EUROOPA LIIT

NIS2 DIREKTIIV

(Direktiiv EL 2022/2555)

Meetmed küberturvalisuse ühtlaselt kõrge taseme tagamiseks kogu liidus

Eestikeelne kokkuvõte CISO-dele ja vastavusjuhtidele

Dokumendi andmed

Väli	Väärtus
Ametlik nimetus	Direktiiv (EL) 2022/2555
Vastuvõtmise kuupäev	14. detsember 2022
Avaldamise kuupäev	27. detsember 2022 (ELT L 333/80)
Jõustumise kuupäev	16. jaanuar 2023
Riiklikku õigusse ülevõtmise tähtaeg	17. oktoober 2024
Kehtetuks tunnistatud õigusakt	Direktiiv (EL) 2016/1148 (NIS1)

> Käesolev dokument on ELi NIS2 direktiivi (14. detsember 2022) mitteametlik kokkuvõte ega ole ametlik tõlge. Siduva tõlgenduse saamiseks pöörduge ametliku teksti poole: ELT L 333/80, 27.12.2022.

Sisukord

1. Juhtkonna kokkuvõte

NIS2 direktiiv (direktiiv EL 2022/2555), mille Euroopa Parlament ja nõukogu võtsid vastu 14. detsembril 2022, on ELi üldine küberturvalisuse baasdirektiiiv. See tunnistab kehtetuks ja asendab varasema NIS1 direktiivi 2016/1148 alates 18. oktoobrist 2024.

Läbivaatamised näitasid, et kuigi NIS1 aitas liidus küberturvalisuse vastupidavusvõimet tõsta, osutus see praeguste ja tulevaste küberturvalisuse ohtudega toimetulekuks ebapiisavaks. NIS2 laiendab kohaldamisala oluliselt, kehtestab ühtsed kriteeriumid, tugevdab riskijuhtimis- ja teatamiskohustusi ning näeb ette tõhusamad täitmise tagamise sätted.

Direktiivi viis sammast

1. **Laiendatud kohaldamisala**: rohkem sektoreid ja ettevõtteid reguleerimise alla.
2. **Tugevdatud riskijuhtimine**: artiklis 21 kohustuslikuks tehtud 10 minimaalsest tehnilist ja organisatoorset meedet.
3. **Kiire ja mitmeastmeline intsidentidest teatamine**: 24-tunnine varajane hoiatus, 72-tunnine intsidentide teatis, 1-kuuline lõpparuanne.
4. **Juhtorgani vastutus**: tippjuhtkonda saab isiklikult vastutusele võtta.
5. **Hoiatavad karistused**: haldustrahvid kuni 2% iga-aastasest ülemaailmsest käibest või 10 miljonit eurot.

2. Eesmärk ja õiguslik alus

Direktiivi õiguslikuks aluseks on **Euroopa Liidu toimimise lepingu (ELi toimimise leping) artikkel 114**, mis lubab võtta meetmeid riigisiseste normide ühtlustamiseks, et tagada siseturu rajamine ja toimimine.

Direktiivi peamised eesmärgid on:

- Kõrvaldada liikmesriikide vahelised suured erinevused ja kehtestada ühised küberturvalisuse miinimumnormid;
- Luua tõhusad piiriülese koostöö ja teabevahetuse mehhanismid;
- Ajakohastada küberturvalisuse kohustuste alla kuuluvate sektorite ja tegevuste loetelu, et see kajastaks tänast ohumaastikku;
- Tagada täitmise tagamise ja õiguskaitsevahendid kohustuste tõhusamaks rakendamiseks;
- Tugevdada kriitilise taristuga operaatorite ja digiteenuse osutajate küberturvalisuse vastupidavusvõimet.

Direktiivi kohaldatakse, piiramata isikuandmete kaitsele (GDPR, määrus EL 2016/679) ja elektroonilise side privaatsusele (direktiiv 2002/58/EÜ) kohaldatavat ELi õigust ning kooskõlas sellega.

3. NIS1-st NIS2-ks: miks uus määrus?

NIS1, mis jõustus 2016. aastal, oli ELi esimene horisontaalne küberturvalisuse määrus. Läbivaatamise käigus ilmnes liikmesriikide rakendamisel tõsiseid erinevusi: kohaldamisala piiritlemise otsus jäeti suuresti liikmesriikide otsustada, mis killustas siseturgu.

