

NÄIDISRAPORT · VÄLJAMÕELDUD ETTEVÕTE JA ANDMED

test-ou.ee

Indikatiivne kontroll domeeni, e-posti, veebilehe ja serveri avalikult nähtava seadistuse kohta.

Valmis: 26.09.2026 12:54

Hinnangu terviklikkus: Kavandatud kontrollid tehtud Skann: 7151f202

**Tõsine risk**
HEALTH SCORE

7

● Korras

9

● Soovitust

2

● Vajab
kinnitamist

2

● Probleemi

8

● Info

0

● Viga

AI-KOKKUVÕTE · REVIEWER KINNITATUD

Kokkuvõte

Terviseskoor on 36/100 ja üldhinnang „Tõsine risk“. Tähelepanu vajavad eelkõige www.test-ou.ee sertifikaadi nimevastavus, peagi aeguv sertifikaat, krüpteerimata FTP ning e-posti võltsimise kaitse nõrkused. Internetist on saavutatavad ka pordid 3306 ja 3389; nende taga olev teenus ja seadistus tuleb kiiresti üle kontrollida, kuid skaneerimine ei kinnitanud MySQL-i ega RDP kasutamist.

Piirang: Tegemist on välise tehnilise kontrolliga, mitte pentesti, auditi ega sertifitseerimisega. Pordid 3306 ja 3389 on küll internetist saavutatavad, kuid nende teenuse identiteet ja seadistus vajavad eraldi kontrolli. Skaneerimine ei loginud teenustesse ega vaadanud andmeid. DKIM-i ei leitud ainult levinud selectorite alt ning PHP versioon põhineb serveri teatatud päisel; mõlemad leiud vajavad vajadusel täiendavat kinnitamist.

Kõige olulisemad tegevused

Probleem

Leiu tase: Kõrge

Sertifikaat on välja antud teisele nimele

MIDA LEIDSIME?

Serveri sertifikaat ei kata kontrollitud aadressi. Tehnilises leius on nimed, millele sertifikaat kehtib.

MIDA TEHA?

Palu veebimajutajal väljastada sertifikaat, mis katab kõik kasutatavad aadressid (nt nii domeen.ee kui www.domeen.ee).

MIKS SEE ETTEVÕTTELE OLULINE ON?

Brauserid näitavad külastajatele hoiatust ja paljud lahkuvad. Tihti juhtub see www-ga või ilma www-ta aadressiga.

MIDA SEE LEID EI TÄHENDA?

See ei tähenda, et keegi liiklust pealt kuulaks. Tegu on peaaegu alati seadistusveaga.

Probleem

Leiu tase: Keskmine

SPF lubab praegu kõigil sinu nimel kirju saata

MIDA LEIDSIME?

SPF-kirje lõpeb reeglina +all. See ütleb, et iga server maailmas tohib sinu domeeni nimel kirju saata.

MIDA TEHA?

Palu e-posti halduril lisada SPF-i kõik päris saatjad ja muuta lõpp kujule -all või ~all. See on kiire ja oluline parandus.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Pettur saab saata sinu aadressilt võltsarve või maksepalve ja see läbib SPF-kontrolli. SPF ei kaitse praegu üldse.

MIDA SEE LEID EI TÄHENDA?

See ei tähenda, et võltskirju oleks juba saadetud. DKIM ja DMARC võivad osa neist siiski kinni püüda.

Soovitus

Leiu tase: Keskmine

Sertifikaat aegub mõne päeva pärast

MIDA LEIDSIME?

Veebisaidi turvasertifikaat aegub vähem kui nädala pärast.

MIDA TEHA?

Palu veebimajutajal kontrollida, et automaatne uuendamine töötab, või uuendada sertifikaat kohe käsitsi.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Kui uuendamine ebaõnnestub, näevad külastajad peagi hoiatust ja sait muutub paljudele kasutuskõlbmatuks.

MIDA SEE LEID EI TÄHENDA?

Sertifikaat kehtib veel. Automaatne uuendamine võib olla juba plaanis – skanner seda ei näe.

Soovitus

Leiu tase: Keskmine

FTP-teenus ei krüpteeri paroole ega faile

MIDA LEIDSIME?

Pordil 21 töötab FTP-server, mis ei paku krüpteerimist (AUTH TLS). Sisselogimine ja failid liiguvad võrgus loetaval kujul.

MIDA TEHA?

Palu IT-partneril või majutajal FTP välja lülitada või asendada see SFTP-ga. Kui FTP-d on vaja, luba ainult krüpteeritud ühendus ja vaheta paroolid.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Kes pääseb võrguliiklusele ligi (nt avalikus WiFi-s), võib näha FTP kasutajanime, parooli ja faile ning nende abil veebisaidile ligi pääseda.

MIDA SEE LEID EI TÄHENDA?

See ei tähenda, et paroole oleks juba varastatud. Skanner ei loginud sisse – ta küsis ainult, kas krüpteerimist pakutakse.

Soovitus

Leiu tase: Madal

Seadista DMARC, et võltskirjadega toime tulla

MIDA LEIDSIME?

