CENTER FOR CYBERSIKKERHED

Vejledning:

Sikker håndtering af domæner

Indhold

CENTER FOR CYBERSIKKERHED

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

Udgivet juli 2020 (første udgave april 2020).

Indledning

Hvis en ondsindet aktør kan få kontrol over et domæne, kan det anvendes til at forhindre adgang til organisationens hjemmeside, blokere for mailkommunikation, omdirigere VPN-trafik, opnå kontrol med krypteringscertifikater og opsnappe data og login-informationer. I nogle tilfælde kan det have omfattende økonomiske eller politiske konsekvenser.

Denne publikation giver en række anbefalinger, der kan hjælpe organisationer med at håndtere deres domæner på sikker vis. Anbefalingerne kan hjælpe organisationerne med at reducere risikoen for negativ påvirkning af deres identitet på internettet, tilgængeligheden af deres systemer eller fortroligheden og integriteten af deres kommunikation.

En organisations identitet på internettet er i høj grad knyttet til domænenavne. Interaktion med organisationen, hvad enten det drejer sig om besøg på hjemmesiden eller kommunikation via mail, afhænger af, at domænenavne kan slås op. Det er derfor vigtigt for enhver organisation at håndtere domæner på sikker vis.

Vejledningen henvender sig først og fremmest til organisationers IT-ledelse og IT-driftsafdeling. Det er hensigten, at anbefalingerne kan indgå i organisationers arbejde med at forbedre eksisterende praksis og sikre, at fremtidig håndtering af domæner ikke udsætter organisationen for unødige risici.

Overordnede anbefalinger
På de følgende sider opstilles og uddybes Center for Cybersikkerheds anbefalinger vedrørende sikker håndtering af domæner. Anbefalingerne kan hjælpe organisationer med at håndtere de risici, der er forbundet med at have domæner.

De overordnede anbefalinger og principper herunder er et udvalg og skal ikke opfattes som en udtømmende liste:

- Sørg for at have overblik over alle organisationens domæner
- Beskyt adgangen til at ændre i domæneregistreringer
- Følg en fast proces for at ændre i domæneregistreringer
- Gennemse jævnligt domæneregistreringerne
- Lav et navneserverdesign der beskytter organisations domæner og sikrer tilgængeligheden
- Beskyt alle domæner med DNSSEC
- Verificér navneopslag med DNSSEC

Baggrund

Specifikationerne til Domain Name System (DNS) blev udgivet i starten af 1980'erne, med fokus på at etablere et distribueret system til opslag af navne, der var effektivt og driftssikkert og kunne håndtere et voksende netværk af computere. Det netværk har siden udviklet sig til det globale internet, vi kender i dag. Internettets mange tjenester afhænger stadig af et velfungerende DNS, men der blev desværre ikke tænkt sikkerhed ind i de oprindelige specifikationer. Derfor er vi i dag nødt til at håndtere en række risici forbundet med vores domæner, og den måde vi administrerer dem på.

I de senere år har Center for Cybersikkerhed set et stigende antal angreb på navneregistre, registranter og navnetjenester (se Bilag A: Begreber for begrebs-definitioner).

Angrebene inkluderer forsøg på:

- Kompromittering af navneregistre og registratorer
- Kompromittering af registranters konti hos registratorer
- DNS-hijacking af navneservere eller navnetjenester
- Anvendelse af navneservere i DDoS-angreb
- Man-in-the-middle-angreb og cache poisoning
- Kompromittering af DNS-opsætning på hjemmeroutere og computere

DDoS: DDoS står for Distributed Denial of Service og er et overbelastningsangreb. Hackere udnytter kompromitterede computere til at generere usædvanligt store mængder datatrafik mod en hjemmeside (webserver) eller et netværk, så hjemmesiden eller netværket ikke er tilgængeligt for legitim trafik, mens angrebet står på.

Man-in-the-middle: Angrebstype hvor en tredjepart opsnapper og/eller modificerer data i transit mellem to parter.

Cache poisoning: I DNS-sammenhæng et angreb hvor falske svar indsættes i DNS serveres cache med det formål at dirigere trafik til en anden adresse end den tiltænkte.

Læsevejledning

Denne vejledning er inddelt i to hovedafsnit, rettet til hver sin målgruppe. Afsnittene indeholder grupperede anbefalinger, der kan hjælpe organisationer med at reducere risici forbundet med angrebstyperne beskrevet ovenfor.

1. Anbefalinger til domæneadministration
Målgruppe: IT-ledelsen,
Anbefalingerne i dette afsnit kan hjælpe IT-ledelsen til at administrere domæner mere sikkert og reducere risikoen for, at forsøg på kompromittering og DNS-hijacking (pkt. 2 og 3) er succesfulde.

2.1 Anbefalinger til navneserverdesign og
2.2 Anbefalinger til DNSSEC
Målgruppe: IT-arkitekter og IT-drift
Anbefalingerne i dette afsnit kan hjælpe IT-arkitekter og IT-driften til at designe og vedligeholde en mere sikker navneservertjeneste. Tiltagene kan reducere risikoen for DNS-hijacking og misbrug af navneservere til DDoS-angreb samt beskytte mod DNS-relaterede man-in-the-middle-angreb (pkt. 3, 4 og 5).

Angreb mod navneregistre og registratorer eller forsøg på kompromittering af DNS-opsætningen på hjemmeroutere og computere er ikke dækket af denne vejledning.

1. Anbefalinger til domæneadministration

På trods af hvor kritiske domæneregistreringer er for en organisations tilstedeværelse på internettet, bliver de ofte konfigureret på registreringstidspunktet og siden glemt. Center for Cybersikkerhed anbefaler, at organisationer har en struktureret tilgang til domæne-administration og aktivt overvåger og vedligeholder både adgang til konti og selve registreringerne.

Sikker administration af en organisations domæner kan reducere risikoen for, at tilgængeligheden af organisations systemer påvirkes gennem for eksempel kompromittering af registrantkonti og DNS-hijacking.

I forbindelse med administration af domæner anbefaler Center for Cybersikkerhed følgende:

1.1	**Domæne administration**	Domæneoversigt
Dokumentér hvilke domæner organisationen anvender, og hvilke(n) registrator der er anvendt.		

Hvis domæner er registreret hos forskellige registratorer, bør man overveje at samle dem hos én registrator for at lette administrationen og have bedre kontrol med adgang. I evalueringen af registratorer bør man se på, hvilke sikringsforanstaltninger der tilbydes, for eksempel om der kan sættes multi-faktor autentifikation op på login-konti.

