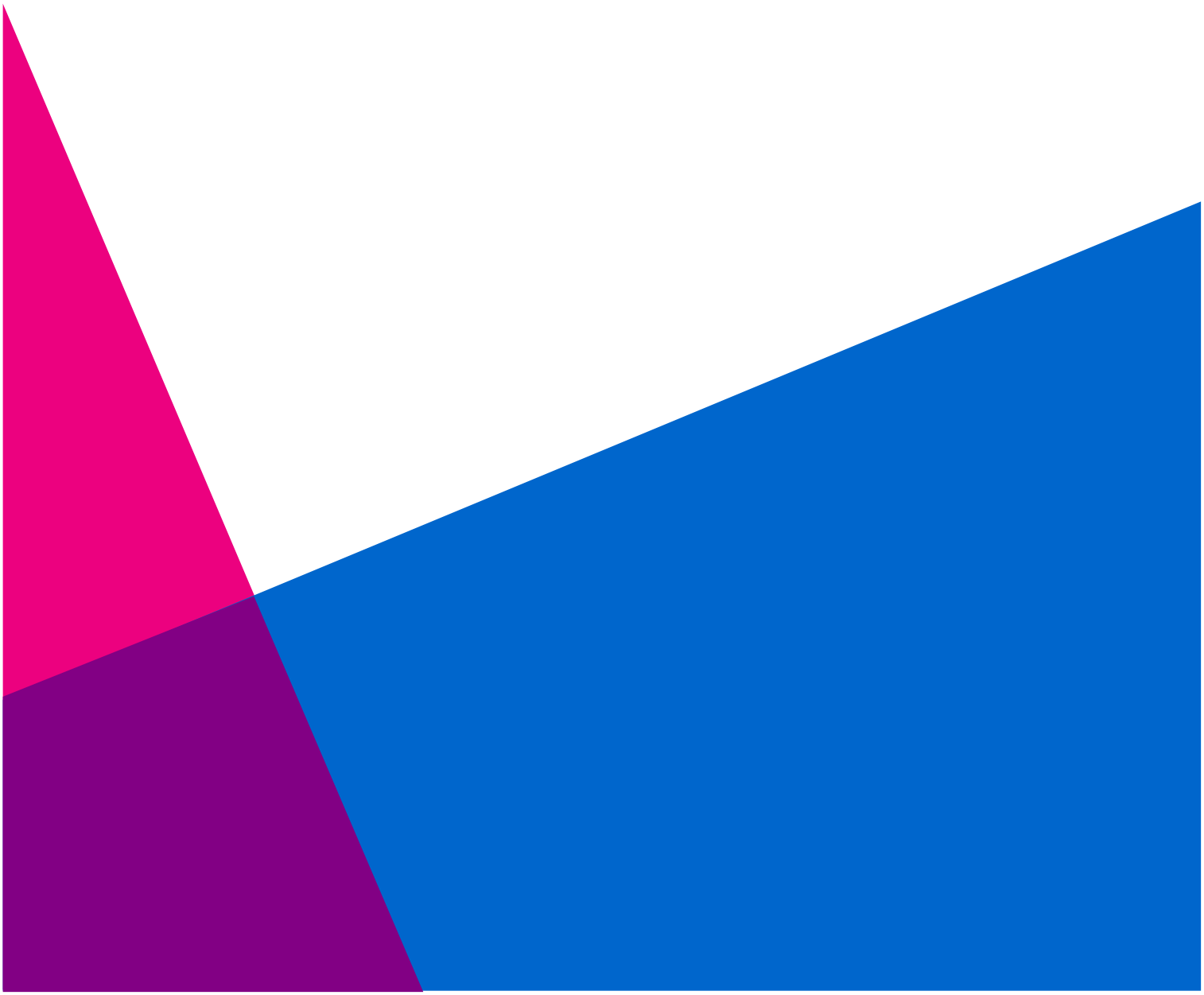
TRAFICOM
Liikenne- ja viestintävirasto

Säker domänförvaltning

Guide för registrarer och användare av domännamn

Teamet för fi-domännamn



Innehållsförteckning

Inledning

Om en illvillig aktör kommer över en organisations domännamn kan åtkomsten till organisationens webbplats förhindras, e-posttrafiken stoppas, VPN-trafik dirigeras fel och krypteringscertifikat, inloggningsuppgifter och andra viktiga uppgifter hamna i orätta händer. En sådan händelse kan ha omfattande ekonomiska eller politiska följder.

I den här publikationen ges rekommendationer för hur organisationer kan skydda sina domännamn. Rekommendationerna kan hjälpa organisationer att minska risken för negativa imageeffekter på internet, förbättra sina systems användarvänlighet och tillförlitlighet samt öka kommunikationens trovärdighet och säkerhet.

Organisationens identitet på internet är starkt kopplad till domännamnet. Kommunikationen med organisationen, från besök på webbplatsen till sändande av e-postmeddelanden, är beroende av att domännamnet går att hitta. Därför behöver varje organisation kunna skydda sitt domännamn.

Anvisningarna är avsedda främst för organisationernas informationshanteringschefer och tekniska personal. Förhoppningen är att rekommendationerna ska stödja organisationerna i arbetet med utveckling av befintliga rutiner samt i att säkerställa att förvaltningen av domännamn inte orsakar onödiga risker för organisationen.

Allmänna rekommendationer

Härnäst presenteras allmänna rekommendationer och god praxis för trygg domänförvaltning. Rekommendationerna kan hjälpa organisationer att hantera risker i förvaltningen av domännamn.

De allmänna rekommendationerna och de principer som nämns nedan är exempel, inte en uttömmande förteckning:

- Organisationen ska känna till alla sina domännamn.
- Funktionen för ändring av registeruppgifter om domännamn ska skyddas genom identifiering.
- Vid ändring av registeruppgifter om domännamn följer man alltid ett standardförfarande.
- Registeruppgifterna om domännamn ska kontrolleras regelbundet.
- Namnservern ska utformas så att den skyddar organisationens domännamn och säkerställer deras användbarhet.
- Alla domännamn bör skyddas med DNSSEC-tillägg.
- Namnförfrågningar bör verifieras med hjälp av DNSSEC.

Bakgrund

Namntjänstsystemet domain name system (DNS) togs i bruk i början av 1980-talet. Målet var att skapa ett effektivt och tillförlitligt distribuerat system för namntjänstförfrågningar, som kunde hantera förfrågningarna från det växande datornätet.

Ur detta nätverk utvecklades det världsomspännande internet, som är välbekant för oss i dag. För att de oräkneliga tjänsterna på internet ska fungera krävs dock fortfarande ett fungerande DNS-system, men när systemet skapades tänkte man dessvärre inte så mycket på säkerheten. Därför möter vi nu många olika slags risker i anknytning till domännamn och förvaltningen av dem.

