TRAFICOM
Liikenne- ja viestintävirasto

Verkkotunnusten turvallinen hallinta

Opas verkkotunnusvälittäjille ja verkkotunnusten käyttäjille

Fi-verkkotunnustiimi

Sisällysluettelo

JOHDANTO **3**
TAUSTAA **4**
LUKUOHJE **5**
1 VERKKOTUNNUSTEN HALLINNOINTIA KOSKEVAT SUOSITUKSET **6**
2 NIMIPALVELINTEN SUUNNITTELUA KOSKEVAT VAATIMUKSET **12**
2.2 DNSSECIÄ KOSKEVAT SUOSITUKSET 21
3 MUITA HYÖDYLLISIÄ TOIMENPITEITÄ **31**
4 LÄHDEVIITTEET **31**
5 LIITE 1: KÄSITTEITÄ **32**
6 LIITE 2: DNS KYSELYPROSESSI **33**
Kuva 4: DNS Kyselyprosessi *33*

Johdanto

Jos organisaation verkkotunnus päätyy vahingollisen toimijan haltuun, pääsy organisaation verkkosivuille voi estyä, sähköpostiliikenne pysähtyä, VPN-liikenne ohjautua toisaalle sekä salausvarmenteita, kirjautumistietoja ja muita tärkeitä tietoja päätyä tunkeilijan haltuun. Tapahtumalla voi olla laajojakin taloudellisia tai poliittisia seurauksia.

Tässä julkaisussa esitetään suosituksia, joiden avulla organisaatiot voivat pitää verkkotunnuksensa turvassa. Suositukset voivat auttaa organisaatioita vähentämään kielteisten imagovaikutusten riskiä internetissä, parantamaan järjestelmien käytettävyyttä ja luotettavuutta sekä lisäämään viestinnän uskottavuutta ja turvallisuutta.

Organisaation identiteetti kytkeytyy internetissä voimakkaasti verkkotunnuksen nimeen. Organisaation kanssa käytävä vuorovaikutus aina verkkosivuilla käymisestä sähköpostiviestien lähettämiseen on riippuvaista siitä, että sen verkkotunnus on löydettävissä. Siksi jokaisen organisaation on pystyttävä pitämään verkkotunnuksensa turvassa.

Ohje on tarkoitettu ensisijaisesti organisaatioiden tietohallinnon johtajille sekä tekniselle henkilöstölle. Suositusten toivotaan tukevan organisaatioita olemassa olevien käytäntöjen kehittämistyössä sekä sen varmistamisessa, ettei verkkotunnusten käsittelystä aiheudu tarpeettomia organisaatioon kohdistuvia riskejä.

Yleisiä suosituksia

Seuraavassa esitellään yleisiä suosituksia ja hyviä käytäntöjä, jotka koskevat verkkotunnusten turvallista hallintaa. Suositukset voivat auttaa organisaatioita verkkotunnusten hallussapitoon liittyvien riskien hallinnassa.

Yleiset suositukset ja alla mainitut periaatteet ovat esimerkkejä, eivät tyhjentävä luettelo:

- Organisaatiolla on oltava selko kaikista verkkotunnuksistaan.
- Verkkotunnusten rekisteröintitietojen muuttamisen on oltava suojattu tunnistautumisella.
- Verkkotunnusten rekisteröintitietojen muuttamisessa noudatetaan aina vakiomenettelyä.
- Verkkotunnusten rekisteröintitiedot on tarkistettava säännöllisesti.
- Nimipalvelin on toteutettava siten, että se suojaa organisaation verkkotunnuksia ja varmistaa niiden käytettävyyden.
- Kaikki verkkotunnukset on syytä suojata DNSSEC-laajennuksella.
- Nimikyselyt on syytä varmentaa DNSSECillä.

Taustaa

Nimipalvelujärjestelmä domain name system (DNS) otettiin käyttöön 1980-luvun alussa. Tavoitteena oli luoda tehokas ja luotettava, hajautettu nimipalvelukyselyjärjestelmä, joka pystyisi käsittelemään kasvavan tietokoneverkoston esittämät pyynnöt.

Verkostosta kehittyi nykypäivänä tuttu maailmanlaajuinen internet. Internetin lukemattomien palveluiden toimivuuden edellytys on edelleenkin toimiva DNS-järjestelmä, mutta valitettavasti sen syntyvaiheessa ei juuri kiinnitetty huomiota turvallisuuteen. Siksi joudumme nykyisin kohtaamaan monenlaisia verkkotunnuksiin ja niiden hallinnointiin liittyviä riskejä.

Traficom on havainnut nimitietokantoihin, verkkotunnusten käyttäjiin ja nimipalveluihin kohdistuvien hyökkäysten lisääntyneen viime vuosina (ks. käsitteiden määritelmät liitteestä A: Käsitteitä)

Esimerkkejä hyökkäysyritysten tyypeistä

- Nimitietokantoihin ja verkkotunnusvälittäjien tietoihin tunkeutuminen
- Välittäjien ylläpitämille verkkotunnusten hallintatileille tunkeutuminen
- Nimipalvelinten tai -tietokantojen DNS-kaappaus
- Nimipalvelinten hyväksikäyttö palvelunestohyökkäyksissä
- Väliintulo- eli *man in the middle* -hyökkäys ja välimuistin myrkytys
- Kotireitittimien ja -tietokoneiden DNS-asetusten peukalointi

Palvelunestohyökkäys: Hajautettu ylikuormitushyökkäys, jonka englanninkielinen nimi on *distributed denial of service* (DDoS). Hakkerit käyttävät haltuunsa ottamiaan tietokoneita ja synnyttävät tietylle kotisivulle (verkkopalvelimelle) tai tiettyyn verkkoon epätavallisen paljon liikennettä. Sen seurauksena sivusto tai verkko kaatuu eikä ole todellisten käyttäjien saatavilla hyökkäyksen aikana.

Man in the middle: Väliintulohyökkäyksenä tunnettu hyökkäystyyppi, jossa kolmas osapuoli nappaa kahden osapuolen välillä kulkevia tietoja ja mahdollisesti myös muokkaa niitä.

Välimuistin myrkytys: DNS-palveluun liittyvä hyökkäys (eng. *cache poisoning*), jossa DNS-palvelimen välimuistiin istutetaan virheellisiä vastauksia liikenteen ohjaamiseksi tahallisesti väärään osoitteeseen.

Lukuohje

Ohje jakautuu kahteen pääosioon, joilla molemmilla on oma kohderyhmänsä. Osioissa on ryhmiteltyjä suosituksia, jotka voivat auttaa organisaatioita vähentämään edellä kuvattuihin hyökkäystyyppeihin liittyviä riskejä.

1. Verkkotunnusten hallinnointia koskevia suosituksia Kohderyhmä: tietohallinnon johto

Osion suositukset voivat auttaa tietohallinnon johtoa verkkotunnusten turvallisessa hallinnoinnissa sekä tunnusten vaarantamiseen ja DNS-kaappauksiin liittyvien yritysten torjunnassa (kohdat 2 ja 3).

2.1 Nimipalvelinten suunnittelua koskevat suositukset ja 2.2 DNSSECiä koskevat suositukset

Kohderyhmä: Tietojärjestelmäasiantuntijat ja tietohallinnon tekninen henkilöstö

Osion suositukset voivat auttaa järjestelmäasiantuntijoita ja tietohallinnon teknistä henkilöstöä suunnittelemaan ja ylläpitämään turvallisia nimipalvelimia. Toimenpiteillä voidaan vähentää DNS-kaappausten riskiä, ehkäistä nimipalvelinten hyväksikäyttöä DDoS-hyökkäyksissä ja antaa suojaa DNS-järjestelmään liittyviltä väliintulohyökkäyksillä.

Ohjeessa ei käsitellä nimitietokantoihin (whois-palvelut, OData), verkkotunnusvälittäjiin kohdistuvia hyökkäyksiä eikä kotireititinten tai -tietokoneiden DNS-määritysten peukalointiyrityksiä.

1 Verkkotunnusten hallinnointia koskevat suositukset

Vaikka verkkotunnukset ovat organisaation internetnäkyvyyden kannalta aivan keskeinen tekijä, ne jätetään usein oman onnensa nojaan sen jälkeen, kun ne on rekisteröinnin yhteydessä määritetty. Traficom suosittelee organisaatioille järjestelmällistä verkkotunnusten hallinnointia sekä käyttäjätilien ja verkkotunnusrekisteröintien aktiivista valvontaa ja ylläpitämistä.