1.2	**Domæne administration**	Domæne vedligeholdelse
Gennemse med jævne mellemrum listen over domæner og vurdér hvorvidt de enkelte domæner skal beholdes eller nedlægges.		

Domæner er relativt nemme og billige at oprette, men de skal både administreres og sikres. Hvis et domæne ikke længere anvendes, kan man overveje at nedlægge det, for at reducere både administrationsbyrden og organisations angrebsflade.
Hvis et domæne har været tæt forbundet med organisationens identitet/brand, bør man overveje om domæneregistreringen i en overgangsperiode skal beholdes for at undgå, at andre overtager domænet. Ved at kigge i logs kan man se, om der stadig er trafik til tidligere hjemmesider.
Når et domæne nedlægges, bør der være en fast proces, der sikrer, at alle referencer til domænet i for eksempel firewalls, krypteringscertifikater, web- og mailservere mm. fjernes.

1.3	**Domæne administration**	Navneregisterkonti
Gennemse med jævne mellemrum hvilke navneregisterkonti, organisationen anvender til domæneadministration, og vurdér om de bør sammenlægges eller holdes adskilt.		

Danske domæner registreres under en navneregisterkonto hos DK Hostmaster. Denne navneregisterkonto (også kaldet "handle" eller "bruger-id") giver adgang til selvbetjeningsportalen på DK Hostmasters hjemmeside. På portalen kan man blandt andet overdrage brugsretten til domænet til andre, ændre hvilke navneservere, der er autoritative for domænet, og opdatere kontaktoplysninger på kontakterne for domænet. En navneregisterkonto kan administrere et eller flere domæner, men nogle organisationer har egne domæner registreret under flere separate konti, da de administreres af forskellige afdelinger. At have flere navneregisterkonti øger administrationsbyrden, og jo flere konti der anvendes, jo flere kan udsættes for kompromitteringsforsøg.

1.4	**Domæne administration**	Registratorkonti
Gennemse med jævne mellemrum hvilke administratorer, der har adgang til at vedligeholde organisationens domæner hos registrator, og sørg for, at det afspejler det forventede.		

Adgang til organisationens konti hos registrator bør begrænses til de administratorer, der har brug for adgangen. Administratorerne bør være deres ansvar og rolle bevidst og bekendt med risikoen for at blive udsat for phishingangreb. Et succesfuldt phishingangreb på en administrator med adgang til en registratorkonto kan resultere i, at organisationens domæner kidnappes.
Ved fratrædelse eller ændret opgaveansvar bør adgangen for administratorer lukkes øjeblikkeligt som led i organisations rettighedshåndteringsproces.

1.5	**Domæne administration**	Registratorkonti passwords
Sørg for, at administratorer anvender sikre passwords i henhold til organisationens politik på området. Hvis registrator understøtter multi-faktor autentifikation, bør dette anvendes.		

Login til registratorkonti er privilegerede og bør sikres tilsvarende. For anbefalinger vedrørende passwords og multi-faktor autentifikation henvises til passwordvejledningen på Center for Cybersikkerheds hjemmeside.

1.6	**Domæne administration**	Kontaktoplysninger
Validér, at kontaktoplysningerne for alle roller (registrant, fuldmægtig og betaler) er korrekte, og at eventuelle betalingsoplysninger er opdaterede.		

Det kan overvejes at anvende funktionspostkasser til de respektive roller for at forhindre, at vigtig kommunikation går tabt ved eventuelle fratrædelser. Det skal dog sikres, at disse aktivt monitoreres af relevante medarbejdere. Medarbejderes private mailadresser bør aldrig anvendes til registrering af en organisations domæner. For at opnå endnu højere sikkerhed kan det overvejes at anvende kontakter, hvis mailadresser ligger i et

andet domæne, der er administreret under en anden registratorkonto. Derved kan en hacker ikke bruge adgangen til en kompromitteret konto til at forhindre, at ændringsnotifikationer når frem til domænets kontakter.

1.7	**Domæne administration**	Retablering
Vær bekendt med registrators proces for at retablere et domæne, der er blevet kidnappet af anden part, og sørg for at have den nødvendige dokumentation.		

Følgende dokumentation kan være relevant for retablering af et kidnappet domæne:

- Udskrift af domæne registrering
  (WHOIS eller skærmprint/eksport fra registrator)
- Faktura og betalingskvittering
- Korrespondance med registrator omhandlende registrerede domæner
- Eventuelle juridiske dokumenter der knytter organisationen til domænenavn

1.8	**Domæne administration**	Domænefornyelse
Hold nøje øje med udløbsdatoen på registrerede domæner, og sørg for at forlænge relevante domæner i god tid.		

Mange registratorer tilbyder automatisk fornyelse af domæner, hvilket reducerer risikoen for, at domænet udløber, men forudsætter, at betalingsoplysninger holdes opdaterede. Selvom registratorer oftest minder registranter om domæner, der nærmer sig deres fornyelsesfrist, bør en organisation etablere sin egen proces for at sikre rettidig fornyelse. Hvis et domæne ikke fornyes i tide, mistes brugsretten til det, og domænet kan overtages af andre.

1.9	**Domæne administration**	Ændringer og gennemsyn
Følg en formel ændringshåndteringsproces, når en registratoroplysning skal ændres, og gennemse regelmæssigt eksisterende oplysninger for tegn på uautoriserede ændringer.		

For at undgå utilsigtede konsekvenser, bør organisationer være yderst varsomme med at ændre i domæneregistreringerne. Fejlkonfiguration kan i visse tilfælde føre til problemer med mailkommunikation og gøre organisations hjemmesider utilgængelige. Planlagte ændringer bør gennemses og godkendes i henhold til organisations ændringshåndteringsproces, før de gennemføres.

1.10	**Domæne administration**	Registrering af nye domæner
Hav en politik for registrering af nye domæner i organisationen, og følg en formel proces herfor.		

For at sikre at organisationen bevarer et overblik over sine domæner, og at nye domæner håndteres på sikker vis, bør en politik og proces for registrering udarbejdes og følges. Dette kan også hjælpe med at sikre, at nye domæner er godkendte, bliver registreret under de rette konti med de rette informationer, administreres af de rette ansvarlige, og sikres i henhold til organisationens politiker.

