Riigi Infosüsteemi Amet

Küberturbe taseme tõstmise teekaardi metoodika

2026

Versioon	*Koostamise aeg*	*Muutus*
4.1	*02.07.2026*	*Täiendatud vastavalt kommentaaridele*
4.2	*05.08.2026*	*Lisatud logod, muudetud pealkirja, täpsustatud kasutust*

Käesolev dokument on juhend „Küberturbe taseme tõstmise teekaardi" koostamiseks. Metoodika toetab organisatsioonide küberturbe olukorra kaardistamist, seda on võimalik kasutada organisatsioonidel endil ning ka teenusepakkujatel. 2026. aastal avatava toetusmeetme „Küberturbe taseme tõstmise toetus" (https://www.riigiteataja.ee/et/akt/121072026010) kontekstis on tegemist määruses nimetatud metoodikaga.

Tegemist on uuendatud ja täiendatud metoodikaga, mis võtab arvesse varasema toetusmeetme „Küberpööre" teekaardi koostajate ja tellijate tagasisidet. Metoodikasse on lisatud komponendid, mis aitavad Küberturvalisuse seaduse (edaspidi KüTS) subjektidel liikuda seaduses nõutud küberturbe taseme saavutamise suunas.

Sisukord

1. Sissejuhatus 2
2. Metoodika 3
3. Teekaardi skoop 4
   3.1. Vajalike turvameetmete ja nõuete tuvastamine 4
   4.2. IT keskkonna turvalisuse hindamine 4
   4.3. Teekaardi koostamise tegevuste kirjeldus 5
4. Tulem 8

1. Sissejuhatus

2026. aasta alguses hakkas kehtima uus Küberturvalisuse seaduse (KüTS)[1] versioon, mis võttis üle NIS2 direktiivi[2] nõuded. KüTS-i uues versioonis on subjektide ringi oluliselt laiendatud, samuti on lisandunud mitmeid täiesti uusi sektoreid. Täpsustati ja lisati täiendavaid kohustusi seaduse subjektidele küberturvalisuse tagamisel ning intsidentidest teavitamisel.

Toetus on mõeldud organisatsioonidele, kellele hakkasid 2026. aastal kehtima KüTS-ist tulenevad uued kohustused (uued subjektid). Toetuse abil saab tellida küberturvalisuse teekaardi ning selle põhjal ellu viia vajalikud arendustegevused, et viia infoturbe korraldus vastavusse seaduse nõuetega. Teekaardi loomise käigus selgitatakse välja ärinõuded ja KüTS-ist tulenevad nõuded küberturvalisusele, pannakse kokku nõuetele vastav turvameetmete komplekt ning hinnatakse olemasolevate meetmete rakendatuse määra. Samuti antakse hinnang organisatsiooni küberturvalisuse hetkeseisule, tuuakse välja puudujäägid ning küberturbe taseme tõstmiseks vajalikud tegevused.

Teekaart koosneb kahest osast – olemasoleva IT keskkonna turvalisuse hindamisest ja vajalike turvameetmete ja nõuete tuvastamisest. Mõlemad osad toetavad teineteist – IT keskkonna turvalisuse hindamine aitab tuvastada tehnilised nõrkused ja seadistusvead, vajalike meetmete ja nõuete tuvastamine aitab tagada pikaajalise organisatsioonile sobiva küberturbe taseme saavutamise ja hoidmise.

[1] Küberturvalisuse seadus https://www.riigiteataja.ee/akt/130122025015?leiaKehtiv
[2] NIS2 direktiiv https://eur-lex.europa.eu/eli/dir/2022/2555

