av klienten, og kommunikasjonen er derfor ikke synlig for eventuelle pakkefiltre mellom klienten og rDNS-serveren.

Selv om det er teknisk mulig å blokkere navnetjenere i ruter/brannmur på WAN-siden, er det **ikke god praksis** fordi det bryter med «alltid tilgjengelig»-tanken bak DNS-tjenesten og introduserer en **tidsforsinkelse** (*server timeout*) for DNS-klientene. Timeout påvirker ytelsen til applikasjonene som benytter DNS. RPZ introduserer ikke slik forsinkelse fordi den gir negativt svar umiddelbart.

Man kan derfor konkludere med at RPZ har den mest presise og skalerbare løsningen for filtrering av DNS-servere.

D.4 HURTIG DISTRIBUSJON AV SVARTELISTER

De første svartelistene ble distribuert via rutingprotokollen BGP med tanke på nullruting hos mottakerne. Innen kort tid bestemte man seg for å distribuere dem som DNS-sonefiler; derav navnet Response Policy Zone (RPZ).

Begge disse distribusjonsmetodene har kort tidsforsinkelse og lave båndbreddekrav. Mange brannmurer har støtte for nedlasting av svartelister, men dette er typisk intervall-basert nedlasting med en times eller et døgns mellomrom. Det er problematisk fordi en økende andel av truslene man ønsker å beskytte seg mot, endrer seg på sekund- og minutt-nivå; jf *fast flux* (G.2 ,[16][17]).

RPZ er bedre egnet til å bekjempe dagens trusler fordi den er konstruert for å oppdatere seg svært raskt.

D.5 FILTRERE IPV6-ADRESSER FRA SVARTELISTER: MANGLENDE STØTTE I BRANNMURER

DNS RPZ og nullruting støtter ulike typer IPv6-filtrering. DNS RPZ filtrerer kun IPv6-adresser i forbindelse med DNS-oppslag, mens nullruting filtrerer IP-protokollen. Se kapittel D.2 og Vedlegg G

De fleste brannmurer støtter IPv6-filtrering i form av regelsett man legger inn manuelt, men det varierer om de støtter IPv6-svartelister når disse hentes inn via andre kanaler (f eks intervall-basert automatisk nedlasting). Dersom man planlegger å benytte en brannmur til IPv6-svartelisting, bør man verifisere at denne funksjonaliteten støttes. Man bør også undersøke om brannmurens IPv6-filtrering gir den ønskede effekten; jf D.4 .

Vedlegg E Eksempel: Skadevareinfeksjon

La oss se på det konstruerte eksempelet hvor en ondsinnet aktør har satt opp egne DNS-servere og lyktes med å få en av brukerne våre til å klikke på et skadelig vedlegg (f eks mottatt via epost). Vi forutsetter at brukerens maskin er sårbar for angrepet, men at svarteliste-leverandøren har publisert oppføringer som gjør det mulig å blokkere kommunikasjonen med angriperens infrastruktur.

Videre er det en forutsetning at skadevaren er avhengig av DNS-oppslag før den kommuniserer med IP-adresser, eller at vi har dynamisk IP-filtrering i ruter/brannmur som stopper hardkodede IP-adresser.

E.1 Sammenligning: Uten og med RPZ-filtrering

En ufiltrert DNS-løsning ville straks kontaktet den ondsinnede aktørens DNS-servere og servert IP-adressene med skadelig innhold til brukerens maskin. Dette er første gangen trusselaktøren får en bekreftelse på at offeret har åpnet skadevaren. Når offerets maskin kontakter angriperens webserver over IP, får angriperen for andre gang indikasjon på at angrepet var vellykket.

Trusselaktøren får med andre ord både en DNS-indikasjon og en webserver-indikasjon på at angrepet var vellykket når man ikke har etablert DNS-filtrering. I tillegg fortsetter den uønskede kommunikasjonen mellom skadevaren og trusselaktøren.

Med RPZ vil ett av følgende inntreffe:

1. RPZ tar ikke kontakt med DNS-serverne, men blokkerer forespørslene direkte
2. RPZ tar kontakt med DNS-serverne, men blokkerer forespørslene likevel

Det første tilfellet inntreffer dersom domenenavnet som klienten spør etter, finnes i en av svartelistene. Da er videre rekursering ikke nødvendig, og RPZ-serveren responderer iht policy action. I dette tilfellet får angriperen ingen indikasjoner på vellykket angrep og kan ikke vite om brukeren mottok eposten og åpnet vedlegget.