Domeenil ega selle ülemistel domeenidel ei leitud DMARC-kirjet. DMARC ütleb vastuvõtjale, mida teha kirjadega, mis sinu nimel ei tundu ehtsad.

MIDA TEHA?

Palu e-posti halduril lisada DMARC-kirje. Alusta jälgimisrežiimist (p=none) koos aruannetega ja karmista seda, kui päris kirjad liiguvad korrektselt.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Ettevõtte nimel saadetud võltsarved ja maksepalved on väikeettevõtete puhul üks levinumaid pettusi. DMARC aitab neid tõkestada.

MIDA SEE LEID EI TÄHENDA?

See ei tähenda, et keegi oleks sinu nimel pettusi teinud. Kontrollitud on ainult domeeni avalik seadistus.

Soovitus

Leiu tase: Madal

Lülita välja vananenud TLS-versioonid

MIDA LEIDSIME?

Server lubab endiselt ühendusi vanade TLS 1.0 või 1.1 versioonidega, millel on teadaolevaid nõrkusi.

MIDA TEHA?

Palu veebimajutajal lubada ainult TLS 1.2 ja 1.3. Tavaliselt on see ühe rea muudatus serveri seadistuses.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Kaasaegsed brauserid neid versioone enam ei kasuta, kuid nende lubamine jätab ründajale võimaluse ühenduse kaitset nõrgendada.

MIDA SEE LEID EI TÄHENDA?

Tavaline külastaja kasutab juba uuemat versiooni. See ei tähenda, et ühendusi oleks pealt kuulatud.

Soovitus

Leiu tase: Madal

Suuna kõik külastajad turvalisele ühendusele

MIDA LEIDSIME?

Aadressil <http://> (ilma s-ita) avanev leht ei suuna külastajat automaatselt turvalisele <https://> aadressile.

MIDA TEHA?

Palu veebihalduril seadistada püsiv ümbersuunamine (301) [http](http://)-lt [https](https://)-le kõigil lehtedel.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Kes jõuab lehele vana lingi või käsitsi trükitud aadressi kaudu, võib jääda kaitsmata ühendusele. Seal sisestatud andmeid saab pealt kuulata.

MIDA SEE LEID EI TÄHENDA?

See ei tähenda, et HTTPS puuduks – turvaline leht on olemas. Puudu on ainult automaatne suunamine.

Soovitus

Leiu tase: Madal

Lase brauseril alati turvalist ühendust kasutada

MIDA LEIDSIME?

Veebileht ei palu brauseril meeles pidada, et sellele saidile tuleb alati minna turvalise ühendusega (HSTS puudub).

MIDA TEHA?

Palu veebihalduril lisada HSTS-päis. Alusta lühema kehtivusajaga ja pikenda seda, kui kõik lehed töötavad HTTPS-iga.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Kui külastaja trükitab aadressi ilma [https](https://)-ita, läheb esimene päring teele kaitsmata. Avalikus WiFi-võrgus saab pahatahtlik osapool seda hetke ära kasutada.

MIDA SEE LEID EI TÄHENDA?

See ei tähenda, et su leht oleks kaitsmata – HTTPS töötab. HSTS lisab ühe kaitsekihi juurde.

Soovitus

Leiu tase: Madal

Lisa veebilehele kaitse võõra koodi käivitamise vastu

MIDA LEIDSIME?

Veebilehel puudub sisuturbe poliitika (CSP), mis ütleb brauserile, kust tohib skripte ja muud sisu laadida.

MIDA TEHA?

Palu veebiarendajal CSP seadistada. Mõistlik on alustada jälgimisrežiimist, et vormid, maksed ja analüütika ei katkeks.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Kui lehele satub mõne vea kaudu võõras kood, aitab CSP selle käivitamist takistada ja külastajate andmeid kaitsta.

MIDA SEE LEID EI TÄHENDA?

See ei tähenda, et lehel oleks viga või et seda oleks rünnatud. CSP on lisakaitse, mitte parandus.

Soovitus

Leiu tase: Madal

Lisa küpsistele turvalipud

MIDA LEIDSIME?

Veebisait seab küpsiseid, millel puudub Secure-lipp (küpsis liigub ainult turvalise ühendusega) või sisselogimisküpsisel HttpOnly-lipp. Küpsiste nimed on tehnilises leius.

MIDA TEHA?

Palu veebiarendajal seada küpsistele Secure ja HttpOnly lipud ning sobiv SameSite väärtus. Enamasti on see veebiplatvormi seadetes.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Ilma nende lippudeta võib sisselogimisküpsis sattuda valedesse kätte ja keegi saab kasutaja nime all tegutseda.

MIDA SEE LEID EI TÄHENDA?

See ei tähenda, et küpsiseid oleks varastatud. Skanner vaatas ainult avalehe küpsiseid ega salvestanud nende sisu.

Soovitus

Leiu tase: Madal

Uuenda aegunud PHP versioon

MIDA LEIDSIME?

Veebiserver teatab PHP versioonist, mille ametlik turvatugi on lõppenud. Täpne versioon on tehnilises leius.

MIDA TEHA?