Organisaation verkkotunnusten turvallinen hallinta voi ehkäistä organisaation järjestelmien käytettävyyteen kohdistuvia ulkopuolisia vaikuttamisyrityksiä, kuten verkkotunnusten haltijoiden käyttäjätilien peukalointia ja DNS-kaappauksia.

1.1	**Verkkotunnusten hallinnointi**	Yhteenveto verkkotunnuksista
Dokumentoi organisaation hallussa olevat verkkotunnukset ja käytetyt verkkotunnusvälittäjät.		

Jos verkkotunnuksia on rekisteröity eri verkkotunnusvälittäjien kautta, kannattaa harkita niiden keskittämistä yhdelle välittäjälle hallinnoinnin sekä tunnusten käytön valvonnan helpottamiseksi.

Verkkotunnusvälittäjiä arvioitaessa on kiinnitettävä huomiota myös välittäjien tarjoamiin turvatoimiin, kuten kaksivaiheisen kirjautumisen mahdollisuuksiin itsepalvelukäyttöliittymän käyttäjätileille kirjauduttaessa.

1.2	**Verkkotunnusten hallinnointi**	Verkkotunnusten ylläpito
Käy luettelo verkkotunnuksista säännöllisesti läpi ja arvioi tarvetta säilyttää kukin verkkotunnus tai luopua siitä.		

Verkkotunnuksen rekisteröiminen on helppoa ja edullista, mutta tunnuksia on hallinnoitava ja niiden turvallisuutta on valvottava. Jos verkkotunnusta ei enää käytetä, kannattaa harkita siitä luopumista niin hallinnollisen taakan kuin hyökkäyksille alttiin pinnan pienentämiseksi organisaatiossa. Fi-verkkotunnuksen voi rekisteröidä myös ilman nimipalvelimia.

Ilman nimipalvelimia rekisteröinti on suositeltavaa, jos verkkotunnuksen haluaa pitää niin sanotusti "parkissa", odottamassa käyttöä tulevaisuudessa.

Jos verkkotunnuksella on ollut tiivis yhteys organisaation identiteettiin tai brändiin, kannattaa harkita sen rekisteröinnin jatkamista siirtymäkauden ajaksi, jotta verkkotunnuksen päätyminen muiden haltuun voidaan estää. Lokeja tarkastelemalla näkee, suuntautuuko vanhaan sivustoon yhä liikennettä.

Verkkotunnuksesta luopumisessa on noudatettava määrämuotoista prosessia, jolla varmistetaan, että kaikki viittaukset verkkotunnukseen esimerkiksi palomuureista, salausvarmenteista sekä verkko- ja sähköpostipalvelimilta poistetaan. Joissain tilanteissa voi olla järkevää pitää verkkotunnus toistaiseksi, vaikka se ei olisikaan enää käytössä. Verkkotunnuksesta luopumisen tulee aina olla tietoinen päätös.

1.3	**Verkkotunnusten hallinnointi**	Verkkotunnusten hallintatilit
Tarkista säännöllisesti, mitä verkkotunnusten hallintatilejä organisaatiossa käytetään verkkotunnusten hallintaan, ja arvioi, kannattaako tilit pitää erillisinä vai yhdistää.		

Fi-verkkotunnukset rekisteröidään Traficomin ylläpitämässä verkkotunnusjärjestelmässä. **Verkkotunnusvälittäjä** pääsee omalla käyttäjätilillään käyttämään Verkkotunnusjärjestelmässä olevaa itsepalveluportaalia. Portaalissa voi muun muassa rekisteröidä ja ottaa hallintaansa verkkotunnuksia, muuttaa verkkotunnuksen autoritäärisiä nimipalvelimia ja päivittää verkkotunnuksen käyttäjän yhteystietoja. Verkkotunnusvälittäjällä voi välittäjätilinsä alla olla useita käyttäjätilejä, joilla järjestelmään pääsee kirjautumaan.

On erittäin tärkeää, että verkkotunnusvälittäjä käy verkkotunnusjärjestelmän käyttäjätilit läpi säännöllisesti. Jos työntekijä on siirtynyt esimerkiksi toisiin tehtäviin siten että tarvitsee edelleen pääsyn välittäjätilille mutta rooli eroaa aiemmasta, tulee käyttäjätilin käyttöoikeudet muokata vastaamaan uutta työnkuvaa.

Tyypillisesti isommat verkkotunnusvälittäjät käyttävät verkkotunnusten hallinnointiin verkkotunnusjärjestelmän EPP-rajapintaa. EPP mahdollistaa verkkotunnusvälittäjän oman järjestelmän liittämisen verkkotunnusjärjestelmään. Tämän jälkeen välittäjä voi tarjota asiakkailleen itsepalvelukäyttöliittymän verkkotunnusten rekisteröintiä ja hallinnointia varten. EPP rajapintaa käytettäessä muutokset päivittyvät parhaimmillaan reaaliaikaisesti

Verkkotunnuksen käyttäjä Hallintatilin kautta voidaan hallinnoida yhtä tai useaa verkkotunnusta. Jotkin organisaatiot ovat liittäneet rekisteröityyn verkkotunnukseensa useita hallintatilejä, jos niitä hallinnoidaan eri osastoilla. Useiden hallintatilien olemassaolo lisää hallinnollista taakkaa, ja mitä useampia tilejä on käytössä, sitä enemmän on vaaralle alttiita mahdollisten hyökkäysten kohteita.

1.4	**Verkkotunnusten hallinnointi**	Käyttäjätilit verkkotunnusvälittäjien järjestelmissä
Tarkista säännöllisesti, keillä järjestelmänvalvojilla on oikeus ylläpitää organisaation verkkotunnuksia niiden välittäjien järjestelmissä. Varmista, että käyttöoikeudet ovat ajan tasalla.		

Pääsy organisaation käyttäjätileille verkkotunnusvälittäjien järjestelmissä on rajattava niille henkilöille, joiden todella on päästävä niihin käsiksi. Järjestelmänvalvojien on oltava tietoisia vastuustaan ja roolistaan sekä tunnettava tietojen kalasteluyrityksiin liittyvät riskit. Jos urkkija onnistuu kalastelemaan käyttäjätiedot henkilöltä, jolla on pääsy verkkotunnusvälittäjän järjestelmään, organisaation verkkotunnukset voidaan kaapata tai mahdollisesti tehdä mielivaltaisia muutoksia nimipalvelinmäärityksiin.

Jos henkilö poistuu organisaation palveluksesta tai hänen toimenkuvansa muuttuu, hänen käyttöoikeutensa on poistettava välittömästi organisaation käyttöoikeuksien hallintaprosessin mukaisesti.

1.5	**Verkkotunnusten hallinnointi**	Salasanat käyttäjätileille verkkotunnusvälittäjien järjestelmissä
Varmista, että järjestelmänvalvojat käyttävät organisaation ohjeistuksen mukaisia turvallisia salasanoja. Jos verkkotunnusvälittäjä tarjoa mahdollisuuden käyttää kaksivaiheista kirjautumista, on sen käyttö hyvin suositeltavaa.		

Käyttäjätunnukset verkkotunnusvälittäjien järjestelmiin ovat arkaluontoista tietoa, ja niitä on kohdeltava sen mukaisesti.

1.6	**Verkkotunnusten hallinnointi**	Yhteystiedot
Varmista, että kaikkien verkkotunnusten yhteystiedot ovat ajan tasalla ja että mahdolliset laskutustiedot verkkotunnusvälittäjän suuntaan ovat ajan tasalla.		

Kannattaa harkita toimenkuvakohtaisten sähköpostiosoitteiden luomista, jotta tärkeää tietoa ei jää huomaamatta mahdollisten henkilövaihdosten vuoksi. Tällöin on varmistettava, että asianosaiset työntekijät seuraavat kyseisiä osoitteita aktiivisesti. Organisaation verkkotunnusten rekisteröintiin ei välttämättä kannata käyttää työntekijöiden yksityisiä sähköpostiosoitteita.

1.7	**Verkkotunnusten hallinnointi**	Palauttaminen
Tutustu verkkotunnusvälittäjän menettelytapoihin kaapattujen verkkotunnusten palauttamiseksi. Varmista että tarvittava dokumentaatio on tallessa.		

Huomaa että prosessit kaapattujen verkkotunnusten palauttamiseksi vaihtelevat merkittävästi verkkotunnusrekisteristä riippuen. Fi-verkkotunnuksen tapauksessa ota yhteyttä omaan verkkotunnusvälittäjääsi ja tarvittaessa Liikenne- ja viestintävirasto Traficomiin.