Traficom har noterat att attackerna mot namndatabaser, domännamnsanvändare och namntjänster har ökat under de senaste åren (se begreppsdefinitionerna i bilaga A: Begrepp)

Exempel på typer av attackförsök

- Intrång i namndatabaser och registrarers uppgifter
- Intrång i administratörskonton domännamn som upprätthålls av förmedlarna
- DNS-kapning av namnservrar eller -databaser
- Utnyttjande av namnservrar i överbelastningsangrepp
- *Man in the middle*-attack och cache-förgiftning
- Manipulering av DNS-inställningarna för routrar och datorer för hemmabruk

Överbelastningsangrepp: Spridd överbelastningsattack, som på engelska kallas för *distributed denial of service* (DDoS). Hackare utnyttjar datorer som de tagit kontroll över för att skapa onormalt mycket trafik till en viss webbplats (webbserver) eller ett visst nätverk. Det leder till att webbplatsen eller nätverket slutar fungera och inte är tillgänglig för verkliga användare under angreppet.

Man in the middle: En typ av angrepp där en tredje part kapar information som sänds mellan två parter och eventuellt även ändrar på den.

Cache-förgiftning: Attack mot en DNS-tjänst (eng. *cache poisoning*), där felaktiga svar planteras i cacheminnet i en DNS-server för att avsiktligt dirigera trafik till fel adress.

Läsanvisning

Anvisningarna är indelade i två huvudsakliga delar med separata målgrupper. Delarna innehåller grupperade rekommendationer, som kan hjälpa organisationer att minska de risker som förknippas med ovan nämnda angreppstyper.

1. Rekommendationer gällande domänförvaltning Målgrupp: ledningen för informationshantering

Rekommendationerna i detta avsnitt kan hjälpa ledningen för informationshanteringen att förvalta domännamn på ett säkert sätt samt bekämpa försök till äventyrande av domännamnen och DNS-kapningar.

2.1 Rekommendationer för planering av namnservrar och 2.2 Rekommendationer gällande DNSSEC

Målgrupp: Datasystemexperter och informationshanteringens tekniska personal

Rekommendationerna i detta avsnitt kan hjälpa systemexperter och informationshanteringens tekniska personal att planera och upprätthålla säkra namnservrar. Genom åtgärderna kan man minska risken för DNS-kapningar, förhindra utnyttjande av namnservrarna i DDoS-angrepp och skydda mot man in the middle-attacker i DNS-systemet.

Anvisningarna berör inte attacker mot namndatabaser (whois-tjänster, OData) eller registrarer, och inte heller försök till manipulering av DNS-bestämningar för routrar eller datorer i hemmen.

1 Rekommendationer för domänförvaltning

Även om domännamnen är centrala faktorer för organisationens synlighet på internet, lämnas de ofta åt sitt öde efter att de har fastställts i samband med registreringen. Traficom rekommenderar att organisationer ska förvalta sina domännamn systematiskt samt aktivt övervaka och upprätthålla sina användarkonton och domännamnsregistreringar.

Genom att förvalta sina domännamn på ett säkert sätt kan organisationen förhindra utomstående försök att påverka åtkomsten till dess system, såsom manipulering av domännamnsinnehavarnas användarkonton och DNS-kapningar.

1.1	**Domänförvaltning**	Sammandrag om domännamn
Dokumentera organisationens domännamn och registrar.		

Om man har registrerat domännamn via olika registrarer, bör man överväga att koncentrera dem till en registrar för att underlätta förvaltningen och övervakningen av användningen.

I bedömningen av registrarer bör man också beakta de säkerhetsåtgärder som de erbjuder, såsom möjlighet till tvåstegsverifiering vid inloggning i användarkonton i ett självbetjäningsgränssnitt.

1.2	**Domänförvaltning**	Upprätthållande av domännamn
Gå regelbundet igenom förteckningen över domännamn och bedöm vilka man behöver behålla och vilka man kunde avstå från.		

Det är enkelt och förmånligt att registrera domännamn, men de måste förvaltas och säkerheten måste övervakas. Om ett domännamn inte längre används bör man överväga att avstå från det både för att minska den administrativa bördan och för att minska ytan för angrepp mot organisationen. FI-domännamn kan registreras även utan namnserver.

Registrering utan namnserver rekommenderas om man så att säga vill ”parkera” domännamnet i väntan på framtida användning.

Om ett domännamn har haft en nära förbindelse med organisationens identitet eller varumärke, bör man överväga att fortsätta ha det registrerat för en övergångsperiod för att förhindra att någon annan får kontroll över det. Genom att kontrollera loggarna kan man se om det fortfarande kommer trafik till den gamla webbplatsen.

När man avstår från ett domännamn ska man följa en viss process, som säkerställer att alla hänvisningar till domännamnet tas bort från exempelvis brandväggar, krypteringscertifikat samt webb- och e-postservrar. I vissa situationer kan det vara förnuftigt att behålla ett domännamn tills vidare, även om det inte längre är i bruk. Att avstå från ett domännamn ska alltid vara ett medvetet beslut.

1.3	**Domänförvaltning**	Konton för förvaltning av domännamn
Kontrollera regelbundet vilka konton organisationen använder för förvaltning av domännamn, och bedöm om de bör hållas separata eller slås ihop.		

Fi-domännamn registreras i Traficoms domännamnssystem. **Registrarer** kan med sina egna användarkonton använda självbetjäningsportalen i domännamnssystemet. I portalen kan man bland annat registrera och ta kontroll över domännamn, ändra auktoritativa namnservrar för domännamn samt uppdatera kontaktuppgifter för användaren av ett domännamn. Registraren kan under sitt registrarskonto ha flera användarkonton, genom vilka man kan logga in i systemet.

Det är mycket viktigt att registraren regelbundet går igenom användarkontona för domännamnssystemet. Om en arbetstagare exempelvis har övergått till andra uppgifter på sådant sätt att hen fortfarande behöver åtkomst till förmedlarkontot men i en annan roll än tidigare, ska användarkontots rättigheter ändras för att motsvara de nya arbetsuppgifterna.

De större domännamnsförmedlarna använder ofta ett EPP-gränssnitt för domännamnssystem för att förvalta domännamn. EPP ger möjlighet att ansluta registrarens eget system till domännamnssystemet. Därefter kan registraren erbjuda sina kunder ett självbetjäningsgränssnitt för registrering och förvaltning av domännamn. Vid användning av ett EPP-gränssnitt uppdateras ändringar i bästa fall i realtid.

Domännamnsanvändare kan hantera ett eller flera domännamn via ett administratörskonto. En del organisationer har kopplat flera

administratörskonton till ett registrerat domännamn, om domännamnet hanteras av flera avdelningar. Flera administratörskonton ökar den administrativa bördan, och ju fler konton man använder, desto fler är målen för potentiella attacker.

1.4	**Domänförvaltning**	Användarkonton i domännamnsförmedlarnas system
Kontrollera regelbundet vilka systemadministratörer som har rätt att förvalta organisationens domännamn i förmedlarnas system. Säkerställ att användarrättigheterna är uppdaterade.		

Åtkomsten till organisationens användarkonton i domännamnsförmedlarnas system ska begränsas till de personer som verkligen måste ha tillgång till dem. Systemadministratörerna måste vara medvetna om sitt ansvar och sin roll samt känna till riskerna för nätfiske. Om någon lyckas få tag på användaruppgifter från en person som har åtkomst till en registrars system, kan organisationens domännamn bli kapade eller egenmäktiga ändringar göras i namnserverinställningarna.

Om en person slutar arbeta för organisationen eller hens uppgifter förändras, ska personens användarrättigheter genast dras in i enlighet med organisationens processer för förvaltning av användarrättigheter.