Det kan være svært for brugere af en webtjeneste at gennemskue, hvem der står bag et domæne, og det kan udnyttes til svindel. Et nyt domæne kan markedsføres under egen identitet, men alene det at domænet er nyt og ukendt, gør det til et interessant phishingmål. Organisationer bør derfor nøje overveje om der er behov for et separat domæne til en ny tjeneste, eller om tjenesten ud fra et sikkerheds- og kundebeskyttelseshensyn bør placeres under et eksisterende og allerede kendt domæne. Et underdomæne (f.eks. kundeservice.eksempel.dk), eller en adresse under et eksisterende domæne (f.eks. eksempel.dk/kundeservice), drager fordel af brugernes eksisterende kendskab til domænet, og af dets eksisterende sikringstiltag. Ud fra et sikkerhedshensyn er brug af kendte domænenavne derfor at foretrække.

For at minimere risikoen for phishing, bør det i samme omgang overvejes at registrere lignende domænenavne som brugerne kunne tænkes at anvende, for eksempel med minimalt ændrede stavemåder.

Hvis et nyt domæne primært anvendes til tjenester rettet mod danske brugere, kan anvendelsen af et .dk-domæne gøre at brugerne har større tillid til domænet, i kraft af de registreringskrav og anvendelsesvilkår .dk-domæner er underlagt.

1.11	**Domæne administration**	Registrator- og navneregisterlåse
Beskyt domæner mod uretmæssig overførsel, opdatering eller sletning ved hjælp af registrator- og navneregisterlåse.		

De specielle domæne-statuskoder: clientTransferProhibited, clientUpdateProhibited og clientDeleteProhibited kan sættes hos registrator for at låse domænet. Det betyder, at det skal låses op, inden man kan lave ændringer. Disse låse bliver i nogle tilfælde sat automatisk af registrator. Processen for oplåsning varierer fra registrator til registrator, men inkluderer ofte en ekstra validering hos de registrerede domænekontakter.

På navneregisterniveau kan domænet også oftest beskyttes mod uretmæssige (eller fejlagtige) ændringer. For gTLD'er foretages dette oftest via registratoren. For danske domæner (.dk) tilbyder DK Hostmaster en VID-Service (Very Important Domain), man kan tilkøbe med henblik på, at udpegede kontakter informeres om mindre kritiske ændringer og aktivt skal godkende ændringer af mere kritisk karakter. VID-Servicen er beskrevet nærmere på DK Hostmasters hjemmeside.

2.1 Anbefalinger til navneserverdesign

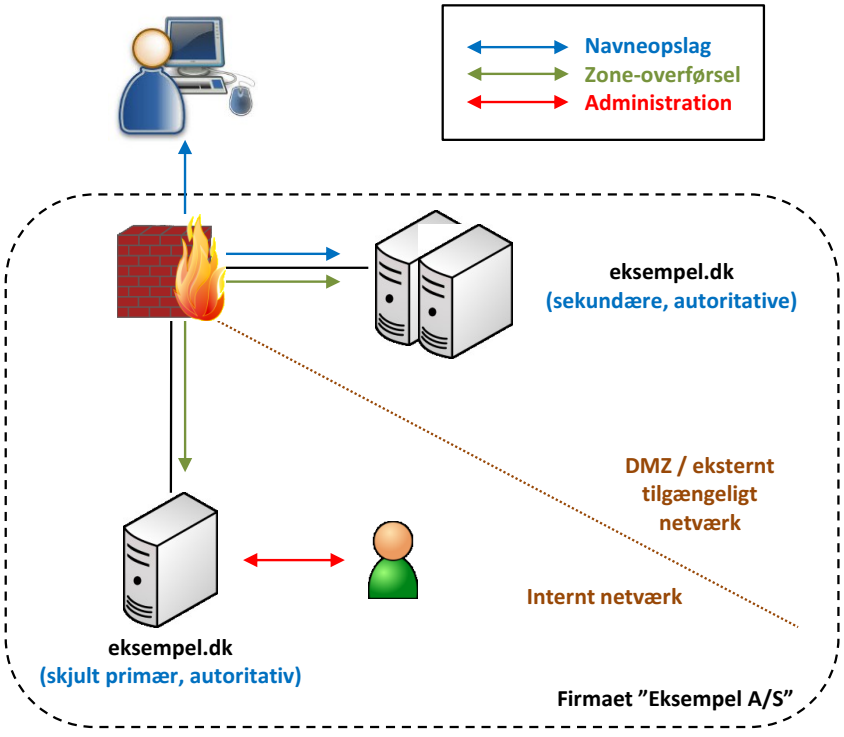
De følgende afsnit og deres anbefalinger er rettet til IT-arkitekter og IT-driften, og forudsætter en grundlæggende viden om DNS. Se Bilag A og B for en beskrivelse af de anvendte begreber og navneopslagsprocessen.

Uanset om en organisation vælger at drive sine egne navneservere, købe navnetjenesten hos en leverandør eller en kombination heraf, bør en række overordnede designprincipper følges.

Et sikkert navneserverdesign hjælper til at sikre både integriteten af organisationens navneserverdata og tilgængeligheden af organisationens systemer. Et sikkert navneserverdesign kan ligeledes reducere risikoen for, at navneserverne misbruges til DNS-baserede DDoS-angreb, eller udsættes for succesfulde cache poisoning-angreb.

Anbefalingerne er primært rettet mod navneservere, der anvendes til forespørgsler på eksterne domænenavne, men flere af principperne er også relevante for interne navneservere.

Et eksempel på et simpelt navneserverdesign for den fiktive virksomhed "Eksempel A/S" er illustreret i Figur 1 herunder:



Figur 1: Eksempel på navneserverdesign

Illustrationen er et eksempel og ikke i sig selv en konkret anbefaling til, hvordan et navneserverdesign bør implementeres. Det bedste design for en organisation afhænger blandt andet af organisationens størrelse, hosting-model, resurser og den geografiske fordeling af brugerne af de internet-tilgængelige tjenester.

I forbindelse med design af en navnetjeneste for internettilgængelige domæner anbefaler Center for Cybersikkerhed følgende:

2.1.1 Navneserver design	Adskil navneserverroller
Konfigurér autoritative navneservere til ikke at tillade rekursive navneforespørgsler.	

Autoritative navneservere, der kan tilgås fra internettet, bør ikke tillade rekursive forespørgsler. Rekursive forespørgsler øger belastningen på serveren og gør den potentielt sårbar over for DNS refleksions- og cache poisoning-angreb. Separate navneservere, der kun er tilgængelige for interne/kendte klienter, bør anvendes til alle rekursive navneforespørgsler.

2.1.2 Navneserver design	Interne og eksterne domæner
Inkludér ikke informationer om interne domæner og servernavne på eksternt tilgængelige navneservere.	