2. Metoodika

Teekaardi koostamise soovituslik tegevuste järjekord

1. Kokkuleppe sõlmimine organisatsiooni ja teekaardi koostaja vahel;
2. Organisatsiooni küberküpsustaseme esmane hindamine ja skoobi ettevalmistamine (suhtlus kliendiga, vajadusel küsitlusleht, vms);
3. IT-keskkonnaga tutvumine (nt olemasoleva IT-dokumentatsiooni läbivaatus jmt);
4. Vajalike turvameetmete ja nõuete tuvastamine:
    - Organisatsioonile kehtivate KüTS-i nõuete ja kohustuste tuvastamine ja kaardistamine;
    - Organisatsioonile sobivate raamistike/standardite tuvastamine ja organisatsiooni juhtkonnale tutvustamine;
    - Vajalike Esmaste turvameetmete määramine, vajadusel E-ITS-i või ISO27001 tegevuste läbiviimine IMR-i või SoA koostamiseks.
5. IT keskkonna turvalisuse hindamine:
    - Tehnilised testid, mis ei vaja kohapeale käiku (välisperimeeter, veebilehed jne);
    - Kohapealne ülevaatus, sh vajalikud tehnilised testid.
6. Teekaardi koostamine, 1 aasta tegevuskava loomine;
7. Teekaardi esitlemine organisatsiooni juhtkonnale;

Juhul, kui selgub, et KüTS-ist nõudeid ei tulene võib siiski edasi minna sobivate raamistike/standardite tuvastamisega. Kõik KüTS subjektid peavad rakendama Esmased turvameetmed, kui lisaks tehakse E-ITS või ISO võib Esmaste infoturbe meetmete määramise ja valitud standardi meetmete määramise teha samaaegselt, kuid peab olema võimalik näidata, et Esmased infoturbemeetmed on määratud. 4. ja 5. sammu võib ära vahetada või viia need ellu paralleelselt.

3. Teekaardi skoop

3.1. Vajalike turvameetmete ja nõuete tuvastamine

1. Organisatsioonile kehtivate KüTS kohustuste tuvastamine;
2. Sobiva küberturvalisuse raamistiku/standardi otsust mõjutavate ärinõuete tuvastamine;
3. Esmaste turvameetmete asjakohasuse ja rakendatavuse hindamine;
4. Koos organisatsiooni juhtkonnaga sobiva raamistiku/standardi valimine;
5. Vajadusel E-ITS või ISO27001 metoodika standardi tegevused IMR-i või SoA koostamiseks.

Projekti mahtu hinnates soovitame teekaardi koostajate tuvastada, kas E-ITS/ISO27001 standardite tegevuste läbiviimiseks on juba olemas piisava täpsusega varade kaardistus, äriprotsesside kirjeldused ja riskide hindamine või peab see olema töö osa.

4.2. IT keskkonna turvalisuse hindamine

1. Avalikust internetist potentsiaalsete rünnete sooritamiseks kasuliku informatsiooni kogumine ja tehniliste nõrkuste leidmine;
2. Avalikud veebilehed;
3. Tulemüürid ja tulemüürireeglite ülevaatus;
4. Kaugligipääsud – VPN tunnelid, RDP, VNC jms;
5. Võrgus olevad seadmed ja teenused;
6. Pilveteenused (Microsoft356, Google for Business, Azure, AWS, Riigipilv jms);
7. Identiteedihaldus (Entra ID, AD jms) ja privilegeeritud kontode haldus;
8. Vajadusel erisüsteemide võrgud – tööstusautomaatika, hooneautomaatika, läbipääsusüsteemid, videovalve jms;
9. Füüsilise turvalisuse hindamine;
10. Olemasoleva IT dokumentatsiooniga tutvumine ja selle asjakohasuse hindamine, riskianalüüsi ja taasteplaanide olemasolu ja ülevaatus.

Teekaardi koostaja võib IT keskkonna turvalisuse hindamise skoopi vähendada, seda põhjendades (näiteks juhul, kui organisatsioon ei kasuta pilveteenuseid või tal puuduvad serverivõrgud, tööstusautomaatika vms). Sel juhul tuleb põhjendada teekaardi lõpparuandes, miks skoopi vähendati.

4.3. Teekaardi koostamise tegevuste kirjeldus

Organisatsioonile kehtivate KüTS kohustuste tuvastamine ja tutvustamine

Teekaardi koostaja ülesanne on selgitada välja, millised on KüTS-ist tulenevad kohustused organisatsioonile ning tutvustama neid organisatsiooni juhatusele. Sealhulgas tuleb tuvastada, kas organisatsioon peab rakendama esmaseid turvameetmeid ja ISO27001 standardit või Eesti infoturbestandardit.