1.5	**Domänförvaltning**	Lösenord för användarkonton i registrarers system
Se till att systemadministratörerna använder säkra lösenord i enlighet med organisationens anvisningar. Om registraren erbjuder möjlighet att använda tvåstegsverifiering, rekommenderas detta starkt.		

Inloggningsuppgifter till registrarens system är känsliga uppgifter, och ska behandlas i enlighet med detta.

1.6	**Domänförvaltning**	Kontaktinformation
Se till att kontaktinformationen för alla domännamn samt eventuella faktureringsuppgifter för registraren är uppdaterade.		

Man kan gärna överväga att skapa särskilda e-postadresser för olika befattningar, så att viktig information inte förbises då personer byts ut. Man ska då också se till att de berörda anställda aktivt följer adresserna i fråga. Det är inte alltid lämpligt att använda anställdas privata e-postadresser för att registrera organisationens domännamn.

1.7	**Domänförvaltning**	Återställning
Ta reda på vilka förfaranden registraren har för återställning av kapade domännamn. Säkerställ att den nödvändiga dokumentationen finns sparad.		

Observera att processerna för återställning av kapade domännamn varierar betydligt mellan olika domännamnsregister. I fråga om fi-domännamn ska man kontakta den egna registraren och vid behov Transport- och kommunikationsverket Traficom.

Följande dokument kan i allmänhet vara till nytta för återställning av kapade domännamn:

- utskrift över registreringen av domännamnet
  (WHOIS-sökning eller skärmdump/export av registrarens uppgifter)
- faktura och verifikat över betalning
- korrespondens med registraren om de registrerade domännamnen
- eventuella juridiska dokument där kopplingen mellan organisationen och domännamnet framgår.

1.8	**Domänförvaltning**	Förnyande av domännamn
Håll koll på alla registrerade domännamns giltighetstid och förläng i god tid registreringen för de domännamn som behövs.		

Många registrarer erbjuder möjlighet till automatiskt förnyande av domännamn. Detta minskar risken för att giltighetstiden för domännamnen ska löpa ut. Med tanke på förnyandet av domännamnen måste faktureringsuppgifterna hållas uppdaterade.

Även om domännamnsförmedlarna i allmänhet påminner domännamnsanvändarna när en giltighetstid är på väg att löpa ut, måste organisationen också ha egna processer för att säkerställa förnyandet. Om registreringen av ett domännamn inte förnyas i tid blir den föråldrad, och domännamnet frigörs efter en skyddstid för andras bruk.

1.9	**Domänförvaltning**	Ändringar och granskningar
Om uppgifterna i en registrarens system behöver ändras ska man följa den formella processen för hantering av ändringar. Kontrollera de gällande uppgifterna regelbundet för att säkerställa att inga olovliga ändringar har gjorts i dem.		

För att undvika tråkiga överraskningar bör organisationen vara mycket vaksam när den gör ändringar i registreringar av domännamn. Felaktiga bestämningar kan orsaka problem exempelvis i e-posttrafiken och till och med förhindra åtkomsten till organisationens webbplats. Tilltänkta ändringar ska granskas och godkännas i förväg i enlighet med organisationens process för hantering av ändringar.

1.10	Domänförvaltning	Registrering av nya domännamn
Organisationen ska ha ett formellt förfarande för registrering av nya domännamn, och det ska följas.		

För att organisationen ska ha klarhet om sina domännamn och för att registreringen av nya domännamn ska ske på ett säkert sätt, ska man skapa ett registreringsförfarande och följa det.

Genom förfarandet kan man också säkerställa att de nya domännamnen är godkända, registreras med rätt uppgifter i rätt konton i registrarens system och förvaltas av rätt ansvarspersoner, samt att deras säkerhet garanteras i enlighet med organisationens riktlinjer.

1.11	Domänförvaltning	Spärrmöjligheter i registrarens system och namndatabasen
Skydda domännamnen från obehöriga överföringar, uppdateringar och raderingar med hjälp av de spärrmöjligheter som registraren erbjuder.		

I Traficoms system kan man förhindra ändringar i uppgifterna om domännamn med ett så kallat registerlås (registry lock). Registerlåset måste inaktiveras innan man kan göra ändringar i domännamnets uppgifter. Inaktiveringen kan endast göras med en kod som skickas till på förhand bestämda telefonnummer. Man bör diskutera detaljerna kring aktiveringen och inaktiveringen av registerlåset med den egna registraren.

2 Krav gällande planeringen av namnservrar

Följande avsnitt och de rekommendationer som ges i det riktar sig till datasystemexperter och informationshanteringens tekniska personal. De förutsätter grundläggande kunskaper om DNS-system. Mer information om begreppen och processerna för namnförfrågningar finns i bilaga A och B.

I planeringen av namnservrar ska man följa vissa grundläggande regler oberoende av om organisationen använder en egen namnserver, köper namntjänsten av någon serviceproducent eller använder en kombination av dessa alternativ.

En namnserver som planerats för att vara säker tryggar både tillförlitligheten hos organisationens namnserveruppgifter och systemets användbarhet. En namnserver som förverkligats på ett säkert sätt kan också minska risken för att namnservern utnyttjas i DNS-baserade överbelastningsangrepp samt risken för framgångsrika cache-förgiftningar.

Rekommendationerna gäller primärt namnservrar som används för förfrågningar gällande externa domännamn, men många av principerna gäller också för interna namnservrar.

I bild 1 nedan ges ett exempel på en enkel namnserverlösning för ett fiktivt företag:

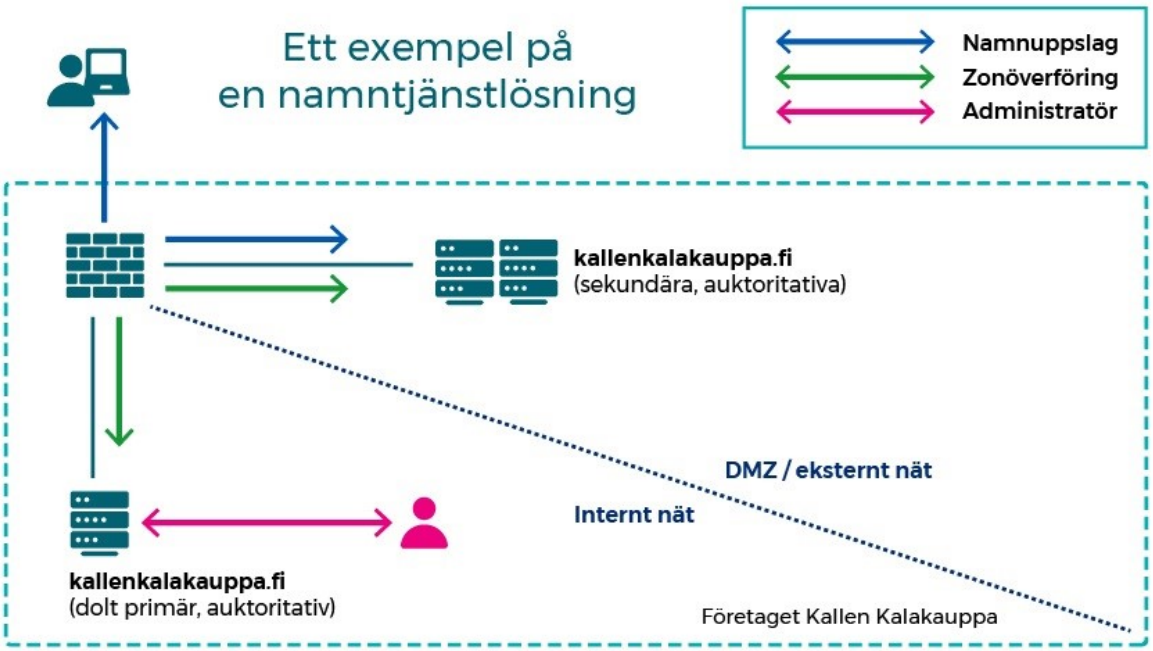


Bild 1: Exempel på lösningar för namnservrar

Bilden visar ett exempel, inte en faktisk rekommendation för namnserverlösningar. Vilken lösning som är bäst för en viss organisation beror bland annat på organisationens storlek, webbhotelltjänsten, resurserna och var användarna av internettjänsterna geografiskt befinner sig.