NIS1 tuvastatud puudused

Probleemivaldkond	NIS1 olukord	NIS2 lahendus
Kohaldamisala piiritlemise	Jäeti liikmesriikide otsustada; praktikas märkimisväärsed erinevused.	Ühtne "suuruse ülempiiri" reegel kogu ELis (keskmise suurusega ja suurettevõtjad).
Sektorite loetelu	Piiratud arv sektoreid; suur osa digimajandusest jäeti välja.	Palju laiem sektorite katvus: digitaristu, avalik haldus, kosmosesektor jne.
Intsidentidest teatamine	Üheastmeline; tähtajad ja sisu erinesid liikmesriigiti.	Mitmeastmeline teatamine: 24 h varajane hoiatus + 72 h teatis + 1-kuuline lõpparuanne.
Riskijuhtimine	Üldine sõnastus; konkreetsed miinimummeetmed ebaselged.	Artikkel 21 loetleb 10 kohustuslikku miinimummeetmete kategooriat.
Karistused	Rakendati liikmesriigiti väga erinevalt.	ELi ülene ühtlustatud maksimumtrahv (10 mln eurot / 2% käibest).
Tippjuhtkonna vastutus	Ebaselge.	Juhtorgan vastutab isiklikult vastavuse eest; kohustuslik koolitus.

NIS2 ei ole NIS1 uuendus, vaid asendus, mis on loodud looma **ühtse, ühtlustatud ja täidetava küberturvalisuse raamistiku** kogu liidus.

4. Kohaldamisala ja väljajäetud valdkonnad

Direktiiv hõlmab peamiselt üksusi, mis tegutsevad ELis **I lisas (kõrge kriitilisuse astmega)** või **II lisas (muudes kriitilistes)** sektorites ning vastavad vähemalt keskmise suurusega ettevõtja määratlusele. Komisjoni soovituse 2003/361/EÜ lisa artikli 2 kohaselt on keskmise suurusega ettevõtja selline, kus on alla 250 töötaja ja aastane käive ei ületa 50 miljonit eurot (või bilansimaht ei ületa 43 miljonit eurot). NIS2 hõlmab keskmise suurusega ettevõtja künnist täitvaid või ületavaid üksusi: kohaldamisalasse kuulumise praktiline alampiir on 50 töötajat või 10 miljonit eurot käivet (sama soovituse alusel "väikeettevõtja" ülempiir).

Suurusest sõltumata hõlmatud üksused

- Üldsusele kasutatavate elektrooniliste sidevõrkude ja -teenuste osutajad;
- Usaldusteenuse osutajad (eIDAS-määruse EL 910/2014 alusel);
- Tippdomeeninimede (TLD) registrid ja domeeninimede süsteemi teenuse osutajad;
- Üksused, kes on liikmesriigis teenuse ainuosutajad või mille teenuse häirumine võib oluliselt mõjutada avalikku julgeolekut, tervist või turvalisust;
- Kõik keskse avaliku halduse üksused (liikmesriigid defineerivad riigisiseselt).

Kohaldamisalast väljajäetud valdkonnad

Avaliku halduse üksused, mille tegevus on peamiselt seotud **riikliku julgeoleku, avaliku julgeoleku, kaitse või õiguskaitse** valdkonnaga (kuritegude ennetamine, uurimine, avastamine ja nende eest vastutusele võtmine), jäetakse direktiivi kohaldamisalast välja. Samuti on välja jäetud liikmesriikide diplomaatilised ja konsulaaresindused kolmandates riikides ning suletud süsteemides kasutatavad usaldusteenused.

5. Põhimõisted

Direktiivi nõuetekohaseks tõlgendamiseks tuleb mõista mõningaid põhimõisteid.

