



Korjausohjeet

Dokumentti 2 / 2 · tekninen toteutusohje. Yhteenvedo päättäjälle on dokumentissa 1 (*Tietoturvan tilannekatsaus*).

ASIAKAS	KOHDE	PALVELU	PÄIVÄMÄÄRÄ
Demo	tilitoimisto.fi	Perustarkastus	8.9.2026

KENELLE TÄMÄ PAPERI ANNETAAN

Sille, joka pääsee muokkaamaan verkkotunnuksenne DNS-asetuksia. Käytännössä se on verkkosivujenne toimittaja, IT-tukenne tai taho jolta verkkotunnus on ostettu. Jos ette tiedä kuka se on, kertokaa se meille, niin selvitämme sen yhdessä. Muutoksia ei tarvitse osata itse.

Osa kohdista ei ole verkkotunnuksen vaan verkkopalvelimen asetus. Ne on merkitty kohtaan *Tekijä* erikseen, ja ne kuuluvat verkkosivujenne ylläpitäjälle. Jos nämä ovat eri tahoja, antakaa paperi molemmille: kumpikin tekee vain omat rivinsa.

Ennen ensimmäistä muutosta: laske DNS-tietueiden TTL arvoon 300 sekuntia. Se tekee jokaisesta virheestä viiden minuutin ongelman tunnin sijaan. Nosta takaisin vasta kun kaikki on ollut vakaata kuukauden.

Verkkotunnuksenne nimipalvelimet: `dnssec3.euronic.fi`, `dnssec1.euronic.fi`, `dnssec2.euronic.fi`. Muutokset tehdään sen palvelun hallintapaneelissa, jolle nämä kuuluvat.

KAIKKI TARKISTETUT KOHDAT

Koko luettelo teknisin nimin ja mitatuin arvoin. Rivejä on enemmän kuin 19 tarkistusta, koska osa tarkistuksista koostuu useasta tietueesta: esimerkiksi sähköpostin väärennössuoja mitataan SPF-, DMARC-, DKIM- ja MX-tietueista. Myös kunnossa oleva tulos on tarkastuksen tulos: se kertoo mitä hyökkääjä yritti nähdä eikä nähnyt. **Korjattava** = tarkistusrivi jolla on korjattavaa (1 riviä). Yhdestä rivistä voi syntyä useampi löydös, joten korjausohjeita on enemmän kuin rivejä.

Kovennus = suositus, ei vika, eikä sillä ole kiirettä (5 kpl).

X	Väärennösten esto (DMARC)	Korjattava	Puuttuu
•	Saapuvan postin salaus (MTA-STX)	Kovennus	Ei käytössä. Lähettävä palvelin voi pudota salaamattomaan yhteyteen.
•	Evästeiden suojausliput	Kovennus	1 / 2 evästeeltä puuttuu lippuja: PHPSESSID (SameSite)
•	Julkiset vakiotiedostot	Kovennus	security.txt puuttuu: tietoturvahavainnon löytäjä ei tiedä kenelle ilmoittaa. robots.txt paljastaa arkaluonteisilta vaikuttavia polkuja: /wp-admin/
•	Verkkotunnuksen allekirjoitus (DNSSEC)	Kovennus	Ei käytössä. Suomessa tämä on harvinaista: noin 96 prosentilla pk-yrityksistä sitä ei ole. Suositellaan kovennuksena.
•	Varmentajan raja (CAA)	Kovennus	Ei rajausta. Salausvarmenteen nimellenne voi myöntää mikä tahansa varmentaja. Suositellaan kovennuksena.
✓	Sähköpostin väärennössuoja (SPF)	Kunnossa	Käytössä, politiikka -all
✓	Viestien allekirjoitus (DKIM)	Kunnossa	Löytyi, selektori s1, s2
✓	Sähköpostipalvelin (MX)	Kunnossa	Määritetty
✓	Sähköpostisuojausjärjestelmä	Kunnossa	Yksi tietue, 5 DNS-hakua (raja 10)
✓	Salausvarmenne (SSL/TLS)	Kunnossa	Voimassa, TLSv1.3, Let's Encrypt, vanhennee 71 päivän kuluttua
✓	Verkkosivun suojausotsikot	Kunnossa	Keskeiset kunnossa