Traficom ger följande rekommendationer för planering av namntjänster för domännamn som är tillgängliga via internet:

2.1.1	Planering av namnservrar	Särskiljande av namnservrarnas roller
Ställ in de auktoritativa namnservrarna så att de inte godkänner rekursiva förfrågningar		

Auktoritativa namnservrar som är tillgängliga via internet får inte behandla rekursiva förfrågningar. Rekursiva förfrågningar ökar belastningen på servern och kan göra den känslig för DNS-reflektionsattacker och försök till cache-förgiftning. För rekursiva namnförfrågningar ska man använda separata namnservrar, som endast är tillgängliga för interna eller kända kunder.

2.1.2	Planering av namnservrar	Interna och externa domännamn
Information om interna domännamn eller servernamn får inte vara tillgänglig från namnservrar som är tillgängliga utifrån.		

De interna systemens namn och IP-adresser, som inte är avsedda för utomstående, får inte vara tillgängliga i de externa namnservrarnas zoner.

Indelning av de interna resurserna i en eller flera underdomäner gör det möjligt att separera förvaltningen av de interna och externa domännamnen och minskar mängden information om de interna strukturerna som är tillgänglig på internet.

2.1.3	Planering av namnservrar	Redundans i namnservrar
Trygga namntjänstens funktion genom att använda flera externa namnservrar.		

Det kan vara en bra lösning att helt eller delvis låta en extern serviceproducent som är oberoende av de interna strukturerna sköta organisationens externa namnservrar. Tillhandahållarna av namntjänster kan i allmänhet erbjuda effektiva skydd mot överbelastningsangrepp, geografiskt diversifierade lägen för namnservrarna, övervakning dygnet runt samt specialiserade tekniska stödtjänster. En del namntjänster stöder också Anycast, som säkerställer att förfrågningar från kunderna behandlas i ett geografiskt diversifierat nät av namnservrar. Svarstiden för kunden blir då också så kort som möjligt.

Transport- och kommunikationsverket Traficom erbjuder en distribuerad Anycast secondary-namntjänst för fi-domännamn utan kostnad. Mer information om Traficoms Anycast-tjänst: https://www.traficom.fi/sv/anycast-dns-registrarer.

Domännamnsanvändarna får tillgång till Traficoms Anycast-tjänst för sina fi-domännamn via sin egen registrar.

2.1.4	Planering av namnservrar	Namnservrarnas särskilda uppgift
Använd inte externa namnservrar för något annat syfte än för att sköta namntjänster.		

Namnservrar ska inte användas för andra uppgifter, och endast programvara som är nödvändig för produktionen av namntjänsten ska användas i dem. Detta minskar risken för attacker och för att någon sårbarhet i programvaran äventyrar säkerheten i namntjänsten.

2.1.5	Planering av namnservrar	Döljande av den primära namnservern
Använd inte den primära namnservern som den namnserver för externa domännamn som är synlig utåt (s.k. hidden primary). Hindra åtkomst till servern via internet.		

Den primära namnservern innehåller den primära kopian av zonen, och åtkomst till den via internet måste förhindras. Servern ska endast användas för administration av zoner och utbyte av zonuppgifter med sekundära namnservrar som är tillgängliga via internet. Åtkomsten till servrarna ska begränsas till godkända systemadministratörer för namntjänsten. I bild 1 ges ett exempel på en namnserverlösning där den primära namnservern är dold.

2.1.6	Planering av namnservrar	De sekundära namnservrarnas läge
Placera de sekundära namnservrarna i ett separat nätverkssegment, till och från vilket endast behörig trafik tillåts.		

Genom att isolera de namnservrar som är tillgängliga via internet i ett separat nätverkssegment som skyddas av en brandvägg kan man minska risken för att en eventuell äventyrad server fungerar som en språngbräda för manipulation av andra tjänster. Ett möjligt exempel på genomförande visas i bild 1, där de namnservrar som är tillgängliga via internet är isolerade till en DMZ-zon. Namnservrarnas användbarhet måste dock säkerställas genom dubbla strukturer och/eller med hjälp av externa producenter av namntjänster.

2.1.7	Planering av namnservrar	Brandväggsskydd för namnservrar
Skydda namnservrarna med brandväggar, som endast tillåter nödvändig datatrafik.		

Helheten av brandväggsbestämningar utformas utifrån den valda hostingmodellen och organisationens övriga datatekniska strukturer.

I bedömningen av hur nödvändig olika slags trafik mellan kunder, servrar och nätverkssegment är ska man beakta följande faktorer.

- Namnförfrågningar måste kunna tillåtas endast från vissa kunder (interna/externa enligt namnserverns roll) till port 53 genom ett kombinerat TCP och UDP.
- Rekursiva namnservrar som betjänar interna användare måste kunna göra namnförfrågningar från internet till port 53 genom ett kombinerat TCP och UDP.
- Auktoritativa sekundära namnservrar måste kunna ta emot anmälningar från primära namnservrar (notify) samt utbyta zonuppgifter endast med primära namnservrar.
- Datatrafik som riktar sig mot den centraliserade loggtjänsten (SIEM) och är nödvändig för administrationen av servrarna måste begränsas till nödvändiga IP-adresser och portar.
- Det är värt att överväga att ta i bruk granskning av DNS-protokoll, om brandväggen stöder detta. På så sätt kan man säkerställa att endast trafik som uppfyller de officiella DNS-kraven tillåts. Man bör dock vara medveten om att aktivering av DNSSEC kan förutsätta att man godkänner stora DNS-paket samt användning av TCP för att göra och besvara sökningar.

Brandväggsbestämningarna ska testas grundligt innan de tas i bruk.

2.1.8	Planering av namnservrar	Säker datatrafik mellan namnservrar
Säkra zonöverföringar mellan primära och sekundära namnservrar med hjälp av TSIG.		

Om zonuppgifter delas till en sekundär namnserver med hjälp av en zonöverföring från en primär namnserver, ska datatrafiken skyddas med en TSIG-signatur[1]. TSIG säkerställer att zonöverföringen endast kan göras till identifierade sekundära namnservrar och att den egentliga uppdateringen av uppgifter sker på korrekt sätt. Varje namnserverpar måste ha unika TSIG-nycklar, och på TSIG-skyddet ska tillämpas lämpliga strikta brandväggsbestämningar (se ovan). Nycklarna skapas med namnserverprogramvara, som ställs in så att den signerar all datatrafik till och från andra namnservrar.