Sobiva küberturvalisuse raamistiku/standardi otsust mõjutavate ärinõuete tuvastamine

Teekaardi koostaja ülesanne on selgitada välja, kas organisatsioonil on ärinõudeid, mida tuleks arvesse võtta sobiva infoturbe raamistiku/standardi valimisel. Näiteks võib organisatsioon kuuluda rahvusvahelisse kontserni või tegutseda rahvusvahelistel turgudel ja sellisel juhul võib olla otstarbekas valida rahvusvaheliselt tuntud standard. Kohalike organisatsioonide jaoks, kes soovivad tasuta standardit või kes kuulub riigile või kohalikule omavalitsusele, võib olla sobivam E-ITS. Ka olukorras, kus KüTS nõuab ainult Esmaste turbemeetmete rakendamist tuleb tuvastada, kas eksisteerib ärinõudeid, mis muudavad täiendavate meetmete või standardi rakendamise mõistlikuks.

Esmaste turvameetmete asjakohasuse ja rakendatavuse hindamine
Teekaardi koostaja ülesanne on hinnata iga Esmaste turvameetmete meedet ning hinnata koos organisatsiooniga, millised meetmed ei ole asjakohase või rakendatavad ning dokumenteerida meetmetega seotud otsused.

Koos organisatsiooni juhtkonnaga sobiva raamistiku/standardi valimine

Kui KüTS-i või ärinõuetest tulenevalt peab organisatsioon kasutusele võtma täiendavalt infoturbe raamistiku, siis on teekaardi koostaja ülesanne on pakkuda välja sobiv standard, mis täidab seadusest tulenevad nõuded ning on tuvastatud ärinõuete poolest teekaardi koostaja hinnangul organisatsioonile sobivaim.

Vajadusel E-ITS või ISO27001 metoodika standardi tegevused IMR-i või SoA koostamiseks

Teekaardi koostaja ülesanne on läbi viia tegevused – dokumentide läbivaatamine, intervjuud, analüüsid jmt, mis on vajalikud E-ITS-i või ISO27001 metoodika järgi turvameetmete nimekirja koostamiseks (IMR või SoA). Muu hulgas peab olema välja toodud, mis mahus meetmed on juba rakendatud.

E-ITS-i puhul leiab tasuta abivahendeid ja materjale E-ITS-i portaalist: https://eits.ria.ee/et. Samuti tasub tutvuda erinevate E-ITS profiilidega – nt kaugkütte ettevõtete, vee-ettevõtete ja perearstide jaoks on loodud näidised.

Avalikust internetist potentsiaalsete rünnete sooritamiseks informatsiooni kogumine ja tehniliste nõrkuste leidmine.

Teekaardi koostaja ülesanne on selgitada välja, mil määral on võimalik potentsiaalseteks rünneteks kasulikku infot ja tehnilisi nõrkusi leida avalikest allikatest. Muuhulgas peab koostaja skaneerima organisatsiooni avalikku arvutivõrku (ehk väliseid staatilisi IP aadresse, kõiki TCP porte ning 100 enimkasutatavad UDP

porti), et leida potentsiaalseid nõrkusi ja seadistusvigu. Skaneerimise tulemused tuleb lisada Teekaardile lisana.
Samuti tuleb tuvastada, kas organisatsiooni domeenidega seotud kasutajakontod/e-postiaadressid ja paroolid on lekkinud ning lekkinud kontod teekaardis välja tuua.

Avalikud veebilehed

Veebilehtede puhul on teekaardi koostaja ülesanne kontrollida, kas kodulehe tarkvara ja pistikprogrammid (plugins) on tootja poolt toetatud, uuendatud viimasele versioonile ja ei sisalda teadaolevaid nõrkusi. Samuti kontrollib pakkuja, et kodulehe seadistused on turvalised ja administreerimise õigusega kontosid on mõistlikul hulgal ning nende kasutajad on tuvastatavad.

Tulemüürid ja tulemüürireeglite ülevaatus

Teekaardi koostaja ülesandeks hinnata tulemüüride tehnilist sobivust, kontrollida kas need on tootja poolt toetatud ja viimasele tarkvaraversioonile uuendatud ning ei sisalda teadaolevaid nõrkusi. Hinnata tulemüürireeglite asjakohasust ja vastavust parimatele praktikatele, sh kasutajakontode haldus. Teekaardi koostaja kontrollib, kas organisatsiooni võrk on jagatud erinevateks võrgusegmentideks ning kas segmentide vaheline liiklus on lubatud minimaalses vajalikus mahus. Juhul, kui organisatsioonil on mitmeid tulemüüre (erinevad asukohad või erinevate segmentide jaoks), tuleb kõik tulemüürid läbi vaadata või põhjendada, miks osade läbivaatamine pole otstarbekas.