Yleisesti ottaen, seuraavat asiakirjat voivat olla hyödyllisiä kaapatun verkkotunnuksen palauttamisessa:

- tuloste verkkotunnuksen rekisteröinnistä
  (WHOIS-haku tai ruutukaappaus / vienti verkkotunnusvälittäjän tiedoista)
- lasku ja tosite maksusuorituksesta
- välittäjän kanssa käyty rekisteröityjä verkkotunnuksia koskeva kirjeenvaihto
- mahdolliset oikeudelliset asiakirjat, joista käy ilmi organisaation ja verkkotunnuksen nimen välinen yhteys.

1.8	**Verkkotunnusten hallinnointi**	Verkkotunnuksen uusiminen
Tarkkaille kaikkien rekisteröityjen verkkotunnusten voimassaoloaikaa ja jatka tarvittavien tunnusten rekisteröintiä hyvissä ajoin.		

Monet verkkotunnusvälittäjät tarjoavat mahdollisuuden verkkotunnusten automaattiseen uusimiseen. Se vähentää verkkotunnuksen voimassaolon umpeutumisen riskiä. Verkkotunnusten uusimista varten tulee laskutustiedot pitää ajan tasalla.

Vaikka fi-verkkotunnusvälittäjillä on lain mukainen velvollisuus tiedottaa fi-verkkotunnusten käyttäjiä voimassaoloajan päättymisen lähestymisestä, organisaatiolla on oltava oma prosessinsa uudistamisen varmistamiseen. Jos verkkotunnuksen rekisteröintiä ei uusita ajoissa se vanhenee ja verkkotunnus vapautuu suoja-ajan jälkeen muiden käyttöön.

1.9	**Verkkotunnusten hallinnointi**	Muutokset ja tarkistaminen
Jos verkkotunnusvälittäjän järjestelmässä olevia tietoja on tarpeen muuttaa, noudata muodollista muutostenkäsittelyprosessia. Tarkista voimassa olevat tiedot säännöllisesti sen varalta, ettei niihin ole tehty luvattomia muutoksia.		

Ikävien yllätysten välttämiseksi organisaatioiden on oltava erittäin valppaita tehdessään verkkotunnusten rekisteröintiä koskevia muutoksia. Virheelliset määritykset voivat aiheuttaa ongelmia esimerkiksi sähköpostiliikenteessä ja jopa estää pääsyn organisaation verkkosivuille. Aiotut muutokset on tarkistettava ja hyväksyttävä etukäteen organisaation muutostenkäsittelyprosessin mukaisesti.

1.10	**Verkkotunnusten hallinnointi**	Uusien verkkotunnusten rekisteröinti
Organisaatiolla on oltava muodollinen menettely uusien verkkotunnusten rekisteröimiseksi, ja sitä on noudatettava.		

Jotta organisaatiolla on selko hallussaan olevista verkkotunnuksista ja jotta uusien verkkotunnusten rekisteröiminen on turvallista, on luotava rekisteröintimenettely ja noudatettava sitä.

Menettelyllä voidaan myös varmistaa, että uudet verkkotunnukset ovat hyväksyttyjä, ne rekisteröidään oikeilla tiedoilla oikeille tileille verkkotunnusvälittäjän järjestelmässä, niitä hallinnoivat oikeat vastuuhenkilöt ja niiden turvallisuus taataan organisaation linjausten mukaisesti.

1.11	**Verkkotunnusten hallinnointi**	Estomahdollisuudet verkkotunnusvälittäjän järjestelmässä ja nimitietokannassa
Suojaa verkkotunnukset oikeudettomalta siirtämiseltä, päivittämiseltä ja poistamiselta verkkotunnusvälittäjän tarjoamilla estomahdollisuuksilla.		

Verkkotunnuksen tietojen muuttamisen Traficomin järjestelmässä voi estää niin sanotulla rekisterilukolla (registry lock). Rekisterilukko on poistettava ennen kuin muutoksia verkkotunnuksen tietoihin voi tehdä. Poisto onnistuu vain ennalta määriteltyihin puhelinnumeroihin lähetetty koodi käyttämällä. Rekisterilukon kytkemisen ja poistamisen yksityiskohdista tulee keskustella oman verkkotunnusvälittäjän kanssa.

2 Nimipalvelinten suunnittelua koskevat vaatimukset

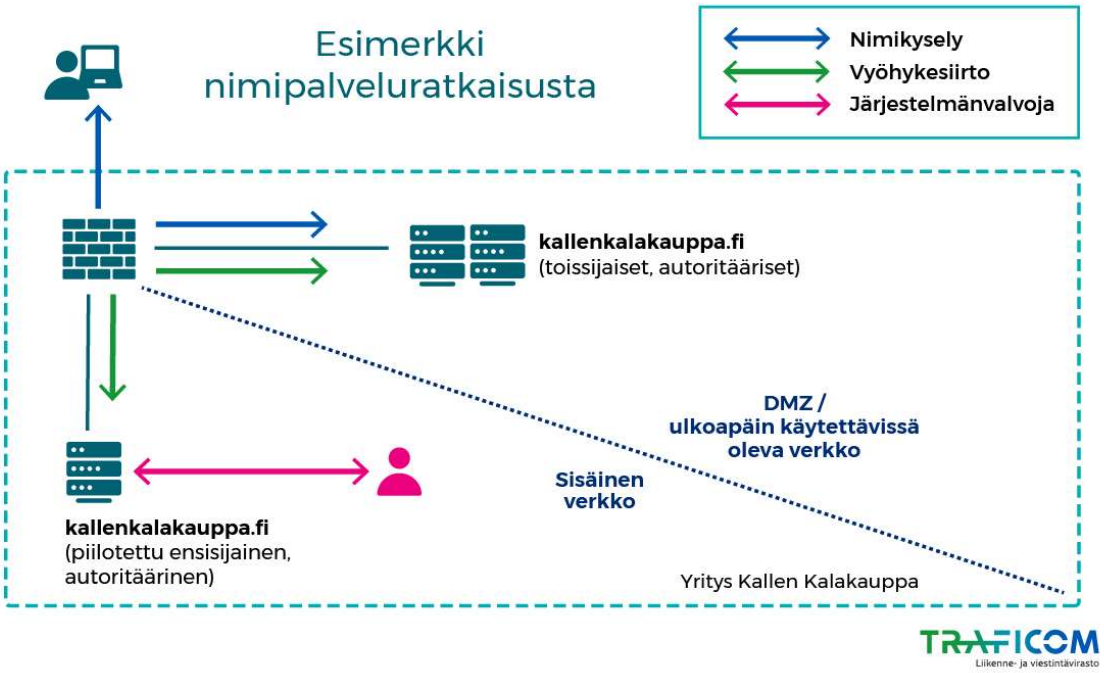
Seuraava osio ja siinä annettavat suositukset on suunnattu tietojärjestelmäsuunnittelijoille ja tietohallinnon tekniselle henkilöstölle. Siinä edellytetään DNS-järjestelmän perustietojen hallintaa. Käytettävistä käsitteistä ja nimikyselyprosessista on lisätietoa liitteissä A ja B.

Nimipalvelinten suunnittelussa on noudatettava tiettyjä perussääntöjä riippumatta siitä, käyttääkö organisaatio omaa nimipalvelinta, ostaako se nimipalvelun joltakin palveluntarjoajalta vai onko käytössä näiden vaihtoehtojen yhdistelmä.

Turvalliseksi suunniteltu nimipalvelin varmistaa sekä organisaation nimipalvelintietojen luotettavuuden, että sen järjestelmien käytettävyyden. Nimipalvelimen turvallinen toteutus voi myös vähentää nimipalvelimen hyväksikäytön riskiä DNS-pohjaisissa palvelunestohyökkäyksissä sekä välimuistin myrkyttämisen onnistumisriskiä.

Suositukset koskevat ensisijaisesti nimipalvelimia, joita käytetään ulkopuolisten verkkotunnusten nimiä koskeviin tiedusteluihin, mutta monet periaatteista pätevät myös sisäisiin nimipalvelimiin.

Kuvassa 1 alla esitetään esimerkki kuvitteellisen yrityksen Esimerkki Oy:n yksinkertaisesta nimipalvelinratkaistusta:



Kuva 1: Esimerkki nimipalvelinratkaisusta

Kuvassa esitetään esimerkki, ei varsinaista suositusta nimipalvelinratkaisun toteuttamiseksi. Organisaation kannalta paras ratkaisu määräytyy muun muassa organisaation koon, hosting-palvelun, resurssien ja internetin kautta käytettävien palvelujen käyttäjien maantieteellisen sijainnin mukaan.