Navne og IP-adresser på interne systemer, der ikke skal tilgås fra eksternt hold, bør ikke være tilgængelige i zoner på eksterne navneservere.
Udskillelse af interne resurser til et eller flere subdomæner gør det muligt at administrere interne og eksterne domæner separat, og reducerer den internettilgængelige information om den interne infrastruktur.

2.1.3 Navneserver design	Navneserver redundans
Anvend flere eksterne navneservere for at sikre tilgængelighed af navnetjenesten.	

Det kan være en fordel at lade eksterne leverandører, der er uafhængige af organisationens egen infrastruktur, drive nogle, eller alle, organisationens eksterne navneservere. Eksterne leverandører af navneservertjenester er ofte i stand til at tilbyde god beskyttelse mod DDoS-angreb, geografisk distribuerede navneservere, samt døgnovervågning og specialiseret teknisk support. Nogle navneservertjenester understøtter også Anycast, der sikrer, at forespørgsler fra klienter håndteres af de geografisk distribuerede navneservere, der giver klienten de hurtigste svartider.

2.1.4 Navneserver design	Dedikerede navneservere
Anvend ikke eksterne navneservere til andet end levering af navnetjenester.	

Navneservere bør så vidt muligt ikke anvendes til andre formål og derfor ikke afvikle andet software end det, der er nødvendigt for navnetjenesten. Det reducerer angrebsfladen og risikoen for, at en sårbarhed i andet software kan påvirke sikkerheden for navnetjenesten.

2.1.5 Navneserver design	Skjult primær navneserver
Registrér ikke den primære autoritative navneserver for eksterne domæner som navneserver, og hold den utilgængelig fra internettet.	

Den primære navneserver indeholder den primære kopi af zonen og bør holdes utilgængelig fra internettet. Serveren bør i stedet kun anvendes til administration af zonen og til udveksling af zonedata med de internettilgængelige sekundære navneservere. Adgang til serveren bør begrænses til godkendte navneadministratorer. Se Figur 1 for illustration af et navneserverdesign med en skjult primær navneserver.

2.1.6 Navneserver design	Placering af sekundære navneservere
Placér sekundære navneservere i et isoleret netværkssegment, hvortil/fra kun relevant trafik tillades.	

Ved at isolere internettilgængelige navneservere på et separat netværkssegment med firewall beskyttelse reducerer man risikoen for, at en eventuel kompromitteret server kan bruges som trædesten til kompromittering af andre tjenester. Se evt. designeksemplet i Figur 1, hvor de internettilgængelige navneservere er isoleret i en DMZ. Tilgængeligheden af navneservertjenesten bør dog sikres gennem redundans i infrastrukturen og/eller ved at supplere med navneservere hos en ekstern leverandør.

2.1.7 Navneserver design	Firewall beskyttelse af navneservere
Beskyt navneservere med restriktive firewallregler, der kun tillader den nødvendige trafik.	

Et komplet firewallregelsæt til beskyttelse af en navnetjeneste afhænger af den valgte hosting-model og organisationens øvrige infrastrukturdesign.

I den nærmere analyse af, hvilken trafik der er nødvendig mellem forskellige klienter, servere og netværkssegmenter, bør følgende inddrages:

- Navneopslag bør kun tillades fra de tiltænkte klienter (interne eller eksterne, afhængig af navneserverens rolle) via TCP og UDP til port 53.
- Rekursive navneservere, der betjener egne brugere, skal kunne foretage navneopslag via TCP og UDP på port 53 mod internettet.
- Autoritative sekundære navneservere skal kunne modtage notifikationer fra den primære navneserver og kunne udveksle zone information med kun denne.
- Trafik til en central logningsservice og trafik nødvendig for administration af serverne, bør begrænses til nødvendige IP-adresser og porte.
- Det bør overvejes at aktivere DNS protokol inspektion, hvis dette er understøttet af firewallen, for at sikre, at kun trafik, der lever op til de officielle DNS-specifikationer, tillades. Vær dog opmærksom på, at aktivering af DNSSEC kan kræve accept af større DNS-pakker og anvendelse af TCP til opslag/svar.

De endelige firewallregler bør testes grundigt, inden navneserverne tages i drift.

2.1.8 Navneserver design	Sikker kommunikation mellem navneservere
Anvend TSIG til at sikre zonetransfers mellem den primære og de sekundære navneservere.	

Hvis zoneinformation distribueres til sekundære navneservere ved hjælp af zonetransfer fra den primære navneserver, bør kommunikationen sikres ved hjælp af transaktionssignaturer (TSIG[1]). TSIG sikrer, at zonetransfer kun sker til autentificerede sekundære navneservere og sikrer integriteten af selve opdateringerne. Man bør anvende unikke TSIG-nøgler for hvert navneserverpar, og TSIG bør suppleres med relevante restriktive firewallregler (se ovenfor). Nøglerne genereres i navneserverprogrammet, der konfigureres til at signere al kommunikation med navneserver-modparten.

2.1.9 Navneserver design	Reducer risiko for deltagelse i DDoS angreb
Konfigurér navneservere og netværksenheder med henblik på at reducere risikoen for at blive udnyttet i DNS reflektionsbaserede DDoS-angreb.	

Navneservere kan i nogle tilfælde anvendes til DNS reflektionsangreb, hvor afsender IP-adressen i en DNS-forespørgsel forfalskes til at anvende et offers IP-adresse i stedet. Da svarpakkerne fra navneservere er større end selve forespørgslen, kan det udnyttes til at overbelaste offerets server eller netværksresurser. Når DNSSSEC anvendes, er svarpakkerne endnu større, da de indeholder en digital signatur. Det gør DNSSEC-understøttende navneservere endnu mere interessante for dem, der vil foretage et DDoS-angreb. Denne risiko kan reduceres med følgende yderligere tiltag:

- Tillad ikke rekursive forespørgsler fra internettet
- Tillad ikke AXFR (zonetransfer) forespørgsler fra andre end autoriserede navneservere
- Overvej at begrænse antallet af forespørgsler, der accepteres fra den samme IP-adresse, inden for et givent tidsrum (rate limiting)
- Konfigurer routere og firewalls til kun at acceptere netværkspakker fra IP-adresser, der er gyldige på det netværk, pakken kommer fra (IP-spoofing beskyttelse)
- Tillad ikke ANY (alle records) forespørgsler, hvis det er muligt i navneserversoftwaren

2.1.10 Navneserver design	Versionsinformation
Konfigurér navneservere til ikke at oplyse navn eller versionsnummer af software i deres svar.	

