# Tietoturvan tilannekatsaus

Dokumentti 1 / 2 · yhteenveto päättäjälle. Tarkat asetukset ovat dokumentissa 2 (*Korjausohjeet*).

| ASIAKAS | KOHDE | PALVELU | PÄIVÄMÄÄRÄ |
|---|---|---|---|
| Demo | tilitoimisto.fi | Perustarkastus | 8.9.2026 |

**KORJATTAVAA LÖYTYI**

Löysimme 1 korjattavaa kohtaa, joista 1 on sellainen jota voidaan käyttää yritystänne vastaan ilman että hyökkääjän tarvitsee osata mitään erityistä.

## YHTEENVETO JOHDOLLE

Teidän tilitoimisto.fi -verkkosivustonne tietoturvan perusteita on nyt tarkastettu. Tarkastuksessa havaittiin, että sähköpostiviestien väärennöksiä ei estetä tehokkaasti, mikä voi mahdollistaa huijausyritykset yrityksenne nimissä. Tämä tarkoittaa, että vaikka väärennetty viesti tunnistettaisiinkin, järjestelmänne ei osaa käsitellä sitä automaattisesti, eikä teille välttämättä ilmoiteta väärennöksistä. On tärkeää huomata, että tämä heikentää luottamusta yrityksenne viestintään.

## TARKASTUKSEN TULOS

Perustarkastus kattaa 19 kohtaa. Mitatuista 17 kohdasta 11 oli kunnossa ja **1 kohdassa on korjattavaa**. 5 kohdassa ei ole vikaa mutta on parannettavaa; niistä seuraa 6 suositusta alla. 2 kohtaa (alidomainien suojaus, verkkotunnus tietovuodoissa) ei ollut olemassa mitattavana, koska niiden edellytys puuttuu. Ne kohdat joista seuraa tekemistä on eritelty alla omina kohtinaan.

## KORJATTAVAT LÖYDÖKSET

### Väärennettyjä viestejä ei estetä (DMARC puuttuu) KORKEA

| | |
|---|---|
| **Käytännössä:** | Vaikka väärennös havaittaisiin, kenellekään ei ole kerrottu mitä sille pitäisi tehdä. Ette myöskään saa tietoa siitä, että nimissänne lähetetään viestejä. |
| **Jos ei korjata:** | Kalasteluviesti teidän nimissänne päätyy asiakkaanne postilaatikkoon, ja saatte tietää siitä vasta kun asiakas soittaa ja kysyy oudosta laskusta. |
| **Aikataulu:** | **heti** |

## KÄYTÄNNÖN VINKKI DMARC-RAPORTTEIHIN

Kun DMARC on otettu käyttöön, se alkaa lähettää sähköpostiinne raportin päivittäin. Ne ovat koneluettavia liitetiedostoja eivätkä kiinnostavaa luettavaa, mutta älkää poistako raporttiosoitetta sen takia. Tehkää sen sijaan sähköpostiinne sääntö, joka siirtää raportit automaattisesti omaan kansioonsa postilaatikon ohi. Raportit säilyvät tallessa, mutta ette näe niitä arjessa.

Sääntö kannattaa tehdä heti, koska raportit ovat ainoa tapa huomata, jos sähköpostinne lakkaa jonain päivänä menemästä perille. Ilman niitä vika näkyy vasta siinä, ettei asiakas vastaa.

Säännön tunnistusehto: viestin aiheessa lukee “Report domain”. Toiminto: ohita postilaatikko ja merkitse luetuksi.

#### SUOSITUKSET

Nämä eivät ole vikoja. Mikään niistä ei ole kiireellinen, eikä yksikään vaadi jatkuvaa ylläpitoa. Tarkat ohjeet ovat dokumentissa 2.

**Evästeiden suojaaminen varastamiselta**

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.

**Ilmoituskanava tietoturvahavainnon löytäjälle**

Tiedosto kertoo mihin osoitteeseen tietoturvahavainnon voi ilmoittaa.

**Julkisen tiedoston sisällön tarkistus**

robots.txt on julkinen tiedosto, ja siihen on merkitty polkuja jotka vaikuttavat sisäisiltä: /wp-admin/.

**Teille tuleva posti kulkemaan aina salattuna**

Ilman tätä lähettävä palvelin voi pudota salaamattomaan yhteyteen, jos joku häiritsee yhteydenmuodostusta.

**Rajaus siihen kuka saa myöntää salausvarmenteen nimellänne**

CAA kertoo julkisesti, mitkä varmentajat saavat myöntää salausvarmenteen teidän nimellenne.

**Verkkotunnuksenne vastausten väärentämisen esto**

DNSSEC allekirjoittaa verkkotunnuksenne nimipalvelutiedot, jolloin vastaanottaja voi varmistaa ettei vastausta ole matkalla muutettu.

#### NÄIN ETENEMME

Dokumentti 2 sisältää jokaisesta kohdasta valmiin ohjeen: mitä muutetaan, mihin se viedään ja missä järjestyksessä. Antakaa se sille joka hallinnoi verkkotunnustanne, niin hän tietää mitä tehdä. Jos ette tiedä kuka se on, selvitämme sen yhdessä.

Tämä raportti kertoo **tämän päivän tilanteen**. Asetukset muuttuvat, varmenteet vanhenevat ja verkkotunnuksia unohtuu auki, eikä mikään niistä ilmoita itsestään. Jos haluatte tietää tilanteen jatkuvasti, Kybervartio-seuranta katsoo samat kohdat joka päivä ja kertoo samana päivänä jos jokin muuttuu.

Kysymykset tästä raportista kuuluvat hintaan. Vastaamme kirjallisesti, eikä kysyminen sido teitä mihinkään.

#### MITEN TARKASTUS TEHTIIN

Perustarkastus kattaa 20 ulkoapäin mitattavaa kohtaa.

Tarkastus tehtiin kokonaan ulkopuolisen näkökulmasta. Tiedot haettiin julkisesta nimipalvelusta, varmennelokeista, verkkotunnusrekisteristä ja julkisilta estolistoilta. Nämä tiedot ovat kenen tahansa haettavissa, ja juuri siksi ne kuuluvat tähän raporttiin: ne ovat myös hyökkääjän käytettävissä ilman että hän tekee mitään.

Osa kohdista edellytti verkkosivunne avaamista: salausvarmenne ja sen hyväksymät salausprotokollat, selainsuojaukset, evästeet, yhteyden ohjautuminen, kansioiden näkyvyys ja sivuston julkiset vakiotiedostot. Ne ovat tavallisia sivulatauksia

ja salausyhteyden avauksia, yhteensä alle kaksikymmentä pyyntöä, eli vähemmän kuin yhden kävijän selain tekee sivua avatessaan.

Palvelin- tai haavoittuvuusskannausta ei tehty. Emme murtautuneet, emme kokeilleet salasanoja emmekä muuttaneet mitään.

Tämä tarkastus kattaa sen, mikä näkyy ulos ilman että kukaan koskee järjestelmiinne. Se ei kerro, onko palvelimellanne vanhentunutta ohjelmistoa tai avoimia palveluita, eikä sitä pidä lukea todisteena siitä että kaikki on kunnossa.