Traficom antaa seuraavat internetin kautta käytettävissä olevien verkkotunnusten nimipalvelun suunnittelua koskevat suositukset:

2.1.1	Nimipalvelimien suunnittelu	Nimipalvelimien roolien erottelu
Määritä autoritääriset nimipalvelimet niin, etteivät ne hyväksy rekursiivisia kyselyjä		

Internetin kautta saatavilla olevat autoritääriset nimipalvelimet eivät saa käsitellä rekursiivisia pyyntöjä. Rekursiiviset pyynnöt lisäävät palvelimen kuormitusta ja voivat tehdä siitä alttiin DNS-reflektiohyökkäyksille ja välimuistin myrkytysyrityksille. Rekursiivisiin nimitiedusteluihin on käytettävä erillisiä nimipalvelimia, jotka ovat ainoastaan sisäisten tai tunnettujen asiakkaiden käytettävissä.

2.1.2	Nimipalvelimien suunnittelu	Sisäiset ja ulkoiset verkkotunnukset
Tietoja sisäisistä verkkotunnuksista tai palvelimien nimistä ei saa olla saatavilla nimipalvelimilta joihin on pääsy ulkoa.		

Sisäisten järjestelmien nimiä ja IP-osoitteita, joita ei ole tarkoitettu ulkopuolisten ulottuville, ei saa olla käytettävissä ulkoisten nimipalvelinten vyöhykkeillä.

Sisäisten resurssien jaottelu yhdelle tai usealle alitunnukselle mahdollistaa sisäisten ja ulkoisten verkkotunnusten hallinnoinnin eriyttämisen ja supistaa tietomäärää, joka sisäisistä rakenteista on saataville internetissä.

2.1.3	Nimipalvelimien suunnittelu	Nimipalvelimien redundanssi
Turvaa nimipalvelun toiminta käyttämällä useita ulkoisia nimipalvelimia.		

Voi olla hyvä ratkaisu antaa organisaation ulkoiset nimipalvelimet osittain tai kokonaan organisaation sisäisistä rakenteista riippumattoman ulkoisen palveluntarjoajan hoidettavaksi. Nimipalvelujen tarjoajat pystyvät yleensä tarjoamaan tehokkaan suojan palvelunestohyökkäyksiltä, maantieteellisesti hajautetun nimipalvelinten sijainnin, ympärivuorokautisen valvonnan sekä erikoistuneen teknisen tukipalvelun. Osa nimipalveluista tukee myös Anycastia, joka varmistaa asiakkaiden pyyntöjen käsittelyn maantieteellisesti hajautetussa nimipalvelinten verkostossa. Tällöin myös vasteaika on asiakkaan kannalta lyhin mahdollinen.

Liikenne- ja viestintävirasto tarjoaa anycast hajautetun secondary nimipalvelun fi-verkkotunnuksille veloituksetta. Lisätietoja Traficom Anycast -palvelusta: https://www.traficom.fi/fi/hajautettu-nimipalvelu-valittajien-kayttoon.

Verkkotunnusten käyttäjät saavat Traficom Anycast -palvelun käyttöön fi-verkkotunnuksilleen oman verkkotunnusvälittäjänsä kautta.

2.1.4	Nimipalvelimien suunnittelu	Nimipalvelimien erityistehtävä
Älä käytä ulkoisia nimipalvelimia mihinkään muuhun tarkoitukseen kuin nimipalvelun hoitamiseen		

Nimipalvelimia ei tule käyttää muihin tehtäviin, ja niillä pitää käyttää ainoastaan nimipalvelun tuottamisen kannalta välttämättömiä ohjelmistoja. Se vähentää alttiutta hyökkäyksille sekä riskiä sille, että jonkin ohjelmiston haavoittuvuus voisi vaarantaa nimipalvelun turvallisuuden.

2.1.5	Nimipalvelimien suunnittelu	Primary nimipalvelimen piilottaminen
Älä käytä ensisijaista nimipalvelinta ulkoisten verkkotunnusten ulospäin näkyvänä nimipalvelimena (ns. hidden primary). Estä pääsy palvelimelle internetistä.		

Ensisijainen nimipalvelin sisältää ensisijaisen kopion vyöhykkeestä, ja pääsy siihen internetistä on estettävä. Palvelinta on käytettävä ainoastaan vyöhykkeen hallinnointiin ja vyöhyketietojen vaihtamiseen internetin kautta käytettävissä olevien toissijaisten nimipalvelinten kanssa. Pääsy palvelimille on rajattava hyväksytyille nimipalvelun järjestelmänvalvojille. Kuvassa 1 on esitetty esimerkki nimipalvelinratkaisusta, jossa ensisijainen nimipalvelin on piilotettu.

2.1.6	Nimipalvelimien suunnittelu	Toissijaisten nimipalvelimien sijainti
Sijoita toissijaiset nimipalvelimet erilliseen verkkosegmenttiin, johon ja josta sallitaan vain asianmukainen liikenne.		

Eristämällä internetin kautta käytettävät nimipalvelimet erilliseen, palomuurilla suojattuun verkkosegmenttiin voidaan pienentää sitä riskiä, että mahdollisesti vaarantunut palvelin toimii ponnahduslautana muiden palveluiden peukaloinnille. Mahdollinen toteutusesimerkki on esitetty kuvassa 1, jossa internetin kautta käytettävissä olevat nimipalvelut on eristetty DMZ-vyöhykkeelle. Nimipalvelun käytettävyys on kuitenkin varmistettava kahdentamalla rakenteita ja/tai käyttämällä ulkoisia nimipalvelun tarjoajia.

2.1.7	Nimipalvelimien suunnittelu	Nimipalvelimien palomuurisuojaus
Suojaa nimipalvelimet palomuureilla, jotka sallivat vain välttämättömän tietoliikenteen.		

Palomuurimääritysten kokonaisuus määräytyy valitun hostingmallin ja organisaation muiden tietoteknisten rakenteiden mukaan.

Arvioitaessa liikenteen välttämättömyyttä eri asiakkaiden, palvelinten ja verkkosegmenttien välillä on otettava huomioon seuraavat seikat:

- Nimikyselyt on voitava sallia ainoastaan tietyiltä asiakkailta (sisäisiltä/ulkoisilta nimipalvelimen roolin mukaan) porttiin 53 yhdistetyn TCP:n ja UDP:n kautta.
- Sisäisiä käyttäjiä palvelevien rekursiivisten nimipalvelinten on voitava tehdä nimikyselyjä internetistä porttiin 53 yhdistetyn TCP:n ja UDP:n kautta.
- Autoritääristen toissijaisten nimipalvelinten on voitava vastaanottaa ilmoituksia ensisijaiselta nimipalvelimelta (notify) sekä vaihtaa vyöhyketietoja ainoastaan ensisijaisen nimipalvelimen kanssa.
- Keskitettyyn lokipalveluun (SIEM) suuntautuva ja palvelinten hallinnoinnin kannalta välttämätön tietoliikenne on rajattava välttämättömiin IP-osoitteisiin ja portteihin.
- On syytä harkita DNS-protokollan tarkastuksen käyttöönottoa, jos palomuuri tukee sitä. Siten voidaan varmistaa, että vain viralliset DNS-vaatimukset täyttävät liikenne sallitaan. Kannattaa kuitenkin huomata, että DNSSECin aktivointi voi edellyttää suurten DNS-pakettien hyväksymistä sekä TCP:n käyttöä hakujen toteuttamiseen ja vastaamiseen.

Palomuurimääritykset on testattava perusteellisesti ennen käyttöönottoa.

2.1.8	Nimipalvelimien suunnittelu	Turvallinen tietoliikenne nimipalvelinten välillä
Varmista ensisijaisen ja toissijaisten nimipalvelinten väliset vyöhykesiirrot TSIG:llä.		

Jos vyöhyketietoja jaetaan toissijaisille nimipalvelimille ensisijaiselta nimipalvelimelta tehtävän vyöhykesiirron avulla, tietoliikenne on suojattava TSIG-allekirjoituksella[1]. TSIG varmistaa, että vyöhykesiirto voidaan suorittaa ainoastaan tunnistetuille toissijaisille nimipalvelimille ja että varsinainen tietojen päivitys suoritetaan asianmukaisesti. Jokaisella nimipalvelinparilla on oltava ainutkertaiset TSIG-avaimet, ja TSIG-suojaukseen on sovellettava asianmukaisia tiukkoja palomuurimäärityksiä (ks. edellä). Avaimet luodaan nimipalvelinohjelmistolla, joka määritetään allekirjoittamaan kaikki muiden nimipalvelinten kanssa tapahtuva tietoliikenne.

