

See on avalikult nähtava info kuupäevastatud vaatlus. See ei ole küberturvalisuse seaduse mõistes turvaaudit ega läbistustest. Me ei logi sisse, ei saada vorme ega ürita ühtegi kaitset ületada.

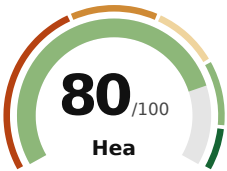
OEJ.

oej.ee

Päris avalikud vaatlused — piiratud valim, mitte kogu veebilehe hinnang.

Veebilehe piiratud avalik turvakontroll · oej.ee

Peamine leid Ettevõtte domeen ei palu postkastidel võltsitud kirju kinni pidada. Ettevõtte DMARC-reegel on ainult jälgimisrežiimis (p=none).



24/29 kontrolli · 25.10.2026

16 täielikult · 8 osaliselt või loendina · 5 hindamata

Turvalisuse hetkeseis

Hea. Üks leid vajab ülevaatus: e-posti võltsimise kaitse.

OEJ kontrolli skoor algab 100 punktist ja iga leid võtab punkte maha.

Skoor põhineb 24 tehtud kontrollil 29-st. See ei ole sertifikaat.

Tulemus: $100 - 20 \times 1 = 80$. Tasemed: 90–100 Väga hea · 75–89 Hea · 60–74 Rahuldav · 40–59 Puudulik · 0–39 Nõrk.

„Vajab ülevaatus“ võtab 20 punkti: tasub muuta, kuid raskusaste ei ole kõrge (vt [meetodi lehte](#)).

Seis valdkondade kaupa

Pooleldi täidetud lõik: osaliselt hinnatud kontroll

Ühendus ja sertifikaat

Ühenduse kontrollides märkusi ei leitud. Osaliselt hinnatud: ühenduse versioonid (TLS).



Osaliselt hinnatud

E-posti võltsimise kaitse

Vajab ülevaatus: võltsitud kirjade reegel (DMARC).



Vajab ülevaatus

Brauseri turvaseaded

Vaadatud brauseriseadetes märkusi ei leitud. Osaliselt hinnatud: skriptide reegel (CSP).



Osaliselt hinnatud

Avalik teave ja kontakt

Avaliku teabe kontrollides märkusi ei leitud. Osaliselt hinnatud: domeeni allkiri (DNSSEC).



Osaliselt hinnatud

Avalik kood

Vaadatud avalikus koodis märkusi ei leitud. Osaliselt hinnatud: saladused koodis, lähtekoodi kaardid, välised skriptid, JavaScripti teegid, sisselogimine.



Osaliselt hinnatud

Selles versioonis hindamata

Nende kohta tulemust ei ole.



Hindamata

Iga lõik tähistab üht kontrolli. „Märkusteta“ kehtib ainult tehtud kontrollide kohta.

Kokkuvõtte 1 leid vajab tööd. Leid ei näita, et keegi oleks ettevõtte lehte rünnanud. See näitab, mida tasub partnerilt küsida.

1 leid vajab ülevaatus. See valim ei tõenda kogu veebilehe turvalisust.

Mida partnerilt esimesena küsida

1. **Ettevõtte domeen ei palu postkastidel võltsitud kirju kinni pidada.** Küsi partnerilt, kas nende e-posti haldur teab, kes saab DMARC-i aruandeid avada (milline teenusepakkuja või konto need vastu võtab), ja loeb neid paar nädalat, kuni kõik õiged saatmisteened läbivad SPF- või DKIM-kontrolli sama domeeniga, mis on nähtaval saatjaväljal (From).

Kes partneri poolel ja kui kaua: e-posti haldur koos DNS-i halduriga · umbes 30 minutit e-posti teenusepakkuja või DNS-i halduriga iga DNS-muudatuse kohta, seejärel 2–4 nädalat aruannete lugemist enne iga rangemat sammu (umbes 2–4 nädalat kuni reeglina p=quarantine; hilisem üleminek reeglile p=reject, kui see valitakse, võtab kauem). · Millal: Kahe nädala jooksul

Kuidas parandust kontrollida: Kontrolli uuesti nime _dmarc.oej.ee TXT-kirjet: täpselt üks v=DMARC1 kirje, milles on p=quarantine või p=reject ja ei ole t=y väärtust.

→ Tehnilise lisa kaart A1

Kui partner on parandused teinud, tee tasuta korduskontroll (kuni 24.11.2026). Siis näed kirjalikult, kas parandused töötavad. DMARC-i puhul kinnitab korduskontroll sammu, milleni partner on selleks ajaks jõudnud (näiteks p=quarantine). Kas minna edasi reeglile p=reject, otsustab partner koos oma e-posti halduriga; see samm võib võtta kauem.