Det andre tilfellet inntreffer dersom domenenavnet ikke er svartelistet, men RPZ-serveren støter på en svartelistet ressurs under rekursering (f eks i en SOA eller NS *Resource Record* (RR)). Da vil den fullføre rekurseringen som vanlig (*). DNS-klienten vil imidlertid motta en blokkering eller omdirigering basert på valgt policy action. Trusselaktøren får normalt kun en indikasjon i dette tilfellet, avhengig av konfigurasjon og hvorvidt han har oversikt over datatrafikken inn til DNS-tjenestetilbyderen sin (**).

I dette tilfellet vet ikke trusselaktøren om den initielle infeksjonen feilet under kjøring, eller om det var andre faktorer som avbrøt infeksjonen før den lyktes. Dersom den ble avbrutt, kunne det skyldtes antivirus/anti-malware, løsninger for «*endpoint protection*» eller nettverksbasert blokkering som RPZ. Uvitenhet hos trusselaktøren er ingen ulempe for oss.

(*) Dette er standard-oppførsel i dagens BIND-programvare, og anbefalt konfigurasjon. Det er mulig å konfigurere RPZ-serveren til å avbryte rekurseringen når den støter på en svartelistet ressurs.

(**) Double flux (se Vedlegg G) avhenger av samarbeid med (eller kompromittering av) DNS-tjenestetilbyderen, fordi domenets SOA NS-informasjon må kobles mot botnettet og roteres hurtig.

E.2 RPZ gir redusert fotavtrykk

Det er fordelaktig at RPZ minimerer virksomhetens fotavtrykk overfor en eventuell angriper og gjør det vanskelig å vite om kompromitteringsforsøket var vellykket. Angrepet stoppes i en tidlig fase, og dette gir oss muligheten til å rydde opp på maskinen.

E.3 En initiell infeksjon er ikke ufarlig

Når en bruker først har åpnet et skadelig vedlegg, er maskinen sannsynligvis infisert av skadevare selv om RPZ blokkerer skadevarens kommunikasjon med bakmennene og motvirker at mer

omfattende skadevare blir lastet ned. Det kan også hende at den infiserte maskinen tas med og benyttes på steder som er utenfor RPZ-serverens rekkevidde. Det er derfor viktig å handle raskt dersom RPZ-loggene gir grunn til mistanke om infeksjon.

Info *I noen tilfeller har man observert at den initielle angrepskoden ikke inneholder funksjoner for å opprette persistent tilstedeværelse på maskinen. I slike tilfeller kan en vellykket RPZ-blokkering medføre at skadevaren ikke får fotfeste og forsvinner ved neste omstart, forutsatt at ikke maskinen medbringes til et åpent nettverk før omstart.*

Det er likevel god praksis å behandle den infiserte maskinen som om den initielle infeksjonen var av det omfattende slaget og har etablert persistent fotfeste.

Vedlegg F Om eksterne tilbydere av DNS-filtrering

Dette vedlegget beskriver fordelene ved interne DNS-servere og intern DNS-filtrering sammenlignet med eksterne tilbydere.

Generelt har interne rekursive DNS-servere ytelsesmessige fordeler: Kortere responstid og lavere båndbreddebruk (*caching*). Interne DNS-servere reduserer også utleveringen av informasjon som kan benyttes til passiv kartlegging av virksomhetens surfevaner og IT-topologi.

De største **sikkerhetsmessige fordelene** ved intern DNS-filtrering i stedet for ekstern, er at man kan se fortløpende hvilke *interne* klient-IP-adresser som blir filtrert (i motsetning til mindre treffsikker NAT-korrelasjon fra utsiden). Følger man anbefalingen om å integrere RPZ-loggingen med virksomhetens sentrale verktøy for logganalyse, kan man produsere automatiserte sikkerhetsvarsler og statistikk på et rikere informasjonsgrunnlag. RPZ-loggene er spesielt interessante fordi de tilbyr sikkerhetsrelevant informasjon om alle typer klientenheter; også de som *ikke* er innlemmet i virksomhetens sentraliserte administrasjon (såkalt *unmanaged* utstyr).