Palu veebimajutajal või arendajal viia sait toetatud PHP versioonile. Enne uuendamist testi, et leht ja pluginad töötavad.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Aegunud PHP-le ei tehta enam turvaparandusi. Uued vead jäävad parandamata ja veebileht (nt WordPress) muutub haavatavamaks.

MIDA SEE LEID EI TÄHENDA?

Mõned Linuxi distributsioonid parandavad vanu versioone ise edasi, seega leid vajab kinnitamist. Skanner näeb ainult serveri teatatud versiooni.

Vajab kinnitamist

Kontrollimise prioriteet: Kõrge

Peida MySQL-andmebaas internetist

MIDA LEIDSIME?

Serveri port 3306 on internetist avatud. Seda kasutab tavaliselt MySQL-andmebaas.

MIDA TEHA?

Palu IT-partneril kontrollida, mis pordil töötab. Andmebaasile peaksid ligi pääsema ainult sinu enda rakendused, mitte kogu internet.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Andmebaasis võivad olla kliendi- ja tellimusandmed. Internetist avatud andmebaasi paroole proovitakse pidevalt ära arvata.

MIDA SEE LEID EI TÄHENDA?

Skanner ei loginud sisse ega näinud andmeid. Jagatud majutuses võib see olla majutaja teenus.

Peida kaugtöölaud internetist

MIDA LEIDSIME?

Serveri port 3389 on internetist avatud. Seda kasutatakse tavaliselt Windowsi kaugtöölauaks (RDP).

MIDA TEHA?

Palu IT-partneril kohe kontrollida, mis pordil töötab. Kaugtöölaud peaks olema kättesaadav ainult VPN-i kaudu ja mitmeastmelise autentimisega.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Internetis avatud kaugtöölaud on üks sagedasemaid teid, kuidas lunavara ettevõttesse jõuab – paroole proovitakse ära arvata ööpäev läbi.

MIDA SEE LEID EI TÄHENDA?

Skanner ei kinnitanud, et seal töötab RDP, ega proovinud sisse logida. Kõrge prioriteet tähendab, et seda tasub kiiresti kontrollida.

TUGEVUSED

Mis töötab hästi



Brauserid usaldavad sertifikaati



Failitüüpide äraarvamine on keelatud

VÕRK

Internetist kättesaadavad pordid

IP	PORT	TAVAPÄRANE KASUTUS*	TEENUS TUVASTATUD?	HINNANG
203.0.113.10	21	FTP	Jah	Soovitus
203.0.113.10	80	HTTP	Ei	Info
203.0.113.10	443	HTTPS	Ei	Info
203.0.113.10	3306	MySQL	Ei	Vajab kinnitamist
203.0.113.10	3389	RDP	Ei	Vajab kinnitamist

* „Jah“ tähendab, et skanner tuvastas teenuse ise (FTP puhul tervitusrea ja krüpteerimise toe järgi, sisse logimata). „Ei“ puhul on teada ainult, et port võtab ühenduse vastu – nimetus näitab pordi tavapärasest kasutust.

Detailsemad leiud

Korras

Domeen suunab veebiserverile (IPv4)

DNS

Leiu tase: Infoks · Tõendi kindlus: kinnitatud

Tehniline tõendus

```
{
  "name": "test-ou.ee",
  "record_type": "A",
  "values": [
    "203.0.113.10"
  ]
}
```

Korras

Domeen võtab e-kirju vastu

DNS

Leiu tase: Infoks · Tõendi kindlus: kinnitatud

Tehniline tõendus

```
{
  "name": "test-ou.ee",
  "record_type": "MX",
  "values": [
    {
      "preference": 10,
      "exchange": "mail.test-ou.ee"
    }
  ]
}
```

Probleem

SPF lubab kõigil serveritel sinu nimel kirju saata

E-POST

Leiu tase: Keskmine · Tõendi kindlus: kinnitatud

SPF lubab praegu kõigil sinu nimel kirju saata

MIDA LEIDSIME?

SPF-kirje lõpeb reegluga +all. See ütleb, et iga server maailmas tohib sinu domeeni nimel kirju saata.

MIDA TEHA?

Palu e-posti halduril lisada SPF-i kõik päris saatjad ja muuta lõpp kujule -all või ~all. See on kiire ja oluline parandus.

Tehniline juhised IT-partnerile: Asenda +all väärtusega ~all või -all pärast seda, kui kõik tegelikud saatjad on kirjesse lisatud.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Pettur saab saata sinu aadressilt võltsarve või maksepalve ja see läbib SPF-kontrolli. SPF ei kaitse praegu üldse.

MIDA SEE LEID EI TÄHENDA?

See ei tähenda, et võltskirju oleks juba saadetud. DKIM ja DMARC võivad osa neist siiski kinni püüda.

Tehniline tõendus

```
{
  "name": "test-ou.ee",
  "records": [
    "v=spf1 a mx +all"
  ]
}
```

Soovitus

DMARC puudub

E-POST

Leiu tase: Madal · Tõendi kindlus: kinnitatud

Seadista DMARC, et võltskirjadega toime tulla

MIDA LEIDSIME?

Domeenil ega selle ülemistel domeenidel ei leitud DMARC-kirjet. DMARC ütleb vastuvõtjale, mida teha kirjadega, mis sinu nimel ei tundunud ehtsad.