2.1.9	Nimipalvelimien suunnittelu	Nimipalvelimen hyväksikäyttö palvelunestohyökkäyksissä
Määritä nimipalvelimet ja verkon osa-alueet siten, että DNS-reflektiohyökkäyksiin perustuvien palvelunestohyökkäysten vaara on mahdollisimman pieni.		

Nimipalvelimia voidaan käyttää hyväksi DNS-reflektiohyökkäyksissä, joissa lähettäjän IP-osoite väärennetään ja DNS-kyselyn yhteydessä käytetään lähettäjän osoitteen sijaan hyökkäyksen uhrin IP-osoitetta. Koska nimipalvelimen lähettämät vastauspaketit ovat suurempia kuin kyselyt, menettelyllä voidaan ylikuormittaa uhrin palvelinta tai verkkoresursseja. DNSSECiä käytettäessä vastauspaketit ovat tavallista suurempia, koska ne sisältävät myös digitaalisen allekirjoituksen. Tämä tekee DNSSECiä käyttävistä nimipalvelimista erityisen kiinnostavia palvelunestohyökkäysten tekijöiden silmissä. Riskiä voi pienentää seuraavin lisätoimenpitein:

- internetin kautta tehtävien rekursiivisten kyselyiden kieltäminen
- AXFR-pyyntöjen (vyöhykesiirtojen) kieltäminen muilta kuin autoritäärisiltä nimipalvelimilta
- samasta IP-osoitteesta tietyn ajan kuluessa tulevien kyselyiden määrän rajoittaminen (*rate limiting*)
- reititinten ja palomuurien määrittäminen hyväksymään ainoastaan paketit, jotka tulevat verkkopaketin lähettämiseen käytettävässä verkossa hyväksytyistä IP-osoitteista (IP-osoitteiden väärentämisen esto)
- ANY-kyselyiden (kaikki tietueet) kieltäminen, jos nimipalvelinohjelmisto mahdollistaa sen.

2.1.10	Nimipalvelimien suunnittelu	Versiotiedot
Määritä nimipalvelimet siten, ettei niiden vastaustietue sisällä ohjelmiston nimeä tai versionumeroa.		

Jos nimipalvelin ilmoittaa sitä pyörittävän ohjelmiston nimen tai versionumeron, hyökkääjä voi helposti iskeä tunnettuihin haavoittuvuuksiin ja räätälöidä hyökkäyksensä juuri tietylle ohjelmistoversiolle. Nimen ja versionumeron piilottaminen ei sinänsä poista haavoittuvuuksia, mutta se voi pakottaa hakkerin tekemään lisäselvityksiä, jotka saatetaan havaita organisaation valvontajärjestelmässä. On hyvien käytäntöjen mukaista olla julkistamatta tarpeettomia tietoja, mutta vielä tärkeämpää on varmistaa, että nimipalvelimet ja niiden käyttöjärjestelmät pidetään aina päivitettyinä (ks. alla).

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

2.1.11	Nimipalvelimien suunnittelu	Päivitykset
Pidä nimipalvelimet ja niiden käyttöjärjestelmät aina päivitettyinä uusimmilla versioilla		

Sekä nimipalvelinohjelmiston että sitä tukevan hostingympäristön turvallisuuspäivityksillä poistetaan havaittuja haavoittuvuuksia ja autetaan turvaamaan verkkotunnustietoja sekä organisaation nimipalvelun käytettävyyttä. Jos nimipalvelusta vastaa kokonaan tai osittain ulkoinen toimittaja, organisaation on varmistettava, että turvallisuuspäivitykset testataan ja asennetaan hyvissä ajoin ja selkeästi määriteltyä, organisaation hyväksymää menettelyä noudattaen.

2.1.12	Nimipalvelimien suunnittelu	Määritysten muuttaminen
Noudata nimipalvelimen määritysten tai ratkaisun perusrakenteiden muuttamisessa muodollista muutostenkäsittelyprosessia.		

Kaikki aiotut muutokset nimipalvelinjärjestelmän rakenteisiin tai määrityksiin on tarkistettava ja hyväksyttävä etukäteen organisaation muutostenkäsittelyprosessin mukaisesti. Järjestelmällinen lähestymistapa muutosten käsittelyyn voi vähentää yllättävien seurausten riskiä ja parantaa käytettävyyttä.

2.1.13	Nimipalvelimien suunnittelu	Lokit
Pidä lokia nimipalvelinten hallinnointitoimista organisaation lokiohjeistuksen mukaisesti. Käy lokit säännöllisesti läpi oikeudettomiin toimiin viittaavien tapahtumien havaitsemiseksi		

Vähimmillään lokia on pidettävä hylätyistä ja hyväksytyistä kirjautumisyrityksistä sekä määritysten ja vyöhykkeiden muutoksista. Hyvät lokit auttavat paikantamaan virheitä ja hoitamaan turvallisuuspoikkeamia.

2.1.14	Nimipalvelimien suunnittelu	Primary nimipalvelimen piilottaminen
Käy vyöhykkeet säännöllisesti läpi sen varmistamiseksi, että tietueet ovat kunnossa ja ettei niihin ole tehty luvattomia muutoksia		

Tietueet on tarkistettava säännöllisesti ja varmistettava, että ne ovat asianmukaisia ja oikean sisältöisiä. Käyttämättömät ja muuhun kuin rekisteröityyn kohteeseen liittyvään IP-osoitteeseen viittaavat tietueet on poistettava. Jos havaitaan merkkejä luvattomista muutoksista, on otettava välittömästi yhteyttä oman organisaation tietoturvavastaavaan.

2.1.15	Nimipalvelimien suunnittelu	DNSSECin käyttäminen
Käytä DNSSECiä mahdollisuuksien mukaan kaikissa käytössä olevissa ulkoisissa verkkotunnuksissa.		

DNSSEC estää nimikyselyihin annettavien vastausten väärentämisen ja varmistaa vastauksen tulevan tunnistautuneelta nimipalvelimelta.

Vaikka verkkotunnus ei olisi käyttäjän aktiivisessa käytössä, ilman DNSSEC-laajennusta vastauksia kyselyihin voidaan väärentää. Tällöin kysyjä voi päätyä jonkin ulkopuolisen tahon hallussa olevalle tietojenkalastelusivulle. Fi-verkkotunnuksen tapauksessa tarpeettomalta verkkotunnukselta kannattaa poistaa nimipalvelimet kokonaan. Fi-verkkotunnuksella ei ole pakko olla nimipalvelimia lainkaan.

2.2 DNSSECiä koskevat suositukset

Koska DNS on olennainen tekijä palvelujen paikantamisessa internetissä, hyökkääjät voivat olla kiinnostuneita nimipalvelukyselyihin annettavien vastausten väärentämisestä väliintulohyökkäyksillä tai välimuistin myrkytyshyökkäyksillä. Jos hyökkäys onnistuu, käyttäjä voidaan esimerkiksi ohjata muulle sivulle kuin varsinaiselle kohdesivulle, ja hänet voidaan saada paljastamaan kirjautumistietonsa tai muita arkaluontoisia tietoja. Tämän kaltaisia hyökkäyksiä kohdistetaan internetissä yleensä ulkoisiin verkkotunnuksiin.

DNSSEC (*domain name system security extensions*) on DNS-standardin laajennus, joka varmistaa salausmenetelmien avulla kysyjän voivan luottaa siihen, että

- vastaus nimikyselyyn tulee oikealta nimipalvelimelta
- vastausta ei väärennetä matkan varrella
- vastaus, jonka mukaan kysyttyä nimeä ei ole olemassa, voidaan todentaa oikeaksi.

Merkille pantavaa on, ettei DNSSEC salaa varsinaista DNS-liikennettä. DNS-liikenteen salaamista, kuten *DNS over TLS*- tai *DNS over HTTPS*-tekniikoiden käyttöä, ei käsitellä tässä ohjeessa.