✓	Palvelimen versiotietojen vuoto	Kunnossa	Palvelin ei kerro ulos tarkkaa versiotaan
✓	Suojaamaton yhteys (HTTPS-ohjaus)	Kunnossa	Salaamaton http-osoite ohjautuu salattuun
✓	Kansiodien näkyvyys	Kunnossa	Ei avoimia tiedostoluetteloita tarkistetuissa kansioissa
✓	Huijausdomainit	Kunnossa	Ei väärennöskelpoisia lähitunnuksia. Samannimisiä eri päätteellä löytyi 4 kpl, ja nämä ovat tyypillisesti yrityksen omia rekisteröintejä
✓	Julkinen altistuminen	Kunnossa	2 alidomainia julkisissa varmennelokeissa
✓	Postipalvelimen maine (mustat listat)	Kunnossa	Ei estolistoilla. Viestinne kulkevat normaalisti.
✓	Käytöstä poistuneet alaosoitteet	Kunnossa	Ei alaosoitteita jotka osoittaisivat olemattomaan palveluun.
✓	Verkkotunnuksen nimipalvelu	Kunnossa	Vastaa normaalisti

KORJATTAVAT LÖYDÖKSET

Väärennettyjä viestejä ei estetä (DMARC puuttuu)

KORKEA

Tekninen:

Verkkotunnukselle ei ole DMARC-tietuetta (_dmarc, v=DMARC1). Vastaanottavalle palvelimelle ei ole annettu käsittelyohjetta eikä raportointiosoitetta.

Korjaus:

Vaihe 1, voidaan tehdä heti. Lisätkää TXT-tietue nimelle _dmarc.

Arvo:

v=DMARC1; p=none; rua=mailto:dmarc@<verkkotunnuksenne>; fo=1

Korvatkaa raportointiosoite sillä postilaatikolla, johon raportit halutaan.

Tämä vaihe EI vaikuta postin kulkuun mitenkään: mitään ei ala hylkääntyä eikä mennä roskapostiin. Ainoa muutos on, että vastaanottavat palvelimet alkavat lähettää päivittäin raportin siitä, kuka verkkotunnuksenne nimissä lähettää.

Vaihe 2 tehdään myöhemmin: kun raporteista näkyy että kaikki omat lähettäjät läpäisevät, arvoksi vaihdetaan p=quarantine. Sen jälkeen väärennetty viesti menee vastaanottajan roskapostiin. Se on tavoiteltua.

Aikataulu:

heti

SSL/TLS-SERTIFIKAATTI

Salausvarmenne on voimassa (TLSV1.3) ja umpeutuu vasta 71 päivän kuluttua. Ei vaadi toimenpiteitä: uusiutuminen tapahtuu näissä yleensä automaattisesti.

JÄRJESTYS

Tee tässä järjestyksessä. Ohjeet ovat yllä kohdassa "Korjattavat löydökset".

1 Väärennettyjä viestejä ei estetä (DMARC puuttuu)

heti

KOVENNUKSET

Nämä eivät ole vikoja eivätkä ne ole korjauslistassa. Ne ovat suosituksia, jotka nostavat suojaustasoa, ja ne voi tehdä silloin kun sopii. Yllä olevassa tarkistustaulussa nämä kohdat lukevat tilassa "Kovennus".