MIDA TEHA?

Palu e-posti halduril lisada DMARC-kirje. Alusta jälgimisrežiimist (p=none) koos aruannetega ja karmista seda, kui päris kirjad liiguvad korrektselt.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Ettevõtte nimel saadetud võltsarved ja maksepalved on väikeettevõtete puhul üks levinumaid pettusi. DMARC aitab neid tõkestada.

MIDA SEE LEID EI TÄHENDA?

See ei tähenda, et keegi oleks sinu nimel pettusi teinud. Kontrollitud on ainult domeeni avalik seadistus.

Tehniline juhised IT-partnerile: Alusta DMARC kirjest p=none koos aruandlusega, vaata üle legitiimsed saatjad ning liigu kontrollitult quarantine või reject poliitika poole.

Tehniline tõendus

```
{
  "name": "_dmarc.test-ou.ee",
  "records": [],
  "checked_names": [
    "_dmarc.test-ou.ee"
  ]
}
```

Info

DKIM-allkirja ei leitud levinud nimedega

E-POST

Leiu tase: Infoks · Tõendi kindlus: kinnitatud

Kontrolli, kas e-kirjad on digitaalselt allkirjastatud

MIDA LEIDSIME?

Levinud nimede alt DKIM-võtit ei leitud. DKIM lisab igale kirjale digitaalse allkirja, mis tõendab, et kiri tuli sinu domeenilt.

MIDA TEHA?

Küsi e-posti teenusepakkujalt, kas DKIM on sisse lülitatud ja millise nime (selector) all võti avaldatud on.

MIKS SEE ETTEVÕTTELE OLULINE ON?

DKIM on koos SPF-i ja DMARC-iga üks kolmest e-posti põhikaitsest. Ilma selleta ei saa DMARC täielikult toimida.

MIDA SEE LEID EI TÄHENDA?

See ei tõesta, et DKIM puudub – võti võib olla avaldatud nime all, mida skanner ei tea. Seetõttu skoori ei vähendata.

Tehniline juhised IT-partnerile: Küsi saatva teenuse DKIM selectorit ja kontrolli kirjet <selector>._domainkey.<domeen>. Vajadusel luba allkirjastamine ja avalda võti.

Tehniline tõendus

```
{
  "name": "test-ou.ee",
  "provider": null,
  "selectors_found": []
}
```

Info

MTA-STS pole seadistatud

E-POST

Leiu tase: Infoks · Tõendi kindlus: kinnitatud

Kaalu meiliserverite vahelise krüpteerimise nõudmist

MIDA LEIDSIME?

Domeenil puudub MTA-STS kirje. MTA-STS ütleb teistele meiliserveritele, et sinu domeenile saadetud kirjad peavad liikuma krüpteeritult.

MIDA TEHA?

Kui e-post on äris olulises rollis, palu e-posti halduril seadistada MTA-STS koos TLS-RPT aruannetega. Microsoft 365 ja Google toetavad seda.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Ilma selleta saab pahatahtlik osapool teatud juhtudel sundida kirju liikuma krüpteerimata. See on olulisem suurema kirjavahetusega ettevõtetele.

MIDA SEE LEID EI TÄHENDA?

Suurem osa meiliserveritest krüpteerib kirju ka ilma MTA-STS-ita. See on täiendav kaitse, mitte viga.

Tehniline juhised IT-partnerile: Avalda <https://mta-sts.<domeen>/.well-known/mta-sts.txt> (alusta mode: testing), lisa _mta-sts TXT (v=STSV1; id=...) ja _smtp._tls TXT (v=TLSRPTv1; rua=mailto:...).

Tehniline tõendus

```
{
  "name": "test-ou.ee"
}
```

Info

CAA-kirje puudub

DNS

Piira, kes tohib sinu domeenile sertifikaate väljastada

MIDA LEIDSIME?

Domeenil puudub CAA-kirje, millega saab määrata, millised sertifikaadipakkujad tohivad sinu domeenile sertifikaate väljastada.

MIDA TEHA?

Kui tead, kes su sertifikaadid väljastab (nt Let's Encrypt), palu domeeni halduril lisada CAA-kirje ainult selle pakkujaga.

MIKS SEE ETTEVÕTTELE OLULINE ON?

CAA vähendab võimalust, et keegi saab sinu domeenile sertifikaadi mõnelt teiselt pakkujalt. See on lihtne lisameede.

MIDA SEE LEID EI TÄHENDA?

CAA puudumine on väga levinud ega tee sinu HTTPS-ühendust ebaturvaliseks.

Tehniline juhised IT-partnerile: Kui sertifikaatide väljastajad on teada, kaalu CAA kirje lisamist ja luba ainult kasutatavad sertifitseerimiskeskused.

Tehniline tõendus

```
{
  "name": "test-ou.ee",
  "records": []
}
```

Info

DNSSEC pole sisse lülitatud

DNS

Kaalu DNSSEC-i sisselülitamist

MIDA LEIDSIME?

Domeenil pole DNSSEC-i. DNSSEC allkirjastab domeeni DNS-kirjed, et neid ei saaks teel võltsida.