Mõiste	Määratlus
Võrgu- ja infosüsteem	Elektroonilised sidevõrgud, mis tahes seade või seadmete rühm, mis töötleb digitaalandmeid, ning kõik digitaalandmed, mida töödeldakse selliste süsteemide toimimiseks, kasutamiseks, kaitsmiseks ja hooldamiseks.
Küberturvalisus	Kõik tegevused, mis on vajalikud võrgu- ja infosüsteemide, nende kasutajate ja teiste isikute kaitsmiseks küberohtude eest.
Intsident	Sündmus, mis kahjustab talletatavate, edastatavate või töödeldavate andmete või võrgu- ja infosüsteemide kaudu pakutavate või kättesaadavate teenuste kättesaadavust, autentsust, terviklikkust või konfidentsiaalsust.
Oluline intsident	Intsident, mis on põhjustanud või võib põhjustada asjaomase üksuse teenuste osutamisel tõsiseid tegevushäireid või rahalist kahju, või mis on mõjutanud või võib mõjutada teisi füüsilisi või juriidilisi isikuid, põhjustades märkimisväärset materiaalset või mittemateriaalset kahju.
Küberoht	Mis tahes potentsiaalne asjaolu, sündmus või toiming, mis võib kahjustada, häirida või muul viisil ebasoodsalt mõjutada võrgu- ja infosüsteeme.
Oluline küberoht	Küberoht, mis oma tehniliste omaduste põhjal on eeldatavasti võimeline avaldama tõsist mõju üksuse võrgu- ja infosüsteemidele, tema kasutajatele või teistele isikutele, põhjustades märkimisväärset materiaalset või mittemateriaalset kahju.
Nõrkus	IKT-toodete või -teenuste nõrkus, vastuvõtlikkus või viga, mida küberoht võib ära kasutada.
Peaaegu toimunud intsident	Sündmus, mis oleks võinud kahjustada talletatavate, edastatavate või töödeldavate andmete või võrgu- ja infosüsteemide kaudu pakutavate või kättesaadavate teenuste kättesaadavust, autentsust, terviklikkust või konfidentsiaalsust, kuid mille realiseerumine edukalt ennetati.
CSIRT	Küberturbe intsidentide lahendamise üksus, intsidentide käsitlemise eest vastutav tehniline meeskond.
ENISA	Euroopa Liidu Küberturvalisuse Amet, kellel on direktiivi rakendamisel keskne nõuandja- ja tugirolli.

6. Üksuste kategooriad: elutähtsad ja olulised üksused

Direktiiv jaotab kõik kohaldamisalasse kuuluvad üksused kahte põhikategooriasse. See eristus määrab kohustuste ning järelevalve- ja täitmise tagamise korra kohaldamise viisi.

Kriteerium	Elutähtsad üksused	Olulised üksused
Sektor	I lisa, kõrge kriitilisuse astmega sektorid	II lisa, muud kriitilised sektorid (ja I lisas keskmise suurusega)
Suurus	Suurettevõtjad (250+ töötajat või 50+ mln eurot käivet)	Keskmise suurusega ettevõtjad (50 kuni 249 töötajat)
Järelevalvekord	Nii ex-ante kui ka ex-post järelevalve	Ainult ex-post tõendite või kaebuse alusel
Haldustrahvi ülempiir	10 miljonit eurot või 2% ülemaailmsest aastasest käibest (kohaldatakse kõrgemat)	7 miljonit eurot või 1,4% ülemaailmsest aastasest käibest (kohaldatakse kõrgemat)
Tippjuhtkonna sanktsioonid	Võidakse kohaldada ajutist juhtimiskeeldu	Ajutist juhtimiskeeldu ei kohaldata

Oluline märkus: Kui üksus on NIS1 alusel identifitseeritud "oluliste teenuste operaatorina", võib liikmesriik otsustada, et seda üksust käsitatakse otse elutähtsa üksusena NIS2 alusel. Lisaks käsitatakse kõiki direktiivi 2022/2557 (elutähtsate teenuste toimepidevuse direktiiv, CER) kohaseid elutähtsaid teenuse osutajaid automaatselt elutähtsate üksustena NIS2 alusel.

7. Kohaldamisalasse kuuluvad sektorid (I lisa ja II lisa)

I lisa, kõrge kriitilisuse astmega sektorid

Nendes sektorites on suurettevõtjad elutähtsad üksused; keskmise suurusega üksused on olulised üksused.

Sektor	Allsektor / üksuse liik
Energia	Elekter (tootmine, ülekanne, jaotus, tarnimine); kaugküte ja -jahutus; nafta (torustik, tootmine, ladustamine, ülekanne); maagaas; vesiniku tootmine, ladustamine ja ülekanne
Transport	Lennundus (lennuettevõtjad, lennujaamad, lennuliikluse juhtimine); raudtee (taristuhaldajad, raudteeoperaatorid); meretransport (mere- ja siseveetranspordi operaatorid); maanteetransport (intelligentsed transpordisüsteemid, teedeoperaatorid)
Pangandus	Krediidiasutused vastavalt määrusele (EL) 575/2013
Finantsturgude infrastruktuur	Kauplemiskohad (börsid) ja kesksed vastaspooled (CCP)
Tervishoid	Tervishoiuteenuste osutajad; ELi referentlaboratooriumid; Ravimite teadus- ja arendustegevusega tegelevad üksused; Ravimitootjad; Avaliku tervisekriisi ajal kriitiliseks peetavate meditsiiniseadmete tootjad (vastavalt määrusele (EL) 2022/123)
Joogivesi	Inimtarbimiseks mõeldud vee tarnijad ja turustajad
Reovesi	Linnaheitvee, olmeheitvee või tööstusheitvee kogumise, käitlemise või puhastamisega tegelevad üksused
Digitaristu	Internetivahetuspunktid (IXP); domeeninimede süsteemi teenuse osutajad (v.a juurnimeserverid); tippdomeeninimede registrid; pilvandmetöötlusteenuse osutajad; andmekeskusteenuse osutajad; sisulevivõrgu (CDN) pakkujad; usaldusteenuse osutajad; üldsusele kasutatavate elektrooniliste sidevõrkude ja -teenuste osutajad
IKT-teenuste haldamine (B2B)	Hallatud teenuse osutajad (MSP); hallatud turbeteenuse osutajad (MSSP)
Avalik haldus	Liikmesriikide poolt määratletud kesk- ja piirkondliku valitsuse üksused
Kosmosesektor	Liikmesriikide või erasektori käitatava maapealse taristu operaatorid