2.1.9	Planering av namnservrar	Utnyttjande av namnservrar för överbelastningsangrepp
Definiera namnservrarna och nätverkets delområden så att risken för överbelastningsangrepp som baserar sig på DNS-reflektionsangrepp blir så liten som möjligt.		

Namnservrar kan utnyttjas i DNS-reflektionsangrepp, där avsändarens IP-adress förfalskas och man i samband med DNS-förfrågan använder IP-adressen för attackens offer i stället för avsändarens adress. Eftersom de svarspaket som namnservrarna skickar är större än förfrågningarna, kan man med denna metod överbelasta offrets server eller webbresurser. Vid användning av DNSSEC är svarspaketen större än vanligt, eftersom de också innehåller en digital signatur. Detta gör namnservrar som använder DNSSEC särskilt intressanta för angripare som ägnar sig åt överbelastningsangrepp. Risken kan minskas genom följande tilläggsåtgärder:

- förbund mot rekursiva förfrågningar som görs via internet
- Förbud mot AXFR-förfrågningar (zonöverföringar) från andra än auktoritativa namnservrar
- begränsning av antalet förfrågningar som kan göras via samma IP-adress inom en viss tid (*rate limiting*)
- routrar och brandväggar ställs in så att de endast godkänner paket som kommer från godkända IP-adresser i nätverket för skickande av paket (förhindrande av förfalskning av IP-adresser)
- Förbud mot ANY-förfrågningar (alla poster), om namnserverns programvara möjliggör det.

2.1.10	Planering av namnservrar	Versionsuppgifter
Gör bestämningar för namnservrarna så att deras svarsposter inte innehåller programvarans namn eller versionsnummer.		

Om namnservern anger namnet eller versionsnumret för den programvara som driver den kan en angripare enkelt rikta in sig på kända sårbarheter och skräddarsy sitt angrepp för den specifika programvaruversionen. Att dölja namnet och versionsnumret eliminerar inte i sig självt sårbarheterna, men kan tvinga en hackare att göra tilläggsutredningar, som kan upptäckas av organisationens övervakningssystem. Det hör till god praxis att inte publicera onödig information, men det är ännu viktigare att se till att namnservrarna och deras operativsystem alltid hålls uppdaterade (se nedan).

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

2.1.11	Planering av namnservrar	Uppdateringar
Håll alltid namnservrarna och deras operativsystem uppdaterade med de nyaste versionerna		

Genom säkerhetsuppdateringar av både namnserverns programvara och den hostingmiljö som stöder den åtgärdar man upptäckta sårbarheter samt bidrar till att trygga domännamnsuppgifterna och användbarheten hos organisationens namnserver. Om en extern leverantör helt eller delvis ansvarar för namntjänsten ska organisationen säkerställa att säkerhetsuppdateringarna testas och installeras i god tid och enligt förfaranden som är tydligt fastställda och som organisationen godkänt.

2.1.12	Planering av namnservrar	Ändring av bestämningar

Vid ändringar i grundstrukturen för namnserverns bestämningar eller lösningar ska man följa den formella processen för hantering av ändringar.

Alla tilltänkta ändringar i namnserversystemets strukturer eller bestämningar ska kontrolleras och godkännas i förväg i enlighet med organisationens process för hantering av ändringar. Ett systematiskt tillvägagångssätt för hantering av ändringar kan minska risken för oväntade följder och förbättra användbarheten.

2.1.13	Planering av namnservrar	Loggar

För logg över administrationsåtgärder för namnservrarna i enlighet med organisationens logganvisningar. Gå igenom loggarna regelbundet för att upptäcka händelser som tyder på oberättigade åtgärder.

Man måste åtminstone föra logg över avslagna och godkända inloggningsförsök samt förändringar i bestämningar och zoner. En bra logg gör det lättare att lokalisera fel och åtgärda säkerhetsavvikelser.

2.1.14	Planering av namnservrar	Döljande av den primära namnservern

Gå igenom zonerna regelbundet för att säkerställa att posterna ser ut som de ska och att inga obehöriga ändringar har gjorts i dem.

Posterna ska granskas regelbundet för att säkerställa att de är korrekta och har rätt innehåll. Poster som inte används eller som hänvisar till någon annan IP-adress än det registrerade objektets ska tas bort. Om man upptäcker tecken på olovliga ändringar ska man omedelbart kontakta dataskyddsombudet

2.1.15	Planering av namnservrar	Användning av DNSSEC
Använd i mån av möjlighet DNSSEC för alla externa domännamn som är i bruk.		

DNSSEC förhindrar förfalskning av svar på namnförfrågningar och säkerställer att svaret kommer från en identifierad namnserver.

Även om användaren inte skulle använda domännamnet aktivt, kan svar på förfrågningar förfalskas utan DNSSEC-tillägg. Den som gör en förfrågan kan då hamna på en webbplats för nätfiske som kontrolleras av en utomstående aktör. I fråga om fi-domännamn bör man helt ta bort namnservrarna för onödiga domännamn. Det är inte nödvändigt att ha en namnserver för ett fi-domännamn.

2.2 Rekommendationer gällande DNSSEC

Eftersom DNS är en central faktor för lokalisering av tjänster på internet, kan angripare vara intresserade av att förfalska svar på namntjänstförfrågningar genom man in the middle-attacker eller cache-förgiftningar. Om attacken lyckas kan användaren exempelvis dirigeras till en annan sida än den egentliga målsidan, och kan fås att avslöja sina inloggningsuppgifter eller andra känsliga uppgifter. Sådana här attacker riktar sig i allmänhet mot externa domännamn på internet.

DNSSEC (*domain name system security extensions*) är ett tillägg till DNS-standarden, som med hjälp av krypteringsmetoder säkerställer att den som gör en förfrågan kan lita på att

- svaret på namnförfrågan kommer från rätt namnserver
- svaret inte förvrängs på vägen
- ett svar som säger att det efterfrågade namnet inte finns stämmer.

Man bör observera att DNSSEC inte krypterar egentlig DNS-trafik. Kryptering av DNS-trafik, exempelvis med hjälp av *DNS over TLS*- eller *DNS over HTTPS*-teknik, tas inte upp i dessa anvisningar.

DNSSEC-valideringsförfarande

En namnförfrågningsprocess för ett domännamn som skyddas av DNSSEC är till stor del likadan som en vanlig förfrågningsprocess (se bilaga B: Namnförfrågningsprocess), men innehåller både kryptografisk validering av enskilda svar och kontroll av de deltagande namnservrarnas hierarkiska ställning.

Validering av svar

För validering av svar på en namnförfrågan används följande poster:

- **RRset (resource record set):**
  Gruppering av alla resursposter av en viss typ (t.ex. A- eller MX-poster)
- **RRSIG (resource record signature):**
  Hashvärde (*hash value*) för signerat RRset utifrån enskilda ZSK-nycklar
- **ZSK (zone signing key):**
  Offentlig krypteringsnyckel för validering av zonens RRSIG:er
- **DNSKEY:**
  En typ av post som används för att lagra offentliga krypteringsnycklar.