MIDA TEHA?

Küsi domeeni registripidajalt või DNS-teenuse pakkujalt, kas nad saavad DNSSEC-i sisse lülitada. Paljud pakuvad seda lihtsa seadena.

MIKS SEE ETTEVÕTTELE OLULINE ON?

DNSSEC kaitseb olukorra eest, kus külastaja suunatakse võltsitud DNS-vastusega vale serveri juurde.

MIDA SEE LEID EI TÄHENDA?

Enamikul domeenidel pole DNSSEC-i. Selle puudumine ei tähenda, et su domeeni oleks rünnatud.

Tehniline juhised IT-partnerile: Lülitada DNSSEC sisse DNS-teenuse pakkuja juures ja lase registripidajal avaldada DS-kirje. Kontrolli pärast muudatust valideerimist (nt dnsviz.net).

Tehniline tõendus

```
{
  "name": "test-ou.ee",
  "records": []
}
```

Korras

Turvaline ühendus töötab

SERTIFIKAAT

Leiu tase: Infoks · Tõendi kindlus: kinnitatud

Tehniline tõendus

```
{
  "protocol": "TLSv1.2",
  "host": "test-ou.ee",
  "port": 443,
  "certificate_sha256": "0000000000000000000000000000000000000000000000000000000000000000"
}
```

Soovitus

Sertifikaat kehtib veel 5 päeva

SERTIFIKAAT

Leiu tase: Keskmine · Tõendi kindlus: kinnitatud

Sertifikaat aegub mõne päeva pärast

MIDA LEIDSIME?

Veebisaidi turvasertifikaat aegub vähem kui nädala pärast.

MIDA TEHA?

Palu veebimajutajal kontrollida, et automaatne uuendamine töötab, või uuendada sertifikaat kohe käsitsi.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Kui uuendamine ebaõnnestub, näevad külastajad peagi hoiatust ja sait muutub paljudele kasutuskõlbmatuks.

MIDA SEE LEID EI TÄHENDA?

Sertifikaat kehtib veel. Automaatne uuendamine võib olla juba plaanis – skanner seda ei näe.

Tehniline juhised IT-partnerile: Kontrolli kohe automaatse uuendamise olekut ja vajadusel uuenda sertifikaat käsitsi.

Tehniline tõendus

```
{
  "not_after": "2026-10-01T09:54:54+00:00",
  "days_remaining": 5,
  "host": "test-ou.ee",
  "port": 443,
  "certificate_sha256": "0000000000000000000000000000000000000000000000000000000000000000"
}
```

Korras

Sertifikaat vastab domeeninimele

SERTIFIKAAT

Leiu tase: Infoks · Tõendi kindlus: kinnitatud

Tehniline tõendus

```
{
  "host": "test-ou.ee",
  "port": 443,
  "certificate_sha256": "0000000000000000000000000000000000000000000000000000000000000000"
}
```

Leiu tase: Infoks · Tõendi kindlus: kinnitatud

Tehniline tõendus

```
{
  "host": "test-ou.ee",
  "port": 443,
  "certificate_sha256": "0000000000000000000000000000000000000000000000000000000000000000"
}
```

Leiu tase: Madal · Tõendi kindlus: kinnitatud

Lülita välja vananenud TLS-versioonid

MIDA LEIDSIME?

Server lubab endiselt ühendusi vanade TLS 1.0 või 1.1 versioonidega, millel on teadaolevaid nõrkusi.

MIDA TEHA?

Palu veebimajutajal lubada ainult TLS 1.2 ja 1.3. Tavaliselt on see ühe rea muudatus serveri seadistuses.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Kaasaegsed brauserid neid versioone enam ei kasuta, kuid nende lubamine jätab ründajale võimaluse ühenduse kaitset nõrgendada.

MIDA SEE LEID EI TÄHENDA?

Tavaline külastaja kasutab juba uuemat versiooni. See ei tähenda, et ühendusi oleks pealt kuulatud.

Tehniline juhised IT-partneritele: Luba ainult TLS 1.2 ja 1.3 (nt nginx: ssl_protocols TLSv1.2 TLSv1.3; Apache: SSLProtocol -all +TLSv1.2 +TLSv1.3). Kontrolli pärast muudatust vanade klientide vajadust.

Tehniline tõendus

```
{
  "legacy_tls": {
    "TLSv1.0": true,
    "TLSv1.1": true
  },
  "host": "test-ou.ee",
  "port": 443,
  "certificate_sha256": "0000000000000000000000000000000000000000000000000000000000000000"
}
```

Leiu tase: Kõrge · Tõendi kindlus: kinnitatud

Sertifikaat on välja antud teisele nimele

MIDA LEIDSIME?

Serveri sertifikaat ei kata kontrollitud aadressi. Tehnilises leius on nimed, millele sertifikaat kehtib.

MIDA TEHA?

Palu veebimajutajal väljastada sertifikaat, mis katab kõik kasutatavad aadressid (nt nii domeen.ee kui www.domeen.ee).