II lisa, muud kriitilised sektorid

Sektor	Allsektor / üksuse liik
Posti- ja kullerteenused	Postiteenuse osutajad (sealhulgas kullerteenused)
Jäätmekäitlus	Jäätmete kogumise, ringlussevõtu ja käitlemise teenuseid pakkuvad üksused
Kemikaalid	Kemikaalide tootmise, töötlemise ja turustamisega tegelevad üksused
Toiduained	Toiduainete tootmise, töötlemise ja hulgimüügiga tegelevad suurettevõtjad
Tootmine	Meditsiiniseadmed/in vitro diagnostikameditsiiniseadmed; arvutid, elektroonika- ja optilised tooted; elektriseadmed; muud mujal klassifitseerimata masinad ja seadmed; mootorsõidukid, haagised ja poolhaagised; muu transpordivahendite tootmine
Digiteenuse osutajad	Veebipõhised kauplemiskohad; veebipõhised otsingumootorid; sotsiaalvõrguteenuse platvormid
Teadustegevus	Ärilistel eesmärkidel teadustegevust läbi viivad teadusorganisatsioonid

8. Liikmesriikide kohustused

Direktiiv kohustab nii liikmesriike kui ka eraisikutest üksusi. Iga liikmesriik peab astuma järgmised sammud:

Riiklik küberturvalisuse strateegia. Võtta vastu riiklik küberturvalisuse strateegia selgete strateegiliste eesmärkide, prioriteetide ja juhtimisraamistikuga. Strateegia käsitleb selliseid teemasid nagu tarneahela turvalisus, lunavara, VKEde toetamine, avatud lähtekood ja aktiivne küberkaitse.

Pädev(ad) asutus(ed). Määrata või luua üks või mitu pädevat asutust direktiivi rakendamise ja järelevalve tagamiseks.

Ühtne kontaktpunkt (SPOC). Määrata ühtne kontaktpunkt, kes vastutab piiriülese koordineerimise eest ELi tasandil.

CSIRT. Luua või määrata üks või mitu CSIRTi, kes vastutavad intsidentide käsitlemise, ennetava seire, koordineeritud nõrkuste avalikustamise ning riikliku ja rahvusvahelise koostöö eest.

Üksuste loetelu. Koostada, korrapäraselt uuendada ja edastada komisjonile elutähtsate ja oluliste üksuste ning domeeninimede registreerimise teenuseid osutavate üksuste loetelu.

Koordineeritud nõrkuste avalikustamine. Määrata koordinaatoriks CSIRT; edendada nõrkuste uurijatele õiguslikku selgust.

Vastastikune abi. Osutada teistele liikmesriikidele vastastikust abi piiriülese järelevalve ja täitmise tagamise küsimustes.

VKEde toetamine. Pakkuda väikestele ja mikroettevõtjatele suuniseid, tasuta tööriistu ning riiklikku/piirkondlikku kontaktpunkti.

9. Küberturvalisuse riskijuhtimismeetmed (artikkel 21)

Direktiivi kõige olulisem tehniline säte on artikkel 21. See loetleb minimaalsed tehnilised, tegevuslikud ja korralduslikud meetmed, mida elutähtsad ja olulised üksused peavad rakendama. Lähtutakse **kõiki ohte hõlmavast lähenemisviisist**: hõlmatud ei ole ainult küberrünnakud, vaid ka sellised ohud nagu füüsiline kahju, looduskatastroofid, seadmete rike ja inimlik viga.