DNSSEC-validointimenettely

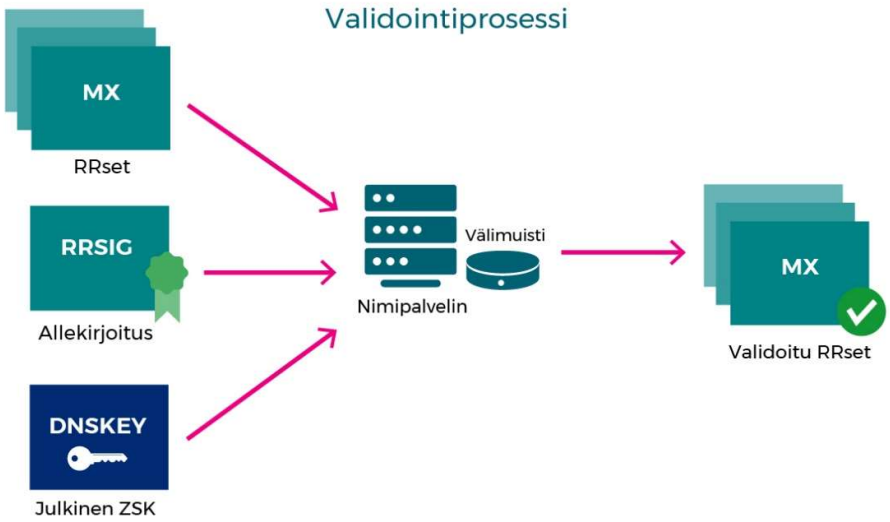
DNSSECillä suojattujen verkkotunnusten nimikyselyprosessi on pitkälti sama kuin tavallinenkin kyselyprosessi (ks. liite B: Nimikyselyprosessi), mutta se sisältää sekä yksittäisten vastausten kryptografisen validoinnin, että prosessiin osallistuvien nimipalvelinten hierarkkisen aseman varmentamisen.

Vastausten validointi

Nimikyselyn vastausten validointiin käytetään seuraavia tietueita:

- **RRset (resource record set):**
  Kaikkien tietyn tyyppisten resurssitietueiden (esimerkiksi A- tai MX-tietueiden) ryhmittely
- **RRSIG (resource record signature):**
  RRsetin allekirjoitettu tiivistearvo (*hash value*) yksityisen ZSK-avaimen perusteella
- **ZSK (zone signing key):**
  Julkinen salausavain vyöhykkeen RRSIG:ien validointiin
- **DNSKEY:**
  Tietuetyyppi, jota käytetään julkisten salausavainten tallentamiseen

Vastausten validointia DNSSEC-allekirjoitetulla vyöhykkeellä kuvataan kuvassa 2 alla.



Kuva 2: Resurssitietueen validointiprosessi (esimerkkinä MX-tietue)

Julkisen ZSK-avaimen eli vyöhykkeen allekirjoitusavaimen avulla kyselyä käsittelevä nimipalvelin voi validoida kysytyn tietueen sisältämän tietuejoukon (RRset) allekirjoituksen (RRSIG). Tällä varmistetaan epäaitojen vastausten havaitseminen.

Vastaavien palvelinten validointi

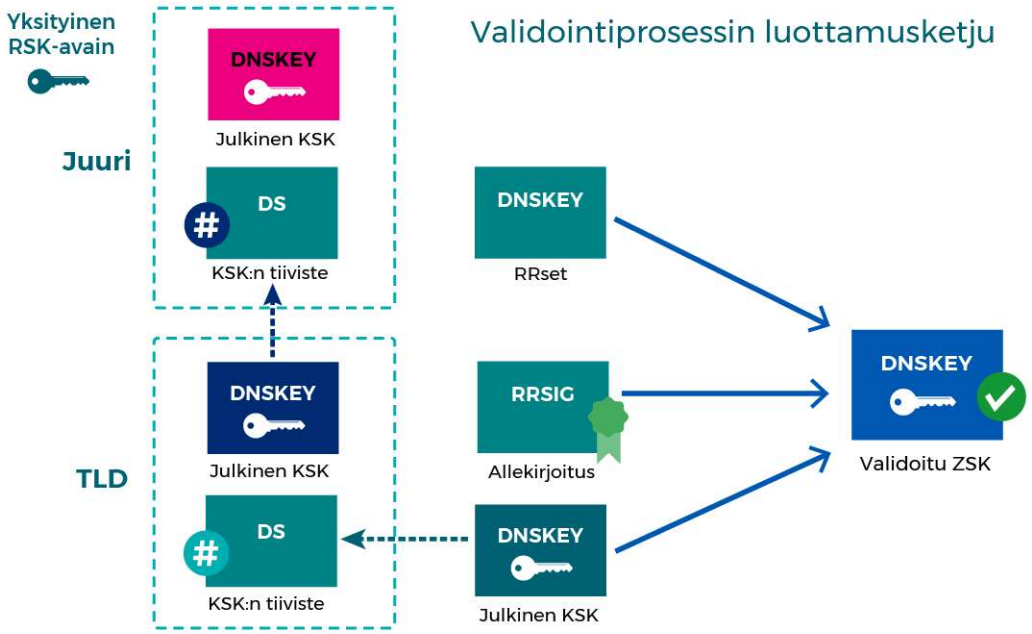
Jotta validoidun vastauksen lähteeksi voidaan todeta asianmukainen nimipalvelin, jolla on valtuutus vastata verkkotunnuksen puolesta, yllä kuvatussa prosessissa käytettävä julkinen ZSK-avain (sininen väri) on kyettävä validoimaan. Tähän käytetään seuraavia tietueita:

- **KSK (key signing key):**
  Julkinen salausavain DNSKEYn RRset-tietuejoukon RRSIG-allekirjoituksen varmentamiseen, esimerkiksi ZSK-avain.
- **DS (delegation signer):**

Julkisen KSK-avaimen tiivistearvo, joka tallennetaan verkkotunnuksen delegoinnista vastaavalle vyöhykkeelle (*parent zone*).

Prosessi on edellä kuvatun kaltainen, mutta se on ketjutettu ”luottamusketjuksi” (*chain of trust*) TLD:n kautta DNS-järjestelmän juureen (ks. kuva 3). Julkinen ZSK-avain validoidaan julkisella KSK-avaimella, jonka tiivistearvo on tallennettu ylätason vyöhykkeen (*parent zone*) DS-tietueeseen.

.fi-verkkotunnusten DS-tietueet on tallennettu Verkkotunnusjärjestelmään, jota ylläpitää Traficom. Rekisterin oma KSK-avain sijaitsee tiivistearvona hierarkian juuressa[2]. Näin läpi vyöhykehierarkian voidaan kryptografisesti varmentaa, että nimikyselyihin antavat allekirjoitettuja vastauksia aina pelkästään valtuutetut nimipalvelimet. Prosessi kuvataan kuvassa 3 alla.



Kuva 3: Yleiskuva DNSSEC-validointimenettelystä

Vaikka validointimenettely voi vaikuttaa monimutkaiselta, DNSSECin käyttöönotto organisaation verkkotunnuksissa on yleensä yksinkertaista. Sen voi ottaa käyttöön nimipalvelutoimittajan (usein yhtä kuin verkkotunnusvälittäjä) kautta, tai organisaation oma nimipalvelinten järjestelmänvalvoja voi aktivoida sen. On kuitenkin ensisijaisen tärkeää, että nimipalvelimien ylläpitäjä suunnittelee avaintenhallintaprosessit huolella.

Riippumatta siitä, käytetäänkö organisaation ulkoisissa verkkotunnuksissa DNSSECiä, Traficom antaa seuraavat suositukset:

2.2.1	Nimipalvelimien suunnittelu	DNSSECin käyttäminen
Käytä DNSSECiä mahdollisuuksien mukaan kaikissa käytössä olevissa ulkoisissa verkkotunnuksissa.		

2 Hierarkian ylimmän tason verkkotunnusten (juuritunnus) julkiset KSK- ja ZSK-avaimet allekirjoitetaan yksityisellä *root signing key* -avaimella monimutkaisessa menettelyssä, joka toistetaan neljä kertaa vuodessa. Tavoitteena on juuriavainten luotettavuuden säilyttäminen.

Jotta organisaation omia käyttäjiä voidaan suojella väärennettyjen tai valtuuttamattomien nimipalvelinten lähettämiltä vastauksilta, nimikyselyitä organisaation käyttäjien puolesta hoitavat nimipalvelimet on määritettävä niin, että DNSSECiä käyttäviä verkkotunnuksia koskevat vastaukset validoidaan. Jos vastaus ei läpäise DNSSEC-validointia, se voi olla merkki vastauksen peukaloinnista, mutta syynä voi olla myös virhe DNSSECillä allekirjoitetun vyöhykkeen määrityksissä.