Teekaardi koostaja ülesandeks on samuti kontrollida, kas on võimalik saavutada kontorivõrgust autoriseerimata ligipääs tundlikes ja halduskriitilistes võrkudes asuvate süsteemideni.

Kaugligipääsud

Teekaardi koostaja ülesandeks on kontrollida, kas nii töötajate, koostööpartnerite kui ka haruüksuste kaugligipääsud kontori- ja kriitiliste äriteenuste osutamiseks vajalikele infosüsteemidele vastavad üldlevinud headele tavadele. Samuti peab pakkuja võimaluse korral tuvastama dokumenteerimata kaugligipääsud.

Võrgus olevate seadmete ja teenuste turvalisuse hindamine.

Teekaardi koostaja ülesandeks on hinnata erinevates võrkudes asuvate tööjaamade, serverite ja võrku ühendatud seadmete turvalisust puudutavate seadistuste vastavust üldlevinud headele tavadele ja (selle olemasolul) organisatsiooni infoturbepoliitikale (näiteks viirusetõrje olemasolu ja signatuuride uuendamine, operatsioonisüsteemi turvapaikade paigaldamine, kõvaketta krüpteerimise kasutamine, keelatud tarkvara olemasolu, ebavajalike võrguteenuste olemasolu, administraatori konto ebaturvaline kasutamine, aegunud (rakendus)tarkvara kasutamine, võrguseadmete jt seadmete püsivara uuendamine jne).

Eriline tähelepanu pöörata administraatorite ja võtmeisikute tööjaamadele ning serveritele, mille kaudu on võimalik mõjutada ärikriitilisi infosüsteeme.

Wi-Fi võrkude puhul on teekaardi koostaja ülesanne kontrollida, kas nendest võrkudest on võimalik saavutada lubamata ligipääs ärikriitilistes võrkudes asuvate

süsteemideni. Lisaks hinnata, kas potentsiaalsel ründajal on võimalik sisevõrku saamiseks ära kasutada avalikes ruumides asuvaid WiFi tugijaamade kaabliühendusi või võrgupesasid.

Pilveteenused (Microsoft365, Google for Business, Azure, AWS, Riigipilv jms)

Teekaardi koostaja ülesandeks on hinnata identiteedi- ja ligipääsuhalduse küpsust, kontrollides mitmikautentimise rakendamist kõikidel kontodel ning privilegeeritud kasutajate arvu ja halduspraktika vastavust parimatele praktikatele. Hinnata, kas on Microsoft Secure Score või Google Security Health või teiste keskkondade vastavaid soovitusi, mida organisatsioon peaks esmajärjekorras rakendama.

Identiteedihaldus (Entra ID, AD jms) ja privilegeeritud kontode haldus

Teekaardi koostaja ülesandeks on hinnata Entra ID ja Active Directory jt sarnaste süsteemide konfiguratsiooni turvalisust, kontrollides privilegeeritud kasutajate ja gruppide halduspraktikat, paroolipoliitikate asjakohasust ning tavakasutajakontode asjakohasust ja paroolipoliitikaid. Erilist tähelepanu pöörata hübriid- ja pilve sünkroniseeritud lahenduste korral pikalt kasutuses olnud kontodele, sh teenuskontodele.

Erisüsteemide võrgud

Teekaardi koostaja ülesanne on hinnata, kas erisüsteemide võrgud või seadmed on ülejäänud organisatsiooni võrkudest ja internetist piisavalt eraldatud, kas võimalikud teenuseosutajate kaughalduslahendused on piisavalt turvalised ning kas neid on vähim võimalik arv. Samuti veenduda, kas kaugligipääs võimaldatakse hoolduspartneritele ainult kokkulepitud hooldustööde ajaks või on neil ligipääs püsivalt olemas. Võimaluse korral hinnata erisüsteemide võrkudes olevate tööjaamade seadistusi käsitsi või vaatluse teel. Automaattööriistade kasutamine on tungivalt mittesoovitatud ja kõik tegevused tuleb organisatsiooni esindajaga eraldi kokku leppida ning selgitada tegevuste võimalikku riski organisatsioonile.