Validering av svaren i DNSSEC-signerade zoner beskrivs i bild 2 nedan.

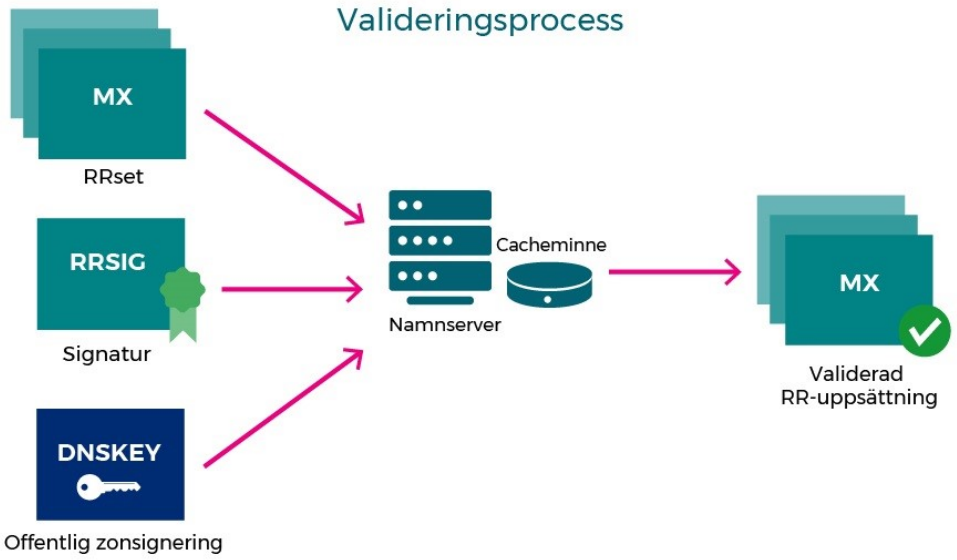


Bild 2: Valideringsprocess för resurspost (MX-post som exempel)

Med hjälp av en offentlig ZSK-nyckel, det vill säga zonens signaturnyckel, kan den namnserver som behandlar förfrågan validera signaturen (RRSIG) för en uppsättning information (RRset) som ingår i en post. På detta sätt säkerställer man att man upptäcker falska svar.

Validering av svarande servrar

För att man ska kunna konstatera att ett validerat svar kommer från rätt namnserver, som har behörighet att svara för domännamnets räkning, måste den offentliga ZSK-nyckel (blå) som används i ovan beskrivna process kunna valideras. För detta används följande poster:

- **KSK (key signing key):**
  Offentlig krypteringsnyckel för verifiering av RRSIG-signaturer av en RRset-datauppsättning i DNSKEY, exempelvis en ZSK-nyckel.
- **DS (delegation signer):**
  Hashvärde för en offentlig KSK-nyckel, som lagras i den zon som ansvarar för delegering av domännamn (*parent zone*).

Processen liknar den som beskrivs ovan, men är kedjad som en ”förtroendekedja” (*chain of trust*) via TLD till DNS-systemets rot (se bild 3). En offentlig ZSK-nyckel valideras med en offentlig KSK-nyckel, vars hashvärde finns lagrat i en DS-post i zonen på toppnivån (*parent zone*).

DS-poster för .fi-domännamn finns lagrade i Traficoms domännamnssystem. Registrets egen KSK-nyckel finns som hashvärde vid hierarkins rot[2]. På så sätt kan man genom hela zonhierarkin kryptografiskt säkerställa att signerade svar på namnförfrågningar endast ges av befullmäktigade namnservrar. Processen beskrivs i bild 3 nedan.

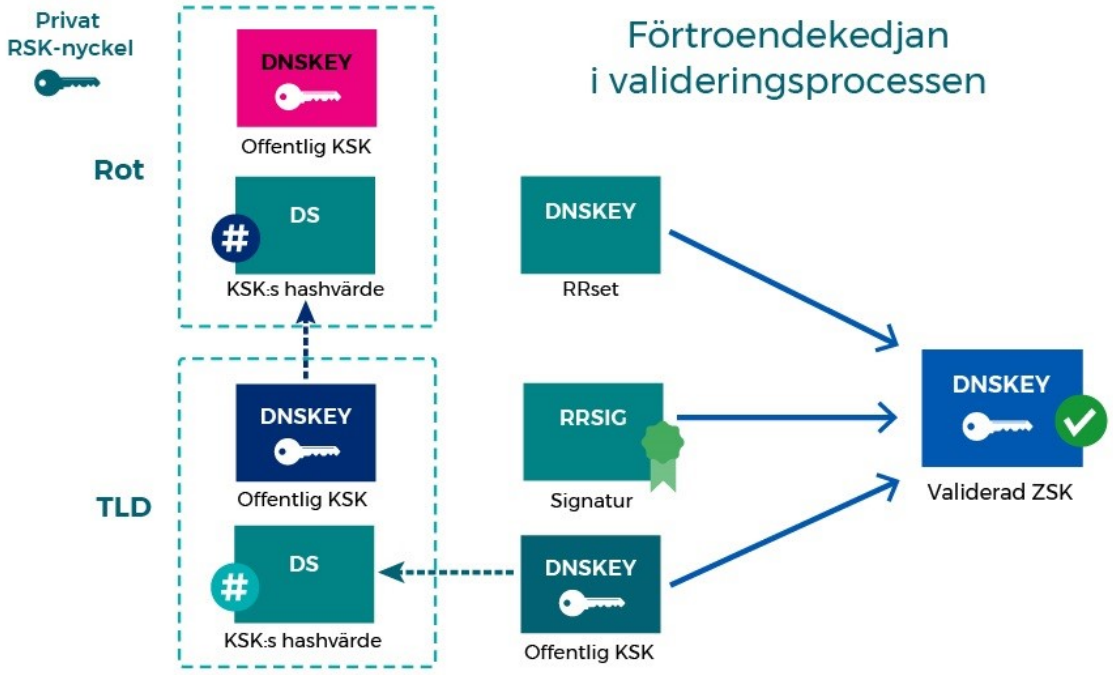


Bild 3: Allmän beskrivning av DNSSEC-valideringsförfarandet

Även om valideringsförfarandet kan verka komplicerat är det i allmänhet enkelt att ta i bruk DNSSEC för organisationens domännamn. Det kan tas i bruk via namntjänstleverantören (som ofta är densamma som registraren), eller så kan det aktiveras av organisationens egen systemadministratör för namnservrar. Det är dock mycket viktigt att administratören av namnservrarna planerar nyckelhanteringsprocesserna med noggrannhet.

Oberoende av om man använder DNSSEC för organisationens externa domännamn ger Traficom följande rekommendationer:

2.2.1	Planering av namnservrar	Användning av DNSSEC
Använd i mån av möjlighet DNSSEC för alla externa domännamn som är i bruk.		

2 De offentliga KSK- och ZSK-nycklarna för domännamnen på hierarkins toppnivå (rotdomän eller rotzon) signeras med en privat *root signing key*-nyckel i ett komplicerat förfarande, som upprepas fyra gånger per år. Målet är att bevara rotnycklarnas tillförlitlighet.