Tehniline juhise IT-partnerile: Kontrolli DNS-i, virtuaalhosti/SNI seadistust ja sertifikaadi SAN nimesid; paigalda domeenile sobiv sertifikaat.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Brauserid näitavad külastajatele hoiatust ja paljud lahkuvad. Tihti juhtub see www-ga või ilma www-ta aadressiga.

MIDA SEE LEID EI TÄHENDA?

See ei tähenda, et keegi liiklust pealt kuulaks. Tegu on peaaegu alati seadistusveaga.

Tehniline tõendus

```
{
  "target": "www.test-ou.ee",
  "certificate_dns_names": [
    "test-ou.ee"
  ],
  "host": "www.test-ou.ee",
  "port": 443,
  "certificate_sha256": "0000000000000000000000000000000000000000000000000000000000000000"
}
```

Korras

Veebileht avaneb turvalise ühendusega

VEEBILEHT

Leiu tase: Infoks · Tõendi kindlus: kinnitatud

Tehniline tõendus

```
{
  "url": "https://test-ou.ee/",
  "status_code": 200,
  "server": "Apache/2.4.41 (Ubuntu)"
}
```

Soovitus

Kaitsmata aadressilt ei suunata turvalisele

VEEBILEHT

Leiu tase: Madal · Tõendi kindlus: kinnitatud

Suuna kõik külastajad turvalisele ühendusele

MIDA LEIDSIME?

Aadressil `http://` (ilma `s-ita`) avanev leht ei suuna külastajat automaatselt turvalisele `https://` aadressile.

MIDA TEHA?

Palu veebihalduril seadistada püsiv ümbersuunamine (301) `http`-lt `https`-le kõigil lehtedel.

Tehniline juhised IT-partnerile: Kontrolli suunamisahelat ja seadista sobiv HTTP 301/302/307/308 suunamine HTTPS-ile; testi vajalikud teekonnad.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Kes jõuab lehele vana lingi või käsitsi trükitud aadressi kaudu, võib jääda kaitsmata ühendusele. Seal sisestatud andmeid saab pealt kuulata.

MIDA SEE LEID EI TÄHENDA?

See ei tähenda, et HTTPS puuduks – turvaline leht on olemas. Puudu on ainult automaatne suunamine.

Tehniline tõendus

```
{
  "status_code": 200,
  "location": null
}
```

Soovitus

HSTS puudub

VEEBI TURVAPÄISED

Leiu tase: Madal · Tõendi kindlus: kinnitatud

Lase brauseril alati turvalist ühendust kasutada

MIDA LEIDSIME?

Veebileht ei palu brauseril meeles pidada, et sellele saidile tuleb alati minna turvalise ühendusega (HSTS puudub).

MIDA TEHA?

Palu veebihalduril lisada HSTS-päis. Alusta lühema kehtivusajaga ja pikenda seda, kui kõik lehed töötavad HTTPS-iga.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Kui külastaja trükitab aadressi ilma `https-ita`, läheb esimene päring teele kaitsmata. Avalikus WiFi-võrgus saab pahatahtlik osapool seda hetke ära kasutada.

MIDA SEE LEID EI TÄHENDA?

See ei tähenda, et su leht oleks kaitsmata – HTTPS töötab. HSTS lisab ühe kaitsekihi juurde.

Tehniline juhised IT-partnerile: Kui kogu sait ja vajalikud alamdomeenid töötavad korrektselt HTTPS-i kaudu, lisa sobiva `max-age` väärtusega `Strict-Transport-Security` päis. Enne `includeSubDomains` või `preload` kasutamist testi mõju eraldi.

Tehniline tõendus

```
{
  "header": "Strict-Transport-Security",
  "value": null,
  "host": "test-ou.ee"
}
```

Leiu tase: Madal · Tõendi kindlus: kinnitatud

Lisa veebilehele kaitse võõra koodi käivitamise vastu

MIDA LEIDSIME?

Veebilehel puudub sisuturbe poliitika (CSP), mis ütleb brauserile, kust tohib skripte ja muud sisu laadida.

MIDA TEHA?

Palu veebiarendajal CSP seadistada. Mõistlik on alustada jälgimisrežiimist, et vormid, maksed ja analüütika ei katkeks.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Kui lehele satub mõne vea kaudu võõras kood, aitab CSP selle käivitamist takistada ja külastajate andmeid kaitsta.

MIDA SEE LEID EI TÄHENDA?

See ei tähenda, et lehel oleks viga või et seda oleks rünnatud. CSP on lisakaitse, mitte parandus.

Tehniline juhised IT-partnerile: Kaardista lehel kasutatavad skriptid, stiilid ja välised allikad ning juuruta CSP esmalt report-only režiimis. Seejärel muuda poliitika jõustavaks pärast valepositiivide kontrollimist.

Tehniline tõendus

```
{
  "header": "Content-Security-Policy",
  "value": null,
  "host": "test-ou.ee"
}
```

Leiu tase: Infoks · Tõendi kindlus: kinnitatud

Tehniline tõendus

```
{
  "header": "X-Content-Type-Options",
  "value": "nosniff",
  "host": "test-ou.ee"
}
```

Leiu tase: Madal · Tõendi kindlus: kinnitatud

Lisa küpsistele turvalipud

MIDA LEIDSIME?