Hvis en navneserver oplyser navn eller versionsnummer på den software, der driver tjenesten, kan en hacker nemt slå eventuelle kendte sårbarheder op og dermed lettere målrette et angreb til den specifikke version. At skjule navn og versionsnummer fjerner ingen sårbarheder, men det kan tvinge en hacker til foretage yderligere rekognoscering, man nemmere kan opdage i organisationens monitoreringssystemer. Det er god praksis ikke at offentliggøre unødvendig information, men det er vigtigere at prioritere, at navneservere og deres underliggende operativsystemer holdes rettidigt opdateret (se herunder).

[1] https://tools.ietf.org/html/rfc2930

2.1.11 Navneserver design Sikkerhedsopdateringer
Hold navneservere og deres underliggende operativsystemer rettidigt opdateret.

Sikkerhedsopdateringer af både navneserver-softwaren og det understøttende hosting-miljø adresserer identificerede sårbarheder og hjælper med at sikre integriteten af domænedata samt tilgængeligheden af organisationens navneservice. Hvis navneservicetjenesten leveres helt eller delvist af en leverandør, skal organisationen sikre sig, at rettidig test og installation af sikkerhedsopdateringer følger en klart defineret, og af organisationen accepteret, proces.

2.1.12 Navneserver design Konfigurationsændringer
Følg en formel ændringshåndteringsproces ved ændringer i navneserveres konfiguration eller i det overordnede design.

Alle planlagte ændringer i navneserverdesign eller konfiguration bør gennemses og godkendes i henhold til organisationens ændringshåndteringsproces, før de gennemføres. En struktureret tilgang til ændringshåndtering kan reducere risikoen for utilsigtede konsekvenser og styrke tilgængeligheden.

2.1.13 Navneserver design Logning
Log administrationsaktiviteter på navneservere i henhold til organisationens logningspolitik, og gennemse logs for tegn på uautoriseret aktivitet.

Som minimum bør man logge både afviste og godkendte logins, samt alle konfigurations- og zoneændringer. Gode logs kan hjælpe når der skal fejlfindes, eller ved håndtering af sikkerhedshændelser. Læs mere i logningsvejledningen på Center for Cybersikkerheds hjemmeside.

2.1.14 Navneserver design Gennemse records
Gennemse regelmæssigt zonerne for at sikre, at records er korrekte, og der ikke er foretaget uautoriserede ændringer.

Man bør jævnligt verificere at eksisterende records er relevante og korrekte. Hvis en record ikke længere anvendes eller peger på IP-adresser, der ikke bruges til det registrerede formål, bør den fjernes. Hvis der findes tegn på uautoriserede ændringer, bør den it-sikkerhedsansvarlige orienteres øjeblikkeligt.

2.1.15 Navneserver design Anvend DNSSEC
Anvend DNSSEC på alle eksterne domæner.

DNSSEC beskytter mod forfalskning af svar på navneforespørgsler og sikrer, at svaret kommer fra autentificerede navneservere. DNSSEC bør derfor anvendes på alle eksterne domæner, uanset om et domæne anvendes aktivt til for eksempel hjemmesider og mail, eller blot er registreret med henblik på at beskytte organisationens online identitet. Selvom et domæne ikke anvendes aktivt af registranten, kan et manipuleret svar lede en forespørger til en phishingside under en andens kontrol, hvis ikke DNSSEC er slået til.

2.2 Anbefalinger til DNSSEC

Da DNS er essentiel for lokaliseringen af tjenester på internettet, kan hackere være interesseret i at manipulere med svar på navneforespørgsler ved hjælp af man-in-the-middle angreb eller cache poisoning. Hvis det lykkes, kan en bruger for eksempel sendes til en anden side end den tiltænkte og blive fraluret sine logindetaljer eller andre beskyttelsesværdige oplysninger. Denne type angreb ses oftest rettet mod eksterne domæner på internettet.

DNSSEC (Domain Name System Security Extensions) er et sæt udvidelser til DNS-standarden, der anvender kryptografi til at sikre, at forespørgeren kan bekræfte, at:

- svaret på et navneopslag kommer fra de rigtige navneservere
- svaret ikke er manipuleret undervejs
- svaret om, at et givet navn ikke eksisterer, kan autentificeres som værende korrekt

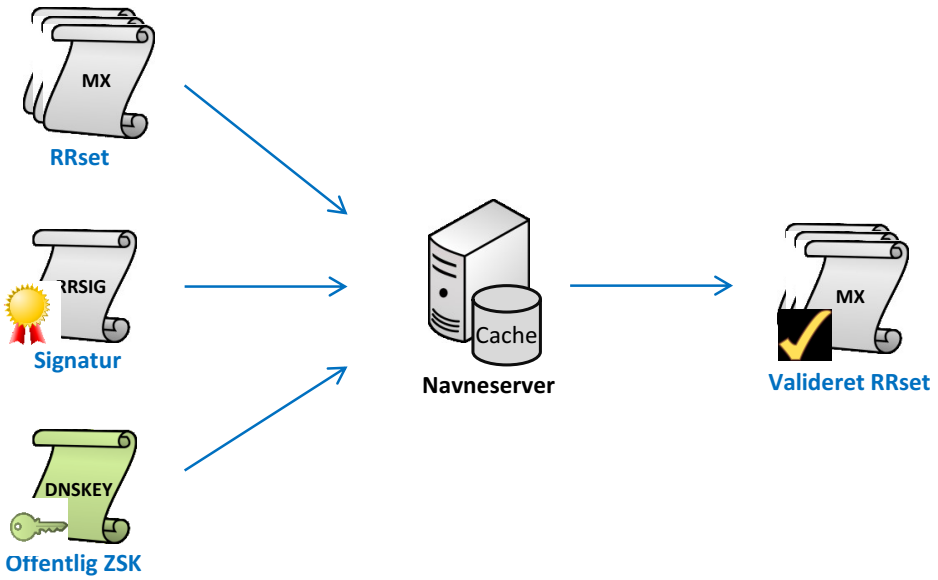
Det bør bemærkes, at DNSSEC ikke krypterer selve DNS-trafikken. Overvejelser vedrørende kryptering af DNS-trafik, herunder anvendelse af teknologier som DNS-over-TLS eller DNS-over-HTTPS, er ikke belyst i denne vejledning.

DNSSEC valideringsprocessen
Processen for navneopslag i DNSSEC-beskyttede domæner følger i store træk den normale opslagsproces (se Bilag B: Navneopslagsprocessen), men inkluderer kryptografisk validering af både de enkelte svar og de navneservere i hierarkiet, der er involveret i processen.