Füüsilise turvalisuse hindamine

Teekaardi koostaja ülesandeks on hinnata, kas IT süsteemide, seadmete, oluliste seadmekappide, serveriruumide jne kaitseks on rakendatud piisavaid füüsilisi turvameetmeid, mis välistaks autoriseerimata isikute ligipääsu nendele (sh ka organisatsiooni enda töötajate). Füüsilise turvalisuse hindamine tuleb teekaardi koostajatel läbi viia füüsiliselt koha peal, vaatluse teel.

IT dokumentatsiooniga tutvumine ja selle asjakohasuse hindamine

Teekaardi koostaja ülesandeks on tutvuda olemasoleva IT dokumentatsiooniga ning hinnata selle asjakohasust. Kontrollida, kas ärikriitiliste infosüsteemide jaoks on loodud piisavad taasteplaanid ning anda hinnang, kas taasteplaanid on sobivad, et nende abil oleks vajadusel võimalik reaalselt süsteeme taastada.

4. Tulem

Projekti lõpuks esitab teekaardi koostaja tellijale “Küberturbe taseme tõstmise teekaardi” kirjaliku dokumendi ehk raporti koos lisadega. Lisadeks võivad olla näiteks Esmaste turvameetmete hindamise tabel, E-ITS-i või ISO 27001 metoodika järgi kohustuslikud dokumendid, sh IMR või SoA, võrgu skaneerimise raportid ja erinevate tööriistade mahukad väljundid.

Juhul, kui käesolevat metoodikat kasutatakse toetusmeetme „Küberturbe taseme tõstmise toetus“ teekaardi jaoks, peab dokument peab vastama alltoodud struktuurile. Nii metoodika kui ka näidisraport on kättesaadav EISi veebilehelt. Teekaardi koostajal on soovituslik kasutada RIA poolt loodud teekaardi vormi.

Teekaardi ülesehitus

1. Sissejuhatus ja lühikokkuvõte
2. Teostatud tööde metoodika ja skoop
3. KüTS-ist tulenevad kohustused ja ärinõuded
4. Vajalikud turvameetmed ja nõuded
    a. Organisatsioonile sobiv infoturbestandard
    b. Esmased turvameetmed ja standardi metoodika tegevuste ülevaade
5. IT keskkonna turvalisuse hindamine
    a. Hindamise läbiviimiseks kasutatud metoodika ja tööriistad
    b. Skoop
    c. Organisatsiooni IT-keskkonna üldine kirjeldus
    d. Tähtsamad leiud (iga ilmnenud probleemi kohta peab aruanne sisaldama vähemalt järgmist):
    - viide komponendile või süsteemile
    - probleemi kirjeldus
    - juhend probleemi esilekutsumiseks
    - hinnang probleemi tõsidusele (risk)
    - soovitused ja ettepanekud probleemi kõrvaldamiseks
    - lahendamise prioriteet ja keerukus
    e. Järeldused ja ettepanekud
6. Tegevuskava.

Tegevuskava kirjeldab, milliste tegevustega saab organisatsioon 1 aasta jooksul kõige paremini liikuda KüTS-ist tulenevate nõuete täitmise suunas (nt valitud standardi metoodika kohaselt infoturbemeetmete elluviimine ja auditeerimine, juhtide ja töötajate koolitamine jms) ja IT keskkonna turvalisuse hindamisel välja toodud leidude parandamine.
Tegevuskava peab sisaldama organisatsiooni jaoks vajalikku tehtavate tööde nimekirja, millele oleks võimalik võtta hinnapakkumine. Näiteks soovitus vahetada nõrka vaikeparooli pole eraldi mõttekas lisada aastase tegevuskava hulka, sest see tuleks ära teha kohe, ilma hinnapakkumist võtmata. Tegevuskava põhieesmärk on pakkuda organisatsioonile head sisendit, milliseid arendustöid oleks tal vaja kas ise teha või sisse osta.