Veebisait seab küpsiseid, millel puudub Secure-lipp (küpsis liigub ainult turvalise ühendusega) või sisselogimisküpsisel HttpOnly-lipp. Küpsiste nimed on tehnilises leius.

MIDA TEHA?

Palu veebiarendajal seada küpsistele Secure ja HttpOnly lipud ning sobiv SameSite väärtus. Enamasti on see veebiplatvormi seadetes.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Ilma nende lippudeta võib sisselogimisküpsis sattuda valedesse kätesse ja keegi saab kasutaja nime all tegutseda.

MIDA SEE LEID EI TÄHENDA?

See ei tähenda, et küpsiseid oleks varastatud. Skanner vaatas ainult avalehe küpsiseid ega salvestanud nende sisu.

Tehniline juhised IT-partnerile: Sea kõigile küpsistele Secure, sessiooni- ja autentimisküpsistele HttpOnly ning sobiv SameSite (Lax/Strict). Kontrolli ka sisselogimise järel seatavaid küpsiseid.

Tehniline tõendus

```
{
  "host": "test-ou.ee",
  "cookies": [
    {
      "name": "PHPSESSID",
      "secure": false,
      "httponly": false,
      "samesite": null
    }
  ],
  "issues": [
    {
      "name": "PHPSESSID",
      "missing": "Secure"
    },
    {
      "name": "PHPSESSID",
      "missing": "HttpOnly"
    }
  ]
}
```

Soovitus

Server teatab aegunud PHP versioonist (PHP/7.4.33)

VEEBI TURVAPÄISED

Leiu tase: Madal · Tõendi kindlus: kinnitatud

Uuenda aegunud PHP versioon

MIDA LEIDSIME?

Veebiserver teatab PHP versioonist, mille ametlik turvatugi on lõppenud. Täpne versioon on tehnilises leius.

MIDA TEHA?

Palu veebimajutajal või arendajal viia sait toetatud PHP versioonile. Enne uuendamist testi, et leht ja pluginad töötavad.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Aegunud PHP-le ei tehta enam turvaparandusi. Uued vead jäävad parandamata ja veebileht (nt WordPress) muutub haavatavamaks.

MIDA SEE LEID EI TÄHENDA?

Mõned Linuxi distributsioonid parandavad vanu versioone ise edasi, seega leid vajab kinnitamist. Skanner näeb ainult serveri teatatud versiooni.

Tehniline juhised IT-partnerile: Vii sait toetatud PHP harule, testi rakendus ja pluginad eelnevalt koopias. Lülita ka `expose_php = Off`.

Tehniline tõendus

```
{
  "host": "test-ou.ee",
  "software": {
    "X-Powered-By": "PHP/7.4.33"
  },
  "php_version": "PHP/7.4",
  "php_end_of_life": "2022-11-28"
}
```

Info

security.txt puudub

VEEBILEHT

Leiu tase: Infoks · Tõendi kindlus: kinnitatud

Avalda kontakt turvaprobleemidest teatamiseks

MIDA LEIDSIME?

Veebisaidil puudub fail `security.txt`, kuhu saab kirja panna, kellele turvaprobleemist teada anda.

MIDA TEHA?

Lisa veebisaidile fail `/.well-known/security.txt` vähemalt ühe kontaktiga, näiteks Contact: `mailto:turva@sinudomeen.ee`.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Kui keegi leiab su saidil turvavea, teab ta nii kohe, kellega ühendust võtta – ja probleem jõuab sinuni enne ründajaid.

MIDA SEE LEID EI TÄHENDA?

See on hea tava, mitte turvaauk. Enamikul väikeettevõtetel seda faili veel pole.

Tehniline juhised IT-partnerile: Avalda `/.well-known/security.txt` väljadega Contact: ja Expires: (RFC 9116). Soovi korral lisa Preferred-Languages: et, en.

Tehniline tõendus

```
{
  "url": "https://test-ou.ee/.well-known/security.txt",
  "status_code": 404,
}
```

```
"has_contact": false
}
```

Info

Pordikontroll tehtud

PORDID

Leiu tase: Infoks · Tõendi kindlus: kinnitatud

Tehniline tõendus

```
{
  "ips_checked": [
    "203.0.113.10"
  ],
  "unchecked_ports": [],
  "unchecked_ips": []
}
```

Soovitus

FTP pordil 21 ei krüpteeri paroole ega faile

PORDID

Leiu tase: Keskmine · Tõendi kindlus: kinnitatud

FTP-teenus ei krüpteeri paroole ega faile

MIDA LEIDSIME?

Pordil 21 töötab FTP-server, mis ei paku krüpteerimist (AUTH TLS). Sisselogimine ja failid liiguvad võrgus loetaval kujul.

MIDA TEHA?

Palu IT-partneril või majutajal FTP välja lülitada või asendada see SFTP-ga. Kui FTP-d on vaja, luba ainult krüpteeritud ühendus ja vaheta paroolid.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Kes pääseb võrguliiklusele ligi (nt avalikus WiFi-s), võib näha FTP kasutajanime, parooli ja faile ning nende abil veebisaidile ligi pääseda.

MIDA SEE LEID EI TÄHENDA?