Leiud lähemalt

Vajab ülevaatus

Kahe nädala jooksul

Ettevõtte domeen ei palu postkastidel võltsitud kirju kinni pidada

DMARC · p=none

Mida see tähendab

Ettevõtte DMARC-reegel on ainult jälgimisrežiimis (p=none). See ei palu postkastidel kinni pidada kirju, mis kontrolli ei läbi, ka siis, kui saatjana on ettevõtte aadress.

Miks parandada

Kui keegi saadab kirja, kus saatjana on ettevõtte aadress, ei palu ettevõtte domeen postkastidel seda kinni pidada.

p=none ei palu DMARC-i kontrolli mitteläbinud kirja puhul lisameetmeid; vastuvõttev teenusepakkuja otsustab ise.

→ Tehnilise lisa kaart A1

Mis on korras

- ✓ HTTPS-i sertifikaat läbis ühenduse kontrolli (usaldatud väljastaja, õige nimi, kehtiv aeg).
- ✓ Avalehe krüpteerimata aadress (http://) suunab turvalisele aadressile.
- ✓ Leht saadab brauserile HTTPS-i kasutamise juhise (HSTS).
- ✓ Lubatud saatjate SPF-kirje on avaldatud ja selle süntaksis vigu ei leitud.
- ✓ E-kirjade allkirjavõtmed (DKIM) leiti kontrollitud selektorinimede alt.
- ✓ Kontrollitud vastus piirab, millised lehed tohivad seda raamis näidata (frame-ancestors või X-Frame-Options).
- ✓ Kontrollitud vastus keelab brauseril failitüüpi oletada (nosniff).
- ✓ Kontrollitud vastuses on viitaja reegel (Referrer-Policy).
- ✓ Brauseri õiguste reegel (Permissions-Policy) on avaldatud.
- ✓ Turvakontakti fail (security.txt) on avaldatud koos kontakti ja kehtivusajaga.
- ✓ E-posti ühenduse tõrgete aruannete aadress (TLS-RPT) on avaldatud.

Mida nägime, kuid täielikult ei hinnanud

- Õnnestunud ühendused: TLSv1.2, TLSv1.3; vanemate versioonide keelamist me ei katsetanud.
- DNS-resolver teatas ettevõtte domeeni võtmekirjete (DNSKEY) kohta allkirjastatud vastusest; allkirju me ise ei kontrollinud.
- Domeen ei avalda sertifikaatide väljastamise reegleid (CAA); see kontroll ei loe seda nõrkuseks.
- Valimisse võetud avalikus koodis ei leitud salajaste võtmete mustreid; muid faile me ei lugenud.
- Kontrollitud koodis ei leitud viiteid lähtekoodi kaartidele; kaardifaile me ei pärinud.
- Leht annab brauserile skriptide reegli (CSP); kontrollisime selles ainult mõnda ohtlikku skriptiseadet, mitte ülejäänud reegleid.
- Kontrollitud vastus saadab päise Access-Control-Allow-Origin: *. Brauser lubab siis mis tahes veebilehe skriptidel lugeda vastuseid päringutele, mis tehakse ilma küpsiste ja muude volitusteta; volitustega päringute vastuseid see ei ava. Päringute saatmist see päis ei piira. Seda väärtust see versioon ei hinda.
- Kontrollitud vastus nimetab serveri tarkvara (cloudflare); tarkvaraversioone see versioon ei hinda.
- MTA-STS-reegel on avaldatud testrežiimis (mode: testing); see aitab ühendusprobleeme leida, kuid ei palu saatjatel veel krüpteerimata ühendusest keelduda.
- Avalehe HTML-is deklareeritud skripte: 2, neist teistelt veebilehtedelt: 0. Me ei käivitanud ega hinnanud neid.
- Skriptide aadressides ei olnud teekide versioone nimetatud; mujal olevaid teeke me ei kontrollinud.

Ulatus ja piirangud

Vaatlusaeg: 25. oktoober 2026 kell 11:19 (Tallinna aeg, UTC+02:00)

Meetodi versioon: oej-security-check-2026-10-26 (reeglid public-security-v2, 29 kontrolli; DMARC RFC 9989, mai 2026).