Vianetsinnässä on apua seuraavista työkaluista:

https://dnssecdebugger.verisignlabs.com/

https://dnsviz.net/

DNSSECin käyttöönottoa ja käyttöä koskevia suosituksia

2.2.2	DNSSEC	DNSSECin käyttöönotto kaikilla autoritäärisillä nimipalvelimilla
Kaikkien nimipalvelimien on tuettava DNSSECiä		

Jos kaikki nimipalvelimet DNSSECillä allekirjoitetulla vyöhykkeellä eivät tue DNSSECiä, validointi voi epäonnistua ja seurauksena olla käytettävyysongelmia.

2.2.3	DNSSEC	Allekirjoitusten uudistaminen
Uudista allekirjoitukset automaattisesti hyvissä ajoin ennen niiden voimassaoloajan päättymistä		

Jos vyöhykkeellä ei käytetä DNSSECiä, sitä päivitetään yleensä vain silloin, kun tietueita muutetaan, poistetaan tai luodaan. DNSSECiä käytettäessä on huomattava, että allekirjoitukset ovat voimassa ainoastaan rajoitetun ajan, ja ne on uudistettava hyvissä ajoin ennen voimassaoloajan umpeutumista. On otettava huomioon myös se, että vanhoihin allekirjoituksiin perustuvia tietueita voi olla välimuistissa, ja niiden validointi onnistuu edelleen siihen asti, kunnes ne poistuvat välimuistista (*time to live* eli TTL, elinaika, päättyy). Aktiivisen allekirjoituksen voimassaolon päättyminen johtaa siihen, että DNSSEC-allekirjoituksen validoivat asiakkaat eivät pääse käyttämään resurssia. Allekirjoitusten uudistaminen tapahtuu useimmiten automaattisesti, mutta prosessin toimintaa on valvottava.

2.2.4	DNSSEC	Vastaaminen olemattomia verkkotunnuksia koskeviin kyselyihin
Käytä NSEC3:a sellaisiin kyselyihin vastaamiseen, jotka koskevat olemattomia verkkotunnuksia. NSEC3 estää "zone walkingin", eli koko zonen sisältöä ei ole mahdollista selvittää		

Olemassa olevia verkkotunnuksia koskeviin kyselyihin annettavien vastausten tavoin myös olemattomia verkkotunnuksia koskevat vastaukset on voitava todentaa DNSSECillä. NSEC3 soveltuu tähän tarkoitukseen: sillä voi ketjuttaa kaikki vyöhykkeellä sijaitsevat verkkotunnukset yhteen ja osoittaa, että ketjusta puuttuvia verkkotunnuksia ei ole olemassa. Jotta vyöhykkeeltä ei voida hakea kokonaista todellisia nimiä sisältävää tietuetta käymällä ketju läpi alusta loppuun, NSEC3 esittää nimien tiivisteet salatussa muodossa selkotekstin sijaan.

2.2.5	DNSSEC	Avainten vaihtaminen
Uudista KSK- ja ZSK-allekirjoitusavaimet säännöllisesti ja automaattisesti sekä aina silloin, kun niiden turvallisuuden epäillään vaarantuneen.		

KSK- ja ZSK-avaimilla on rajattu voimassaoloaika. Ne on myös uudistettava säännöllisesti, jotta niiden turvallisuus ei vaarannu. Useimmissa nimipalvelinratkaisuissa prosessi on mahdollista automatisoida. Huomaa kuitenkin, että KSK-avainten uudistaminen edellyttää päivitettyjen DS-tietueiden vaihtamista ylätason vyöhykkeen (*parent zone*) kanssa. Käytännössä fi-verkkotunnuksen tapauksessa uudet DS-tietueet tulee päivittää fi-juureen.

Prosessissa on ehdottomasti otettava huomioon aiemmin luotujen allekirjoitusten voimassaoloaika, tietojen elinaika (TTL) välimuistissa sekä DNS-tietueiden replikointi DNS-järjestelmässä.

2.2.6	DNSSEC	KSK-avaimien luominen ja säilyttäminen
Luo ja säilytä KSK-allekirjoitusavaimet turvallisessa ympäristössä		

DNSSECillä turvattujen vyöhykkeiden ZSK-avaimet perustuvat KSK-avaimiin, joten KSK-avaimet on luotava ja säilytettävä turvallisessa ympäristössä. Jos organisaation turvallisuusvaatimustaso on korkea tai sillä on salaustarpeita, kannattaa harkita HSM-turvamoduulin (*hardware security module*) käyttöä salaus- ja allekirjoitusavainten luomiseen ja säilyttämiseen.

2.2.7	DNSSEC	Avain- ja tiivistealgoritmi
Käytä vain yleisesti turvallisina pidettyjä algoritmeja		

DNSSEC-allekirjoitettujen .fi-vyöhykkeiden salauksen perustana ylivoimaisesti yleisimmin käytetty algoritmi on RSA/SHA-256 (8). Algoritmia 8 pidetään yleisesti turvallisena.

Sen sijaan algoritmeja 5 (RSA/SHA-1), 6 (DSA-NSEC3-SHA1) tai algoritmia 7 (RSASHA1-NSEC3-SHA1) EI tule käyttää.

ECDSA:han perustuvat avaimet ja allekirjoitukset (fi-verkkotunnuksilla voi käyttää algoritmia 13 ECDSAP256SHA256) ovat paljon lyhyempiä kuin RSA:han perustuvat, joten ne vievät vähemmän tilaa vyöhykkeellä ja nimihauissa. Allekirjoittaminen niillä on nopeampaa, mutta niiden validointi on hitaampaa.

Jos turvallisuutta ja nopeutta halutaan painottaa toisenlaisessa suhteessa, myös algoritmeja 8 (RSA/SHA-256) ja 10 (RSA/SHA-512) voi harkita. Toisin kuin voisi ajatella ei algoritmi 10 käytännössä ole turvallisempi kuin algoritmi 8. Algoritmin 10 käyttämiselle ei kuitenkaan ole käytännön esteitä.

Uusimpia DNSSEC algoritmeja ovat algoritmit 15 (Ed25519) ja 16 (Ed448). Algoritmit ovat vielä melko uusia, eivätkä kaikki resolverinimipalvelimet tue vielä algoritmeja 15 ja 16. Fi-verkkotunnuksille algoritmin 15 tuki on tulossa, vielä sitä ei ole mahdollista käyttää.

Käytettävästä algoritmista riippumatta DNSSECillä allekirjoitetut vastaukset ovat usein niin suuria, että ne on lähetettävä TCP-yhteydellä. Kuten aiemmin todettu, tämän vuoksi on tärkeää sallia aina TCP:n kautta tapahtuvat DNS-kyselyt.

2.2.8	DNSSEC	DNSSEC-liikenteen tukeminen verkossa
Varmista, että nimipalvelun käyttämä verkkoratkaisu tukee DNSSEC-tiedonsiirtoa.		

Koska nimikyselyt ovat DNSSEC-allekirjoitetulla vyöhykkeellä tavallista suurempia, on varmistettava, että verkkokokoonpano ja palomuurit tukevat niitä. Asia on testattava ennen DNSSECin käyttöönottoa, jotta palveluiden käyttävyys ei vaarannu. Esimerkiksi EDNS0 ei enää useimmille palomuureille ja muille verkkolaitteille ole enää ongelma, on asiaan kuitenkin hyvä kiinnittää huomiota.

3 Muita hyödyllisiä toimenpiteitä

Alla mainittavia teknisiä ratkaisuja ei käsitellä tässä ohjeessa, mutta ne kannattaa ottaa huomioon mahdollisina hyödyllisinä lisätoimenpiteinä, joilla voi edistää organisaation infrastruktuurin ja viestinnän suojaamista:

- DANE: DNS-based Authentication of Named Entities
  DNSSECiä vastaava menetelmä soveltuu seuraaviin tehtäviin:
  - sen ilmaiseminen, minkä varmenteiden myöntäjän verkkotunnuksen omistaja sallii myöntää verkkotunnuksen resursseja koskevia varmenteita,
  - verkkotunnuksen resurssien käyttämien hyväksyttyjen salausvarmenteiden ilmaiseminen
  - ilmoittaminen sähköpostiviestien lähettäjille siitä, että heidän on salattava verkkotunnuksen sähköpostipalvelimelle suuntautuva viestiliikenne.
- SPF: sender policy framework
  DKIM: domain keys identified mail

  DMARC: domain-based message authentication, reporting and conformance DNS-pohjaiset toimenpiteet, joilla voidaan estää väärennettyjen sähköpostiviestien toimittamista vastaanottajalle.