För att organisationens egna användare ska kunna skyddas från svar som är förfalskade eller skickas av obehöriga namnservrar, ska de namnservrar som sköter namnförfrågningar för organisationens användare ställas in så att svar som gäller domännamn som använder DNSSEC valideras. Om svaret inte går igenom DNSSEC-valideringen kan det vara ett tecken på att svaren manipulerats, men orsaken kan också vara ett fel i bestämningarna i en zon som signerats med DNSSEC.

I felsökningen kan följande verktyg vara till hjälp:

https://dnssecdebugger.verisignlabs.com/

https://dnsviz.net/

Rekommendationer gällande ibruktagande och användning av DNSSEC

2.2.2	DNSSEC	Ibruktagande av **DNSSEC för alla auktoritativa namnservrar**
Alla namnservrar måste stödja DNSSEC		

Om alla namnservrar i en zon som signerats med DNSSEC inte stöder DNSSEC, kan valideringen misslyckas vilket kan leda till problem med användningen.

2.2.3	DNSSEC	**Förnyelse av signaturer**
Förnya signaturerna automatiskt i god tid innan deras giltighetstid löper ut		

Om en zon inte använder DNSSEC uppdateras den i regel endast när poster ändras, raderas eller skapas. Vid användning av DNSSEC bör man notera att signaturerna endast är i kraft en viss tid, och de måste förnyas i god tid innan giltighetstiden löper ut. Man ska också beakta att det kan finnas poster som baserar sig på gamla signaturer i cacheminnet, och validering av dem lyckas tills de tas bort ur cacheminnet (*time to live* dvs. TTL, livstiden, tar slut). Om giltighetstiden för en aktiv signatur löper ut leder det till att de kunder som validerats av DNSSEC-signaturen inte kan använda resursen. Förnyelsen av signaturer sker i de flesta fall automatiskt, men man måste övervaka att processen fungerar.

2.2.4	DNSSEC	Svar på förfrågningar om obefintliga domännamn

Använd NSEC3 för besvarande av förfrågningar som gäller obefintliga domännamn. NSEC3 förhindrar ”zone walking”, vilket innebär att det inte blir möjligt att ta reda på hela zonens innehåll.

Precis som svar på förfrågningar om existerande domännamn måste även svar gällande obefintliga domännamn kunna verifieras med DNSSEC. NSEC3 lämpar sig för detta syfte: det kan länka ihop alla domännamn i zonen och visa att domännamn som saknas i kedjan inte finns. För att man inte ska kunna söka efter poster som innehåller hela verkliga namn i zonen genom att gå igenom kedjan från början till slut, visar NSEC3 koncentrerade namn i krypterad form i stället för läsbar text.

2.2.5	DNSSEC	Byte av nycklar
Förnya KSK- och ZSK-signaturnycklarna regelbundet och automatiskt samt alltid när deras säkerhet misstänks ha äventyrats.		

KSK- och ZSK-nycklar har begränsad giltighetstid. De måste också förnyas regelbundet för att deras säkerhet inte ska äventyras. I de flesta namnserverlösningar är det möjligt att automatisera processen. Observera dock att förnyelsen av KSK-nycklar kan förutsätta utbyte av uppdaterade DS-poster med zonen på toppnivån (*parent zone*). I fall med fi-domännamn handlar det i praktiken om att nya DS-poster ska uppdateras i fi-roten.

I processen måste man alltid beakta giltighetstiden för signaturer som skapats tidigare, uppgifternas livstid (TTL) i cacheminnet samt replikering av DNS-poster i DNS-systemet.

2.2.6	DNSSEC	Skapande och lagring av KSK-nycklar
Skapa och lagra KSK-signaturnycklar i en trygg miljö		

ZSK-nycklar för DNSSEC-säkrade zoner baserar sig på KSK-nycklar, och KSK-nycklarna måste därför skapas och lagras i en trygg miljö. Om organisationen har höga säkerhetskrav eller behov av kryptering, bör man överväga att använda en HSM-säkerhetsmodul (*hardware security module*) för att skapa och lagra krypterings- och signaturnycklar.

2.2.7	DNSSEC	Nyckel- och hashalgoritmer
Använd endast algoritmer som allmänt betraktas som säkra		

Den överlägset vanligaste algoritmen för kryptering av DNSSEC-signerade .fi-zoner är RSA/SHA-256 (8). Algoritm 8 betraktas allmänt som säker.

Däremot ska algoritmerna 5 (RSA/SHA-1), 6 (DSA-NSEC3-SHA1) eller 7 (RSASHA1-NSEC3-SHA1) INTE användas.

Nycklar och signaturer som baserar sig på ECDSA (för fi-domännamn kan man använda algoritm 13 ECDSAP256SHA256) är mycket kortare än RSA-baserade nycklar och signaturer, och tar därför mindre plats i zoner och namnsökningar. Det går snabbare att signera med dem, men valideringen går långsammare.

Om man vill betona säkerhet och snabbhet i ett annat slags förhållande, kan man även överväga algoritmerna 8 (RSA/SHA-256) och 10 (RSA/SHA-512). Till skillnad från vad man kan tro är algoritm 10 i praktiken inte säkrare än algoritm 8. Det finns dock inte några praktiska hinder för att använda algoritm 10.

De nyaste DNSSEC-algoritmerna är algoritm 15 (Ed25519) och 16 (Ed448). Algoritmerna är ännu ganska nya, och alla resolvernamnservrar stöder inte ännu algoritmerna 15 och 16. För fi-domännamn är stöd för algoritm 15 på väg, men inte ännu möjligt att använda.

Oberoende av vilken algoritm som används är DNSSEC-signerade svar ofta så stora att de måste skickas över en TCP-förbindelse. Som tidigare nämnts är det därför viktigt att alltid tillåta DNS-förfrågningar via TCP.

2.2.8	DNSSEC	Stödjande av DNSSEC-trafik på internet
Säkerställ att den nätverkslösning som namntjänsten använder stöder DNSSEC-dataöverföring.		

Eftersom namnförfrågningar är större än vanligt i DNSSEC-signerade zoner, måste man säkerställa att nätverkets sammansättning och brandväggarna stöder dem. Man måste testa detta innan DNSSEC tas i bruk, så att tjänsternas användbarhet inte äventyras. EDNS0 är exempelvis i de flesta fall inte längre något problem för brandväggar och nätverksutrustning, men det är ändå bra att beakta saken.

3 Andra nyttiga åtgärder

De tekniska lösningar som nämns nedan behandlas inte i dessa anvisningar, men de bör beaktas som möjliga användbara tilläggsåtgärder som kan främja skyddet av organisationens infrastruktur och kommunikation:

- DANE: DNS-based Authentication of Named Entities
  En metod som motsvarar DNSSEC och lämpar sig för följande uppgifter:
  - uttrycka vilken certifikatutfärdare som domännamnets ägare tillåter att bevilja certifikat för domännamnets resurser,
  - uttrycka godkända krypteringscertifikat som används av ett domännamns resurser
  - meddela avsändare av e-postmeddelanden om att de måste kryptera meddelandetrafik till domännamnets e-postserver.
- SPF: sender policy framework
  DKIM: domain keys identified mail

  DMARC: domain-based message authentication, reporting and conformance DNS-baserade åtgärder som kan förhindra att förfalskade e-postmeddelanden levereras till mottagaren.