Validering af svar
Til validering af svar på navneopslag anvendes følgende records:

- **RRset (Resource Record Set):**
  Gruppering af alle records af en given type, for eksempel alle A-records eller MX-records
- **RRSIG (Resource Record Signature):**
  Signeret hash-værdi af et RRset, baseret på den private ZSK
- **ZSK (Zone Signing Key):**
  Offentlig krypterings nøgle til validering af RRSIGs i zonen
- **DNSKEY:**
  Record type, der anvendes til opbevaring af offentlige krypteringsnøgler

Processen for validering af svar i en DNSSEC-signeret zone er illustreret i Figur 2 herunder:



Figur 2: Proces for validering af en Resource Record (i dette tilfælde en MX record)

Ved hjælp af den offentlige Zone Signing Key (ZSK) kan navneserveren, der håndterer forespørgslen, validere signaturen (RRSIG) for det Resource Record Set (RRset), der indeholder den efterspurgte record. Dette sikrer, at et kompromitteret svar bliver opdaget.

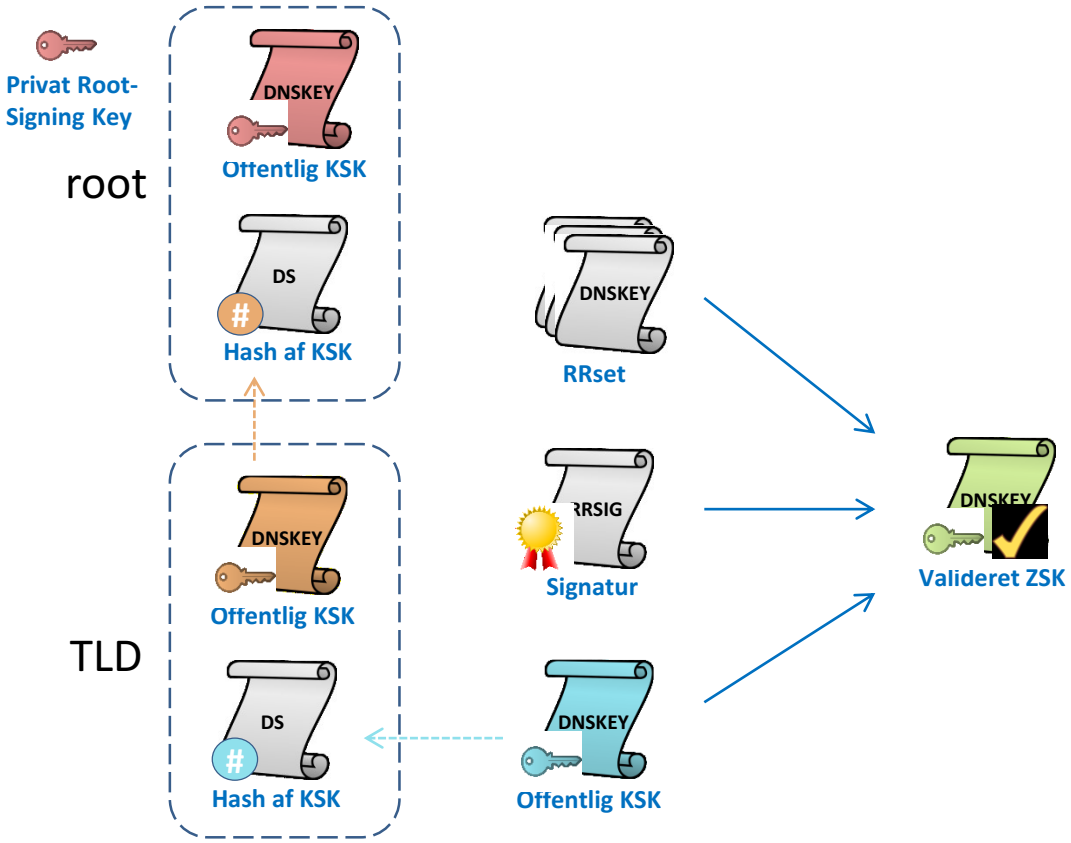
Validering af svarende servere

For at sikre, at det validerede svar også er kommet fra en gyldig navneserver, der er autoriseret til at svare for domænet, skal den offentlige ZSK, der blev anvendt i processen herover (grøn farvet), kunne valideres. Til dette formål anvendes følgende records:

- **KSK (Key Signing Key):**
  Offentlig krypterings nøgle til validering af RRSIG-signaturen for et RRset af DNSKEYs, herunder Zone Signing Keys.
- **DS (Delegation Signer):**
  Hash-værdi af den offentlige KSK, der gemmes i zonen hvorfra domænet er delegeret (parent zone).

Processen ligner den tidligere illustrerede, men er kædet sammen gennem TLD op til roden af DNS-systemet i et "chain of trust" (se Figur 3). Den offentlige ZSK valideres med en offentlig KSK, hvis hash-værdi er gemt i en DS-record i zonen over (parent zone). For .DK domæners vedkommende er denne DS-record gemt i ccTLD-registeret (hos DK

Hostmaster), hvis egen KSK er repræsenteret med sin hash-værdi i roden af hierarkiet[2]. På den måde kan det igennem zone-hierarkiet kryptografisk valideres, at det er autoriserede navneservere, der giver de signerede svar på navneforespørgslen.



Processen er illustreret i Figur 3 herunder:

Figur 3: Oversigt over DNSSEC valideringsprocessen.

Selvom valideringsprocessen måske ser kompleks ud, er det er ofte simpelt at aktivere DNSSEC på organisationens domæner. Aktiveringen kan foretages via navneserviceudbyderen (ofte registrator) eller af egen navneserveradministrator. For yderligere information vedrørende DNSSEC på .dk-domæner henvises til DK Hostmasters hjemmeside.

Uafhængigt af aktivering af DNSSEC på organisationens eksterne domæner anbefaler Center for Cybersikkerhed følgende:

2.2.1 DNSSEC	Validering af DNSSEC på rekursive navneservere
Aktivér validering af DNSSEC-signerede svar på de rekursive navneservere, der betjener organisationens brugere.	

[2] De offentlige KSK og ZSK for det øverste domæne i hierarkiet (rod-domænet) signeres af den private Root-Signing Key ved en ceremoni, der finder sted fire gange om året, og følger en omstændig proces, der har til formål at bevare tilliden til rod-nøglerne. Processen er beskrevet af en af deltagerne på Cloudflares blog: https://cloudflare.com/dns/dnssec/root-signing-ceremony

For at beskytte egne brugere mod forfalskede svar, eller svar fra uautoriserede navneservere, bør navneservere, der foretager navneopslag på vegne af organisationens brugere, konfigureres til at validere svar for domæner, der har aktiveret DNSSEC. Vær opmærksom på, at hvis et svar fejler DNSSEC-valideringen, kan det være tegn på manipulation af svaret, men kan også skyldes fejlkonfiguration i den DNSSEC-signerede zone.