Ulatus: avalehe vastused, e-posti ja DNS-i reeglid ning kaks tänapäevast TLS-i versiooni. Loeme HTML-i koodi käivitamata. Saadud tõendid ja puuduv teave on allpool. Sisselogimist, vorme, rakenduse ründeid, väliseid skripte ega nõusoleku eelset käitumist ei kontrollitud.

Kontrollide seis: 16 tehtud täielikult, 8 osaliselt, 5 tegemata. Hindamata ei tähenda viga.

Miks on 5 kontrolli hindamata: 2 vajab eraldi kokkulepitut ja lubatud testimist; 3 ei ole selles versioonis veel olemas. Hindamata ei tähenda ohtu ega turvalisust. „Märkusteta“ hõlmab 23 kontrolli, neist 8 osaliselt tehtud või loendavat; see ei tähenda, et 23 turvakontrolli on läbitud.

E-kirjade allkirjastamise võtmed (DKIM)

Otsisime nimesid, mida e-posti teenusepakkujad kõige sagedamini kasutavad (brevo1, brevo2, google, selector1, selector2, default, k1, s1):

- brevo1 — Võtme süntaksi kontrollis viga ei leitud. Piiratud parser ei tõenda kirjade autentimise toimimist. Küsi partnerilt, kas nende teenusepakkuja on kontrollinud päris allkirjastatud kirja.
- brevo2 — Võtme süntaksi kontrollis viga ei leitud. Piiratud parser ei tõenda kirjade autentimise toimimist. Küsi partnerilt, kas nende teenusepakkuja on kontrollinud päris allkirjastatud kirja.

Otsiti ainult ülal loetletud nimesid. Muid selektoreid ega kirjade allkirjade kehtivust ei kontrollitud.

Olulised piirangud

Hindamata ei tähenda viga. DNSSEC-i kohta on DNS-resolveri teave, mitte sõltumatu krüptograafiline kontroll. Vanade TLS-i versioonide keelamine, brauseri nõusoleku eelne käitumine, sisselogimine ja rakenduse pääsuõigused on tõendamata.

Selles versioonis hindamata

Neid olukordi me ei näita ka siis, kui need esinevad, seega nende puudumine sellelt lehelt ei tähenda, et kõik on korras:

- HSTS-i kehtivusaja pikkus: kontrolliti ainult, kas positiivne max-age on deklareeritud; lühikest kehtivusaega (näiteks alla kuue kuu) me ei näita.
- security.txt: hindame faili kuju ning välju Contact ja Expires vaatlusaja seisuga; kontakti kättesaadavus, näiliste 404-vastuste (soft 404) võrdlus, allkirjad ja täielik RFC-le vastavus jäävad kontrollimata.
- DNSSEC: domeeni allkirjastatust me ei hinda; allkirjastamata domeeni me ei näita.
- Päistes Server või X-Powered-By avaldatud tarkvaraversioone me ei hinda ega näita.

Veebilehte ei muudetud. Algsed tõendid hoitakse privaatsetl; räsld viitavad neile. Täpsemad tõendid on eraldi tehnilises lllas ja vastavas aruande-JSON-is.

Mida me ei vaadanud

- Peidetud failid serveris, näiteks varukoopiad: vajab eraldi kokkulepitud ja lubatud testimist.
- Rakenduse sisemine loogika ja sisestusvead: vajab eraldi kokkulepitud ja lubatud testimist.
- Kõpsiste ja jälgimise käitumine enne nõusolekut: selles versioonis veel ei ole.
- Sarnase nimega domeenid, mida keegi võiks klientide eksitamiseks kasutada: selles versioonis veel ei ole.
- Alamdomeenid, mis on kirjas sertifikaatide avalikes logides: selles versioonis veel ei ole.
- Selle kontrolli ulatusse ei kuulu sisselõgimine, vormide täitmine ega teistel domeenidel olevad teenused, näiteks makse- või broneerimissüsteemid.
- Serveri seadeid ja paigaldatud pluginate versioone ei saa selle kogumise põhjal kindlaks teha.

OEJ OÜ · Meelis Sootalu · info@oej.ee · +372 5846 0000

Kui partner vajab parandamisel abi, võib ta pöörduda OEJ poole – saadame hinnapakkumise ühe tööpäeva jooksul.

Tehniline lisa

Nende kaartide täielik sisu on tehnilise lisa PDF-failis.

A1 · E-posti võltsimise vastane reegel (DMARC)

Jagamiseks mõeldud koopia: autentimisandmete ja CSP ühekordsete tunnuste väärtused on varjatud. Algsed tõendid hoitakse privaatsetl. Räsld viitavad algsetele baitidele, mitte sellele jagamiskoopia.