4 Källhänvisningar

Transport- och kommunikationsverket tackar det danska cybersäkerhetscentret *Center for Cybersikkerhed* för källmaterialet

Tips gällande innehållet har fåtts exempelvis från följande källor:

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://tools.ietf.org/html/rfc6781

5 Bilaga 1: Begrepp

Nedan presenteras ett antal begrepp med definitioner samt en beskrivning av namnförfrågningsprocessen som bakgrund till rekommendationerna i dessa anvisningar.

- DNS (domain name system): Ett system och ett nätverksprotokoll vars primära syfte är att underlätta konvertering av namn till IP-adresser på internet. Namnsystemet har en hierarkisk struktur och administreras via ett distribuerat nätverk av namnservrar.
- Top-level domain (TLD): Domännamn på den högsta nivån i namnhierarkin. Toppdomänerna kan vara generiska (gTLD), såsom .com, .org och .edu, eller nationella (ccTLD), såsom .fi eller .se.
- Namndatabas: Databas över alla domännamn i en viss TLD-domän samt deras innehavare och auktoritativa namnservrar. Traficom upprätthåller en namndatabas över finländska domännamn som slutar på .fi.
- Registrar: En förmedlare som erbjuder en tjänst för registrering av domännamn. Många registrarer erbjuder också webbplatsutrymme och namnservertjänster, men dessa är inte obligatoriska delar av registrarens uppgifter.
- Användare av domännamn: En person eller organisation som har rätt att använda ett visst domännamn.
- Befullmäktigad: En person eller organisation som har fått fullmakt av innehavaren av ett domännamn att utföra åtgärder som berör domännamnet.
- Namnserver: En server eller tjänst som översätter namn på IP-adresser med hjälp av ett DNS-protokoll.
    - Rekursiv namnserver: En namnserver som hjälper till att hitta svar på namntjänstförfrågningar från kunddatorer genom att kontrollera om namnet redan finns i cacheminnet. Om så inte är fallet skickar servern förfrågningar till nödvändiga namnservrar, tills den får ett auktoritativt svar.
    - Auktoritativ namnserver: En namnserver som har beviljats ett auktoritativt ansvar för vissa zoner.
- Zon: Zonen omfattar alla uppgifter om det domännamn som namnservern har auktoritativt ansvar för. Om domännamnet inte har underdomäner som hanteras av andra namnservrar, kan en zon vara detsamma som ett domännamn. Om domännamnet har en eller flera underdomäner som hanteras av andra namnservrar, har domännamnet flera zoner.
- Resource record (RR): Zonens RR- dvs. resurspost, som i allmänhet innehåller ett visst namn, en typ och ett värde. Exempel på en resurspost av A-typ för zonen kallenkalakauppa.fi:
    - www A 193.163.102.58 – adress/värdpost (A), som returnerar IP-adressen 193.163.102.58 vid sökning på namnet www.kallenkalakauppa.fi.

6 Bilaga 2: DNS-förfrågningsprocess

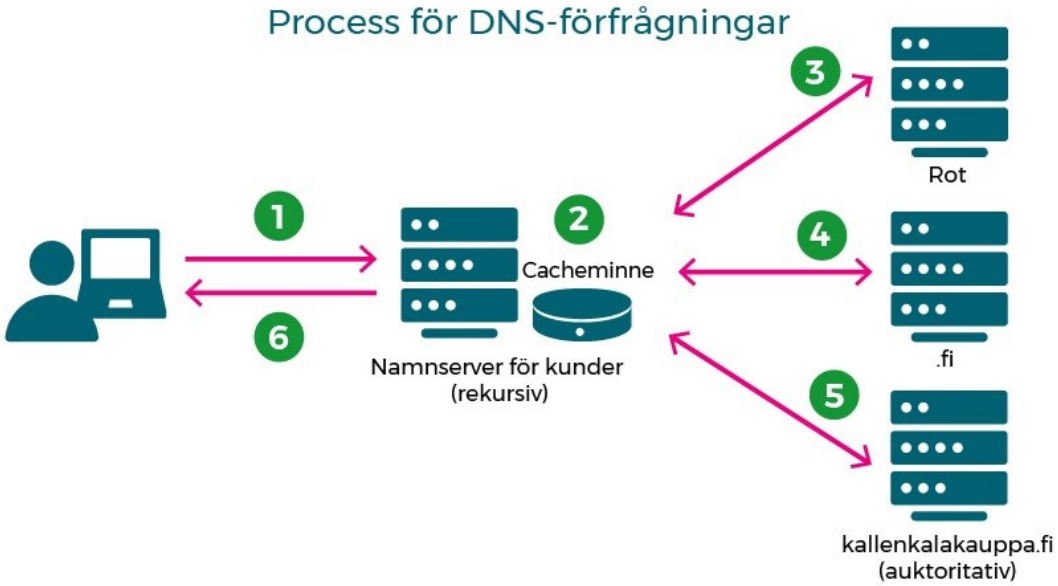


Bild 4: DNS-förfrågningsprocess

1. När kunden vill besöka en webbplats som heter www.kallenkalakauppa.fi, skickas förfrågan först till den namnserver som datorn har ställts in att använda. Hos ett företag är detta i allmänhet en namnserver i företagets eget nätverk. I hushåll används i allmänhet internetleverantörens namnserver.
2. Namnservern söker information i cacheminnet om huruvida svaret på förfrågan redan har identifierats utifrån tidigare förfrågningar.
   Om svaret hittas i namnserverns cacheminne meddelas det till kunden, och processen avslutas här.
3. Om svaret inte är känt och namnservern inte vet vilka namnservrar som ansvarar för domännamnet kallenkalakauppa.fi eller toppdomänen .fi, frågar den några namnservrar vid root-hierarkins rot som den känner till vilka namnservrar som ansvarar för .fi-domännamn.
   Om det är känt vilka webbservrar som ansvarar för domännamnet kallenkalakauppa.fi, går man direkt till steg 5. Om det är känt vilka webbservrar som ansvarar för .fi-domännamn, går man direkt till steg 4.
4. Därefter frågar namnservern några av de .fi-namnservrar den fått kännedom om vilka namnservrar som ansvarar för domännamnet kallenkalakauppa.fi.
5. Namnservern skickar sedan en förfrågan till någon av de namnservrar för kallenkalakauppa.fi som den fått kännedom om och får IP-adressen för domännamnet www.kallenkalakauppa.fi som svar.
6. Svaret skickas till kunden och sparas i namnserverns cacheminne för en viss tid. Tack vare detta kan förfrågningar som gäller samma

domännamn eller någon av de namnservrar som ingick i kedjan besvaras utan att man behöver gå igenom hela processen från början till slut.

Kundens namnserver framför för kundens räkning en rekursiv förfrågan (punkt 3–5) och säkerställer att den får ett svar, även om det kräver förfrågningar till flera namnservrar.

Den organisation som sköter ett visst domännamns auktoritativa namntjänst (i detta fall det fiktiva företaget Esimerkki Oy, vars domännamn är kallenkalakauppa.fi) ansvarar för att skicka information om domännamnets alla namn till rekursiva namnservrar som framför förfrågningar.

Transport- och kommunikationsverket Traficom

PB 320, 00059 TRAFICOM
tfn 029 534 5000

traficom.fi

Liikenne- ja viestintävirasto