Dersom virksomheten ikke ønsker eller ikke er i stand til å nyttegjøre seg disse fordelene, kan man vurdere en ekstern tilbyder av DNS-filtrering.

Vedlegg G DNS-filtrering og botnet (fast flux)

Dette vedlegget utdyper IP-filtreringens ulemper som introdusert i D.2 , samt hvordan botnet og DNS misbrukes av trusselaktører til å omgå IP-filtrering. Løsningen på disse problemene er DNS-filtrering (RPZ).

G.1 IP-KONVERTERING AV DOMENENAVN I SVARTELISTER

Filtrering basert på IP-konvertering av domenenavn kan medføre følgende problemer:

- IP-blokkering rammer shared hosting-nettsteder blindt
- Ufullstendig behandling av DNS-responsen
- Lav oppdateringsfrekvens på IP-konvertering av domenenavn
- Botnet [1] gjør IP-blokkering lite effektivt

IP-blokkering rammer shared hosting-nettsteder blindt. Det er kjent at mange websider og epost-servere befinner seg på delt infrastruktur (jf *shared hosting*). Dersom man blokkerer IP-adressen i stedet for domenavnet, risikerer man å blokkere et stort antall ikke-relaterte domener [18].

Dette unngår man ved bruk av DNS RPZ, fordi RPZ støtter blokkering på domenenivå uten å måtte slå opp de involverte IP-adressene. RPZ:

- Blokkerer det svartelistede domenet uten å ramme andre domener på samme IP-adresse
- Blokkerer domenet før den har slått opp IP-adressen(e) til domenet

> ***Shared hosting*** *Mange nettsider er lokalisert på en delt webserver; de ti største selskapene innen web hosting har i snitt 421 domener per web host [18]. Epost-servere er et annet eksempel på slik organisering.*

Ufullstendig behandling av DNS-responsen sikter til brannmurer som gjør domeneoppslag uten å ta hensyn til alle IP-adressene i DNS-responsen. Noen brannmurer velger ut en av IP-adressene, eller mangler støtte for IPv6-adresser eller AAAA *Resource Records*. Skal filtreringen være effektiv, må alle IP-adressene til domenenavnet svartelistes.

Lav oppdateringsfrekvens på IP-konvertering av domenenavn gjør situasjonen verre. Det kan være at brannmuren sjeldent laster ned svartelistene, og når de først blir lastet ned, konverteres domenenavn til IP-adresser kun en gang (ved innlasting). I såfall er en del av filtreringsinformasjonen oppdatert og nyttig kun de første sekundene eller minuttene etter innlasting av svartelisten, for deretter å være ute av synk til neste nedlasting.

Hyppigheten på både nedlastingene og domeneoppslagene vil påvirke resultatene, men det endrer ikke på det fundamentale problemet: Man forsøker å blokkere basert på sekundær informasjon; andre ledd i en potensielt hurtig vekslende en-til-mange-relasjon.

Botnet gjør IP-blokkering lite effektivt. IP-filtrering av botnet er vanskelig fordi det ikke finnes noen generell, treffsikker og skalerbar måte å gjøre det på uten å overta styringen av botnettet. Uten slik mulighet, må man ha kontinuerlig global *Dolev-Yao*-innsikt [19] i IP-trafikken kombinert med helt presise indikatorer for ikke å gå glipp av innlemmede maskiner.

G.2 BOTNET OG FAST FLUX

Et botnet kan være stort, og tempoet på endringer kan være høyt. Når trusselaktøren peker domenene sine til et stadig skiftende utsnitt av botnettet (jf *fast flux*), blir IP-filtrering en lite effektiv løsning.

Dette skyldes dels problemet med å identifisere alle innlemmede kompromitterte datamaskiner, og dels at man i liten grad har oversikt over nye kompromitteringer. Selv når man har presise indikatorer som identifiserer datatrafikken til og fra kompromitterte maskiner, er man avhengig av samarbeid på tvers av ISP-er, landegrenser og kontinenter for å avsløre samtlige involverte IP-adresser.