4 Lähdeviitteet

Liikenne- ja viestintävirasto kiittää Tanskan Kyberturvallisuuskeskusta *Center for Cybersikkerhed* lähdemateriaalista

Sisältöä koskevia vinkkejä on saatu esimerkiksi seuraavista lähteistä:

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

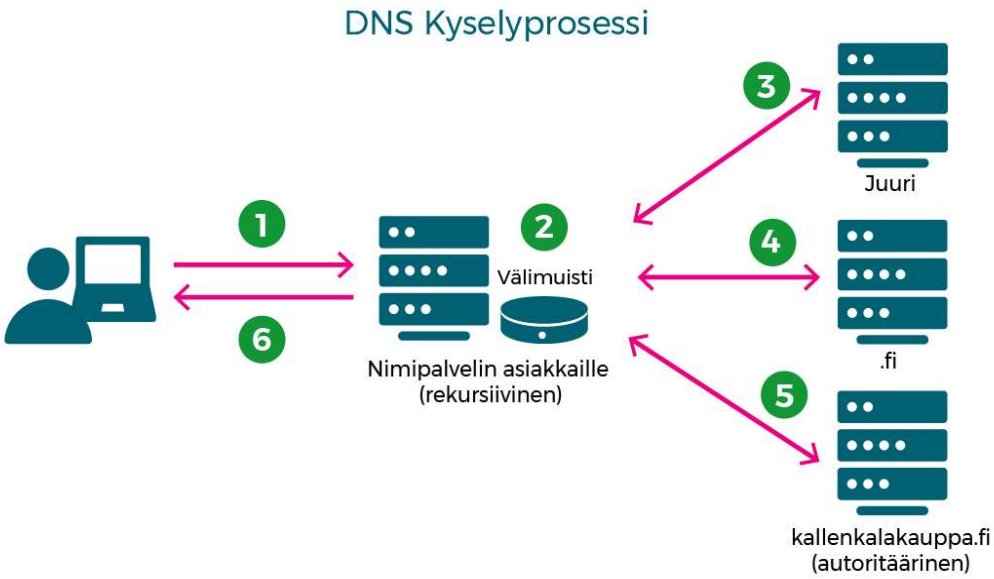
https://tools.ietf.org/html/rfc6781

5 Liite 1: Käsitteitä

Seuraavassa esitellään joukko käsitteitä määritelmineen sekä nimikyselyprosessin kuvaus tässä ohjeessa annettavien suositusten taustaksi:

- DNS (domain name system): Järjestelmä ja verkkoprotokolla, jonka ensisijainen tarkoitus on helpottaa nimien muuntamista IP-osoitteiksi verkossa. Nimijärjestelmä on rakenteeltaan hierarkkinen, ja sitä hallinnoidaan hajautetulla nimipalvelinten verkostolla.
- Top-level domain (TLD): Nimihierarkian ylimmän tason verkkotunnus. Ylätason tunnukset voivat olla yleisiä (gTLD), kuten .com, .org ja .edu, tai maatunnuksellisia (ccTLD), kuten .fi tai .se.
- Nimitietokanta: Tietokanta tietyn TLD-verkkotunnuksen kaikista verkkotunnuksista, niiden haltijoista ja autoritäärisistä nimipalvelimista. Suomalaisten .fi-loppuisten verkkotunnusten nimitietokantaa ylläpitää Traficom.
- Välittäjä: Verkkotunnusten nimien rekisteröintipalvelua tarjoava välittäjä. Monet verkkotunnusvälittäjät tarjoavat myös kotisivutilaa ja nimipalvelinpalveluita, mutta ne eivät ole pakollinen osa välittäjien toimenkuvaa.
- Verkkotunnuksen käyttäjä: Henkilö tai organisaatio, jolla on tietyn verkkotunnuksen käyttöoikeus.
- Valtuutettu: Henkilö tai organisaatio, jolla on verkkotunnuksen haltijan myöntämä valtuutus suorittaa verkkotunnusta koskevia toimenpiteitä.
- Nimipalvelin: Palvelin tai palvelu, joka kääntää IP-osoitteiden nimiä DNS-protokollaa käyttäen.
    - Rekursiivinen nimipalvelin: Nimipalvelin, joka auttaa löytämään vastauksia asiakaskoneiden nimipalvelupyyntöihin tarkistamalla, onko nimi jo välimuistissa. Jos ei ole, palvelin esittää kyselyitä tarvittaville nimipalvelimille, kunnes saa autoritäärisen vastauksen.
    - Autoritäärinen nimipalvelin: Nimipalvelin, jolle on myönnetty autoritäärinen vastuu tietystä vyöhykkeestä.
- Vyöhyke: Vyöhyke käsittää kaikki tiedot verkkotunnuksesta, josta nimipalvelimella on autoritäärinen vastuu. Jos verkkotunnukseen ei liity muiden nimipalvelinten käsittelemiä alitunnuksia, vyöhyke voi olla yhtä kuin verkkotunnus. Jos verkkotunnukseen liittyy yksi tai useita muiden nimipalvelinten käsittelemiä alitunnuksia, verkkotunnuksella on useita vyöhykkeitä.
- Resource record (RR): Vyöhykkeen RR- eli resurssitietue, joka sisältää yleensä tietyn nimen, tyypin ja arvon. Esimerkki A-tyypin resurssitietueesta vyöhykkeellä kallenkalakauppa.fi:
    - www A 193.163.102.58 – osoite/isäntätietue (A), joka palauttaa IP-osoitteen 193.163.102.58 haettaessa nimellä www.kallenkalakauppa.fi.

6 Liite 2: DNS kyselyprosessi



Kuva 4: DNS Kyselyprosessi

1. Kun asiakas haluaa käydä verkkosivulla nimeltä www.kallenkalakauppa.fi, pyyntö lähetetään ensimmäiseksi nimipalvelimelle, jota tietokone on määritetty käyttämään. Yrityksessä tämä on yleensä yrityksen omassa verkossa toimiva nimipalvelin. Kotitalouksissa käytetään yleensä internetpalveluntarjoajan nimipalvelinta.
2. Nimipalvelin hakee välimuististaan tiedon siitä, onko vastaus kyselyyn jo tunnettu aiempien kyselyiden perusteella.
   Jos vastaus löytyy nimipalvelimen välimuistista, se ilmoitetaan asiakkaalle, ja prosessi päättyy tähän.
3. Jos vastaus ei ole tiedossa, eikä nimipalvelin tiedä, mitkä nimipalvelimet vastaavat verkkotunnuksesta kallenkalakauppa.fi tai ylätason tunnuksesta .fi, se kysyy joltakin tuntemaltaan root-hierarkian juureen sijoittuvalta nimipalvelimelta, mitkä nimipalvelimet vastaavat .fi-verkkotunnuksista.
   Jos kallenkalakauppa.fi-verkkotunnuksesta vastaavat verkkopalvelimet ovat tunnettuja, siirrytään suoraan vaiheeseen 5. Jos .fi-verkkotunnuksista vastaavat verkkopalvelimet ovat tunnettuja, siirrytään suoraan vaiheeseen 4.
4. Tämän jälkeen nimipalvelin kysyy joltakin tietoonsa tulleista .fi-nimipalvelimista, mitkä nimipalvelimet vastaavat verkkotunnuksesta kallenkalakauppa.fi.
5. Sitten nimipalvelin esittää pyynnön jollekin tietoonsa tulleista kallenkalakauppa.fi-nimipalvelimista ja saa vastauksena www.kallenkalakauppa.fi-tunnuksen IP-osoitteen.

6. Vastaus toimitetaan asiakkaalle ja tallennetaan joksikin aikaa nimipalvelimen välimuistiin. Sen ansiosta samaa verkkotunnuksen nimeä tai joitakin ketjuun sisältyneitä nimipalvelimia koskeviin tiedusteluihin voidaan vastata käymättä koko prosessia läpi alusta loppuun.

Asiakkaan nimipalvelin esittää asiakkaan puolesta rekursiivisen pyynnön (kohdat 3–5) ja varmistaa vastauksen saamisen, vaikka se edellyttäisi useilta nimipalvelimilta kysymistä.

Tietyn verkkotunnuksen autoritäärisestä nimipalvelusta (tässä esimerkissä kuvitteellinen yritys Esimerkki Oy, jonka verkkotunnus on kallenkalakauppa.fi) huolehtiva organisaatio vastaa verkkotunnuksen kaikkia nimiä koskevan tiedon toimittamisesta pyynnön esittävälle rekursiiviselle nimipalvelimelle.

Liikenne- ja viestintävirasto Traficom

PL 320, 00059 TRAFICOM
p. 029 534 5000

traficom.fi

TRAFICOM
Liikenne- ja viestintävirasto