Evästeiden suojausliput kuntoon (PHPSESSID)

Evästeestä puuttuu SameSite. Secure estää evästeen kulkemisen salaamattomana, HttpOnly estää sivulle ujutettua koodia lukemasta sitä, ja SameSite estää sen lähettämisen vieraalta sivulta. Istuntoevästeen kaappaus on tavallisin tapa päästä kirjautuneen käyttäjän tilille ilman salasanaa. Liput lisätään palvelinasetuksissa.



security.txt-tiedoston lisääminen sivustolle

Tiedosto kertoo mihin osoitteeseen tietoturvahavainnon voi ilmoittaa. Ilman sitä havainnon tehnyt ei tiedä kenelle kertoa, ja tieto joko jää tulematta tai päättyy julkisuuteen ennen teitä. Käytäntö on kansainvälinen (RFC 9116) ja tiedosto on muutama rivi tekstiä osoitteessa /.well-known/security.txt.

```
Tiedosto https://tilitoimisto.fi/.well-known/security.txt:
Contact: mailto:tietoturva@tilitoimisto.fi
Preferred-Languages: fi, en
Expires: 2027-09-08T00:00:00.000Z
```



robots.txt-tiedoston sisällön tarkistaminen

robots.txt on julkinen tiedosto, ja siihen on merkitty polkuja jotka vaikuttavat sisäisiltä: /wp-admin/. Tiedosto ohjaa hakukoneita mutta ei estä ketään avaamasta polkuja, joten se toimii myös karttana niille jotka etsivät juuri niitä. Suojaus kuuluu tehdä pääsynhallinnalla, ei piilottamalla.



MTA-STS: saapuvan sähköpostin salauksen pakottaminen

Ilman tätä lähetävä palvelin voi pudota salaamattomaan yhteyteen, jos joku häiritsee yhteydenmuodostusta. Silloin viestit kulkevat selväkielisinä. MTA-STS kertoo lähettäjiille, että salausta on vaadittava. Käyttöönotto on yksi DNS-tietue ja yksi tiedosto.

```
TXT _mta-sts v=STSV1; id=2026090801
TXT _smtp._tls v=TLSRPTv1; rua=mailto:tls@tilitoimisto.fi

Tiedosto https://mta-sts.tilitoimisto.fi/.well-known/mta-sts.txt:
version: STSV1
mode: testing
mx: tilitoimisto-fi.mail.protection.outlook.com
max_age: 604800
```



CAA-tietueen lisääminen verkkotunnukselle

CAA kertoo julkisesti, mitkä varmentajat saavat myöntää salausvarmenteen teidän nimellenne. Ilman sitä varmenteen voi myöntää kuka tahansa varmentaja maailmassa. Tietue lisätään kerran eikä se vaadi ylläpitoa. Se ei voi katkaista mitään, kunhan siihen merkitään se varmentaja jota jo käytätte. Tarkastuksessa havaittu varmentaja: Let's Encrypt.

```
CAA @ 0 issue "letsencrypt.org"
CAA @ 0 iodef "mailto:tietoturva@tilitoimisto.fi"
```



DNSSEC-allekirjoituksen kytkeminen päälle

DNSSEC allekirjoittaa verkkotunnuksenne nimipalvelutiedot, jolloin vastaanottaja voi varmistaa ettei vastausta ole matkalla muutettu. Ilman sitä liikenne voidaan suotuisissa oloissa ohjata väärään paikkaan ilman että käyttäjä huomaa mitään. Useimmilla verkkotunnustarjoajilla tämä on yksi valinta hallintapaneelissa. Suomessa DNSSEC on käytössä noin neljällä prosentilla pk-yrityksistä.

MIHIN TÄMÄ TOIMITUS PÄÄTTYY

DMARC-asetuksen kiristäminen loppuun asti vaatii sähköpostiraporttien seurannan usean viikon ajan. **Se ei sisälly tähän toimitukseen.** Tämä raportti kertoo mitatun nykytilan, tavoitearvot ja turvallisen järjestyksen. Ensimmäinen vaihe (p=none ja raportointiosoite) ei vaikuta postin kulkuun mitenkään ja sen voi tehdä heti. Seuraavia vaiheita ei pidä tehdä ennen kuin raportit on luettu.