Ved fejlsøgning kan følgende værktøjer være til hjælp:
https://dnssec-debugger.verisignlabs.com/
https://dnsviz.net/

Aktivering og drift af DNSSEC
Hvis administrationen af organisationens eksterne domæner og tilhørende navneserver-infrastruktur håndteres af en leverandør, findes der gode råd at hente i vejledningen "Informationssikkerhed i leverandørforhold" på Center for Cybersikkerheds hjemmeside.

Uanset hvem der står for navneservertjenesten, bør følgende anbefalinger i forbindelse med aktivering og drift af DNSSEC følges:

2.2.2 DNSSEC	Aktiver DNSSEC på alle autoritative navneservere
Understøt DNSSEC på alle navneservere, der er autoritative for en given zone.	

Hvis ikke alle navneservere i en DNSSEC-signeret zone understøtter DNSSEC, kan valideringen fejle og resultere i tilgængelighedsproblemer.

2.2.3 DNSSEC	Fornyelse af signaturer
Forny signaturer automatisk i god tid inden udløb af deres gyldighedsperiode.	

En zone, der ikke er DNSSEC-aktiveret, opdateres oftest kun, når eksisterende records ændres, slettes, eller når nye oprettes. Ved anvendelse af DNSSEC bør man være opmærksom på, at signaturer kun er gyldige i en begrænset periode og derfor skal fornyes i god tid inden periodens udløb. Der bør også tages højde for, at records baseret på de gamle signaturer kan være cachet, og at de derfor fortsat skal kunne valideres, indtil de ikke længere er cachet (Time-To-Live (TTL) er udløbet). Hvis en aktiv signatur udløber, vil det resultere i at klienter, der validerer DNSSEC signaturen, ikke vil kunne tilgå resursen. Processen for fornyelse af signaturer håndteres oftest automatisk, men bør monitoreres.

2.2.4 DNSSEC	Svar på forespørgsler om ikkeeksisterende domænenavne
Anvend NSEC3 til håndtering af svar på forespørgsler om ikkeeksisterende domænenavne.	

Ligesom svar på navneopslag på eksisterende domænenavne kan autentificeres med DNSSEC, er der også behov for at kunne autentificere svar på forespørgsler på ikkeeksisterende domænenavne. NSEC3 kan anvendes til det formål ved at kæde alle eksisterende navne i zonen sammen og derved bevise, at navne, der ikke optræder i kæden, ikke er gyldige. For at beskytte zonen mod at der kan indhentes et komplet sæt af gyldige navne ved at gå hele kæden igennem, anvender NSEC3 saltede hash-repræsentationer af navnene i stedet for at angive dem i klar tekst.

2.2.5 DNSSEC	Fornyelse af nøgler
Forny Key Signing Keys og Zone Signing Keys regelmæssigt og automatisk og altid ved mistanke om kompromittering	

Key Signing Keys og Zone Signing Keys har ingen gyldighedsperiode, men bør regelmæssigt fornyes for at undgå eller håndtere kompromittering. De fleste navneserver-løsninger kan automatisere denne proces, men vær opmærksom på at fornyelse af Key Signing Keys kræver udveksling af opdaterede DS records med zonen over (parent zone).
Man bør sikre, at processen tager hensyn til gyldighedsperioden for de tidligere genererede signaturer, cache levetid (TTL), og replikering af DNS records i DNS-infrastrukturen.

2.2.6 DNSSEC	Key Signing Key generering og opbevaring
Generér og opbevar Key Signing Keys på en sikret enhed.	

Da Key Signing Keys ligger til grund for de Zone Signing Keys der anvendes i en DNSSEC aktiveret zone, bør de genereres og opbevares sikkert. Organisationer med høje sikkerhedskrav og/eller krypteringsbehov kan med fordel anvende et Hardware Security Module (HSM) til sikker generering og opbevaring af krypterings- og signeringsnøgler.

2.2.7 DNSSEC	Nøgle- og hash algoritmer
Anvend algoritme 13 - ECDSAP256SHA256 (ECDSA Curve P-256 med SHA-256)[3] til kryptering og hashing.	

Blandt de anvendte krypteringsalgoritmer i DNSSEC-signerede .dk-zoner er langt de fleste baseret på Algoritme 13[4]. Nøgler og signaturer baseret på ECDSA er meget kortere end RSA-baserede algoritmer og fylder derfor mindre i zonen og navneopslag. De er hurtigere at signere med, men langsommere at validere. Hvis der er brug for en anden balance mellem sikkerhed og hastighed, kan andre algoritmer overvejes. Uanset hvilken algoritme der anvendes, vil DNSSEC-signerede svar ofte have en størrelse, der kræver, at de sendes over en TCP forbindelse. Som tidligere angivet er det derfor vigtigt at tillade DNS-forespørgsler via TCP.

2.2.8 DNSSEC	Netværksunderstøttelse af DNSSEC trafik
Verificér, at den netværksinfrastruktur, navnetjenesten anvender, understøtter DNSSEC trafik.	

Da svar på navneforespørgsler i en DNSSEC-signeret zone er større, end hvis DNSSEC ikke var aktiveret, bør man sikre sig, at netværksudstyr og firewalls understøtter dette. Dette bør grundigt testes inden DNSSEC aktiveres, for at undgå problemer med tilgængeligheden af ens tjenester.

[3] https://tools.ietf.org/html/rfc6605 og https://tools.ietf.org/html/rfc8624
[4] https://stats.dk-hostmaster.dk/domains/dnssec_domains/algorithm

Yderligere relaterede tiltag

Nedenstående teknologier er ikke behandlet i denne vejledning, men kan med fordel overvejes som supplerende tiltag til beskyttelse af en organisations infrastruktur og kommunikation:

- DANE: DNS-based Authentication of Named Entities
  Forudsætter DNSSEC og kan anvendes til:
  - at angive hvilken Certificate Authority domæneejeren tillader, at udstede certifikater for resurser i domænet
  - at angive godkendte krypteringscertifikater i anvendelse for resurser i domænet
  - at indikere over for afsendere af mails, at de skal kryptere trafik til domænets mail servere
- SPF: Sender Policy Framework
  DKIM: DomainKeys Identified Mail
  DMARC: Domain-based Message Authentification, Reporting and Conformance
  DNS-baserede tiltag, der kan hjælpe til at forhindre, at forfalskede mails bliver leveret til modtageren.
  Læs mere på Center for Cybersikkerheds hjemmeside i vejledningen: ”Reducér risikoen for falske mails”.