The Honeynet Project [16] har beskrevet hvordan trusselaktører benytter fast flux-konseptet for å skjule sin egen IT-infrastruktur og dermed omgå mye av den IP-baserte filtreringen. Skadevaren benytter DNS til å slå opp domenenavn som gjør den istand til å kommunisere med fast flux-botene. DNS-tjenesten til trusselaktøren sørger for rask utskiftning av IP-adressene til:

- Webserverne (A/AAAA Resource Records, single-flux)
- Navnetjenerne (NS Resource Records; impliserer double-flux)

Fast flux *Når man roterer IP-adressene bak et domenenavn i høyt tempo for å unngå IP-basert svartelisting, kalles det* ***single-flux****. Benytter man i tillegg et lag med hurtig roterende navnetjenere og/eller proxy-noder i forkant av single-flux, kalles teknikken* ***double-flux****. Hensikten med disse teknikkene er hovedsaklig å skjule bakmennenes IT-infrastruktur, servere skadevare og å gjøre skadevarens kommunikasjon med bakmennenes IT-infrastruktur mer robust. Etterforskning og forsøk på å stoppe slik kommunikasjon er vanskeligere og krever samarbeid med nettleverandører (ISP-er) og berørte virksomheter [16][17].*

DNS-filtrering forenkler jobben med å lage svartelister både fordi det kan gjøres deterministisk basert på førstehånds informasjon, og fordi det kan gjøres hierarkisk. Førstnevnte kan f eks utledes fra analyse av skadevare (*reversing*). Hierarkisk blokkering kan f eks innebære trusselaktørens DNS-servere, eller DNS-serverne til trusselaktørens domeneleverandør.

Vedlegg H Referanser

[1] «Botnet: Når et «botnet» kaprer datamaskinen», http://www.nettvett.no/virus/datamskinkapring, besøkt 07.04.2016
[2] Wikipedia: «Null route», https://en.wikipedia.org/wiki/Null_route
[3] RFC 5782: «DNS Blacklists and Whitelists», http://tools.ietf.org/html/rfc5782
[4] Wikipedia: «Comparison of DNS blacklists», https://en.wikipedia.org/wiki/Comparison_of_DNS_blacklists
[5] Technical University of Denmark, Connery: «RPZ: History, Usage and Research», https://dnsrpz.info/RPZ-History-Usage-Research.pdf, besøkt 15.04.2016
[6] Bok: «Pro DNS and BIND, Chapter 7 - Response Policy Zone», http://www.zytrax.com/books/dns/ch7/rpz.html
[7] RFC 2308: «Negative Caching of DNS Queries (DNS NCACHE)», https://tools.ietf.org/html/rfc2308, besøkt 13.04.2016
[8] ISC-TN-2010-1: «DNS Response Policy Zones (Format 3)», https://kb.isc.org/getAttach/21/AA-00512/rpz.txt, besøkt 15.04.2016
[9] AXFR (DNS zone transfer): «DOMAIN NAMES - CONCEPTS AND FACILITIES», http://tools.ietf.org/html/rfc1034, besøkt 04.05.2015
[10] IXFR: «Incremental Zone Transfer in DNS», http://tools.ietf.org/html/rfc1995, besøkt 04.05.2015
[11] ISC: «Best Practices for those running Recursive Servers», https://kb.isc.org/article/AA-00874/0/Best-Practices-for-those-running-Recursive-Servers.html
[12] O'Reilly: «Five Basic Mistakes Not to Make in DNS», http://archive.oreilly.com/pub/a/sysadmin/2007/04/26/5-basic-mistakes-not-to-make-in-dns.html?page=2
[13] «TSIG» (Transaction Signature), http://en.wikipedia.org/wiki/TSIG
[14] ISC: «DNSRPZ performance and scaleability when using multiple RPZ zones», https://deepthought.isc.org/article/AA-01121/0/DNSRPZ-performance-and-scaleability-when-using-multiple-RPZ-zones.html
[15] ZyTrax: «DNS BIND view Clause», http://www.zytrax.com/books/dns/ch7/view.html
[16] The Honeynet Project: «HOW FAST-FLUX SERVICE NETWORKS WORK», http://www.honeynet.org/node/132, besøkt 30.03.2016
[17] Wikipedia: «Fast flux», https://en.wikipedia.org/wiki/Fast_flux, besøkt 30.03.2016
[18] «Web Hosting. The most comprehensive Web Hosting statistics in the world», http://www.webhosting.info/web-hosting, besøkt 07.03.2016
[19] Wikipedia: «Dolev–Yao model», https://en.wikipedia.org/wiki/Dolev–Yao_model, besøkt 08.04.2016

Vedlegg I Dokumenthistorie

2017-09-20 Første utgave for publisering ferdigstilt.