See ei tähenda, et paroole oleks juba varastatud. Skanner ei loginud sisse – ta küsis ainult, kas krüpteerimist pakutakse.

Tehniline juhised IT-partnerile: Eelista SFTP-d (SSH). Kui FTP on vajalik, luba FTPS ja nõua seda (nt vsftpd: ssl_enable=YES, force_local_logins_ssl=YES). Vaheta FTP-kontode paroolid.

Tehniline tõendus

```
{
  "ip": "203.0.113.10",
  "port": 21,
  "expected_service": "FTP",
  "service_fingerprinted": true,
  "verification_state": "service_confirmed",
  "ftp_tls_supported": false
}
```

Info

Port 80 (HTTP) on internetist avatud

PORDID

Leiu tase: Infoks · Tõendi kindlus: kinnitatud

Tehniline tõendus

```
{
  "ip": "203.0.113.10",
  "port": 80,
  "expected_service": "HTTP",
  "service_fingerprinted": false
}
```

Info

Port 443 (HTTPS) on internetist avatud

PORDID

Leiu tase: Infoks · Tõendi kindlus: kinnitatud

Tehniline tõendus

```
{
  "ip": "203.0.113.10",
  "port": 443,
  "expected_service": "HTTPS",
  "service_fingerprinted": false
}
```

Vajab kinnitamist

Port 3306 (MySQL) on internetist avatud

PORDID

Kontrollimise prioriteet: Kõrge · Tõendi kindlus: kinnitatud

Peida MySQL-andmebaas internetist

MIDA LEIDSIME?

Serveri port 3306 on internetist avatud. Seda kasutab tavaliselt MySQL-andmebaas.

MIDA TEHA?

Palu IT-partneril kontrollida, mis pordil töötab. Andmebaasile peaksid ligi pääsema ainult sinu enda rakendused, mitte kogu internet.

Tehniline juhis IT-partnerile: Kinnita teenus. Kui pordil töötab MySQL, piira ligipääs ainult vajalikele rakendusserveritele või turvalisele privaatvõrgule.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Andmebaasis võivad olla kliendi- ja tellimusandmed. Internetist avatud andmebaasi parooli proovitakse pidevalt ära arvata.

MIDA SEE LEID EI TÄHENDA?

Skanner ei loginud sisse ega näinud andmeid. Jagatud majutuses võib see olla majutaja teenus.

Tehniline tõendus

```
{
  "ip": "203.0.113.10",
  "port": 3306,
  "expected_service": "MySQL",
  "service_fingerprinted": false,
  "verification_state": "requires_verification"
}
```

Vajab kinnitamist

Port 3389 (RDP) on internetist avatud

PORDID

Kontrollimise prioriteet: Kõrge · Tõendi kindlus: kinnitatud

Peida kaugtöölaud internetist

MIDA LEIDSIME?

Serveri port 3389 on internetist avatud. Seda kasutatakse tavaliselt Windowsi kaugtöölauaks (RDP).

MIDA TEHA?

Palu IT-partneril kohe kontrollida, mis pordil töötab. Kaugtöölaud peaks olema kättesaadav ainult VPN-i kaudu ja mitmeastmelise autentimisega.

Tehniline juhis IT-partnerile: Kinnita teenus. Kui tegemist on RDP-ga, eelista VPN-i või muud ligipääsuvära, piira lähteadresse ning kasuta tugevat autentimist ja MFA-d.

MIKS SEE ETTEVÕTTELE OLULINE ON?

Internetis avatud kaugtöölaud on üks sagedasemaid teid, kuidas lunavara ettevõttesse jõuab – paroole proovitakse ära arvata ööpäev läbi.

MIDA SEE LEID EI TÄHENDA?

Skanner ei kinnitanud, et seal töötab RDP, ega proovinud sisse logida. Kõrge prioriteet tähendab, et seda tasub kiiresti kontrollida.

Tehniline tõendus

```
{
  "ip": "203.0.113.10",
  "port": 3389,
  "expected_service": "RDP",
  "service_fingerprinted": false,
  "verification_state": "requires_verification"
}
```

PIIRANGUD

Raporti piirangud

Kontroll kasutab ainult väliseid ja mitteinvasiivseid meetodeid. See ei sisalda autentimist, eksploateerimist, paroolikatseid ega täielikku portide või rakenduste turvatesti.

Health Score on Kyberturve.ee indikatiivne sisemine näitaja. See ei ole ründe tõenäosus ega objektiivne turvalisuse protsent. Puudulikult kontrollitud tulemusele ei anta terviklikku hinnangut. See arvestab ka tõendi tugevust ega käsitle pelgalt avatud TCP porti kinnitatud teenuse või haavatavusena. See ei ole pentesti, auditi, vastavushinnangu ega sertifikaadi tulemus. Tulemusi tuleb tõlgendada koos süsteemi tegeliku konteksti ja omaniku konfiguratsiooniga.

[k] NÄIDISRAPORT – ettevõtte, domeen ja leiud on väljamõeldud · kyberturve.ee · info@kyberturve.ee · Skanni ID 7151f202-a75b-4a1f-9a3b-c71fb5feb443