Referencer

Center for Cybersikkerhed vil gerne takke DK Hostmaster (https://www.dk-hostmaster.dk) for den faglige sparring i forbindelse med udarbejdelsen af denne vejledning.

Inspiration til indhold er blandet andet hentet fra:

https://blogs.akamai.com/2019/02/protecting-your-domain-names-taking-the-first-steps.html
https://www.icann.org/en/system/files/files/sac-044-en.pdf
https://www.cloudflare.com/dns/dnssec/how-dnssec-works/
https://www.enisa.europa.eu/publications/gpgdnssec
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-81-2.pdf
https://www.cisco.com/c/en/us/about/security-center/dnssec-best-practices.html
https://www.stigviewer.com/stig/domain_name_system_dns_security_requirements_guide/
https://tools.ietf.org/html/rfc6781

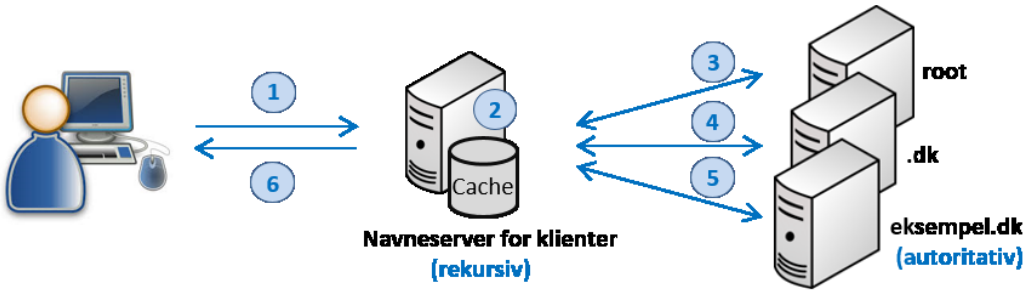
Bilag A: Begreber

Herunder opstilles en række begreber, deres definitioner, samt en beskrivelse af navneopslagsprocessen, som baggrund for anbefalinger i denne vejledning:

- DNS (Domain Name System): System og netværksprotokol der primært faciliterer oversættelse af navne til IP-adresser på et netværk. Navnesystemet er hierarkisk opbygget og håndteres af et decentraliseret netværk af navneservere.
- Top-Level Domæne (TLD): Øverste domæne i navnehierarkiet. Kan være både globale (gTLD) som .com, .org, .edu osv. og lande-specifikke (ccTLD) som .dk, .se osv.
- Navneregister: Database over alle domæner i et givet TLD, deres registranter og de autoritative navneservere. For .dk-domæner er det DK Hostmaster, der administrerer navneregisteret.
- Registrator: Forhandler der formidler registrering af domænenavne. Mange registratorer tilbyder også hosting af hjemmesider og navneservertjenester, men det er ikke et krav, at disse leveres af registratoren.
- Registrant: Person eller organisation med registreret brugsret til et domæne.
- Fuldmægtig: Person eller organisation med fuldmagt fra registranten af et domæne til at udføre handlinger vedrørende domænenavnet.
- Navneserver: Server eller service der oversætter navne til IP-adresser ved hjælp af DNS-protokollen.
    - Rekursiv navneserver: Navneserver der hjælper klienter med at finde svar på deres navneforespørgsler ved at se, om det allerede er cachet, og ellers spørge relevante navneservere, indtil et autoritativt svar opnås.
    - Autoritativ navneserver: Navneserver der har fået delegeret det autoritative ansvar for en given zone.
- Zone: En zone indeholder alle oplysninger om et domæne, som navneserveren har autoritativt ansvar for. Hvis domænet ikke indeholder subdomæner, der håndteres af andre navneservere, kan begreberne ”zone” og ”domæne” være sammenfaldende. Hvis domænet indeholder et eller flere subdomæner, der håndteres af andre navneservere, siges domænet at være opdelt i flere zoner.
- Ressource record (RR): En record i en zone, der som udgangspunkt består af et navn, en type, og en værdi. Eksempel på en type A Ressource Record fra zonen eksempel.dk:
    - www A 193.163.102.58 - En Address/host record (A) der returnerer IP-adressen 193.163.102.58 på forespørgsler på navnet www.eksempel.dk

Bilag B: Navneopslagsprocessen

Processen for navneopslag er illustreret og beskrevet herunder:



Figur: Proces for navneopslag

1. Når en klient vil besøge hjemmesiden "www.eksempel.dk" sendes forespørgslen først til en af de navneservere, som computeren er sat op til at anvende. I en virksomhed er det oftest interne navneservere på virksomhedens eget netværk. I hjemmet er det oftest navneservere hos internetudbyderen, der anvendes.
2. Navneserveren ser i sin cache, om den allerede kender svaret på baggrund af en tidligere forespørgsel.
   Hvis svaret er i navneserverens cache, returneres det til klienten og processen stopper.
3. Hvis svaret ikke er kendt, og navneserveren ikke ved hvilke navneservere, der er ansvarlige for domænet "eksempel.dk", eller for top-level domænet ".dk", spørges en af de kendte navneservere i roden af hierarkiet "root" om hvilke navneservere, der er ansvarlige for ".dk"-domæner.
   Hvis de ansvarlige navneservere for "eksempel.dk" kendes, gås direkte til trin 5.
   Hvis de ansvarlige navneservere for ".dk" kendes, gås direkte til trin 4.
4. Navneserveren spørger herefter en af de ".dk"-navneservere, der blev henvist til, om hvilke navneservere, der er ansvarlige for domænet "eksempel.dk".
5. Herefter spørger navneserveren en af de "eksempel.dk"-navneservere, der blev henvist til, og får svaret på forespørgslen (IP-adressen på "www.eksempel.dk").
6. Svaret returneres til klienten og caches i et stykke tid på navneserveren. Forespørgsler på samme navn, eller forespørgsler på nogle af de involverede navneservere, kan derfor gives uden at skulle gentage hele processen.

Klientens navneserver foretager en rekursiv forespørgsel på vegne af klienten (pkt. 3-5) og sikrer, at et svar opnås, selvom flere navneservere måske skal konsulteres.

Den organisation, der driver den autoritative navneservice for et domæne (for eksempel det fiktive firma "Eksempel A/S" med domænet "eksempel.dk"), er ansvarlig for at kunne levere viden om alle navne i domænet til den forespørgende rekursive navneserver.