Artikkel 21, kümme miinimummeedet

#	Meede	Kirjeldus
1	Riskianalüüsi ja infosüsteemide turbe põhimõtted	Kõigi riskide analüüs ja üldiste infoturbepoliitikate kirjalik koostamine.
2	Intsidentide käsitlemine	Intsidentide ennetamise, avastamise, neile reageerimise ja nendest taastumise protsessid.
3	Talitluspidevus	Varundushaldus, avariitaaste ja kriisiohje.
4	Tarneahela turvalisus	Sealhulgas tarnijate turvatavad; küberturvalisuse sätted otseste tarnijatega sõlmitud lepingutes.
5	Võrgu- ja infosüsteemide hankimise, arendamise ja hooldamise turvalisus	Turvalisus kogu elutsükli vältel, sealhulgas nõrkuste käsitlemine ja avalikustamine.
6	Meetmete tõhususe hindamise tööpõhimõtted ja menetluskord	Riskijuhtimismeetmete tõhususe korrapärane hindamine.
7	Küberhügieeni põhitavad ja küberturvalisuse koolitus	Küberhügieeni tavad ja teadlikkuse suurendamise koolitus töötajatele.
8	Krüptograafia ja krüpteerimise kasutamise põhimõtted ja menetlused	Krüpteerimise kasutamise põhimõtted; täisotsast krüpteerimine seal, kus see on asjakohane.
9	Personali turvalisus, juurdepääsukontrolli põhimõtted ja varade haldus	Personali turbekontrollid, volitused ja varade inventuur.
10	Mitmikautentimine ja turvaline side	Mitmikautentimine seal, kus asjakohane, pidevautentimine, turvaline hääl-, video- ja tekstside ning turvalised hädaolukorra sidesüsteemid.

Neid meetmeid kohaldatakse **proportsionaalsuse põhimõtte** alusel, arvestades üksuse riskidele avatust, suurust, sektorilist tähtsust ning intsidentide võimalikku mõju.

10. Intsidentidest teatamise kohustused (artikkel 23)

Direktiivi kõige kriitilisem operatiivne uuendus on mitmeastmeline intsidentidest teatamise kord. Elutähtsad või olulised üksused peavad teatama **olulistest intsidentidest**, mis on määratletud kui need, mis põhjustavad tõsiseid tegevushäireid, rahalist kahju või märkimisväärset mõju teistele isikutele, CSIRTile või pädevale asutusele järgmiste tähtaegade jooksul.

Etapp	Tähtaeg	Sisu
Varajane hoiatus	Hiljemalt 24 tunni jooksul pärast olulisest intsidendist teada saamist	Märge selle kohta (kui see on kohaldatav), kas olulise intsidendi põhjuseks on eeldatavasti ebaseaduslik või pahatahtlik tegevus; võimaliku piiriülese mõju olemasolu; põhiteave CSIRTi teavitamiseks.
Intsidentiteatis	Hiljemalt 72 tunni jooksul pärast olulisest intsidendist teadlikuks saamist	Varajase hoiatuse ajakohastamine; tõsidus, mõju ning võimaluse korral rikkeindikaatorid.
Vahearuanne / lõpparuanne	Hiljemalt ühe kuu jooksul pärast intsidenditeate esitamist	Intsidendi, sealhulgas selle tõsiduse ja mõju üksikasjalik kirjeldus; ohu liik või lähtepõhjus, mis intsidendi tõenäoliselt põhjustas; juba kohaldatud ja kohaldamisel olevad leevendusmeetmed; piiriülene mõju, kui see on asjakohane.
Vahearuanne	Kui intsident jätkub lõpparuande esitamise ajal	Vahearuanne intsidendi praeguse oleku kohta; lõpparuanne ühe kuu jooksul pärast intsidendi käsitlemise lõpetamist.

Teenuse kasutajatele teavitamine: Kui on tõenäoline, et oluline küberoht realiseerub, peavad üksused teavitama oma teenuste kasutajaid põhjendamatu viivituseta ja tasuta võimalikest leevendusmeetmetest ning vajaduse korral ka ohust endast selges ja arusaadavas keeles.

Peaaegu toimunud intsidendid ja vabatahtlik teatamine

Lisaks intsidentidele **võivad üksused vabatahtlikult teatada peaaegu toimunud intsidentidest ja olulistest küberohtudest** CSIRTile või pädevale asutusele. Direktiivi kohaldamisalasse mittekuuluvad üksused võivad samuti vabatahtlikult teatada. Vabatahtlik teatamine ei too kaasa täiendavaid kohustusi teatajale.

> **Praktiline mõju:** 24-tunnine varajase hoiatuse tähtaeg kohustab üksuseid omama küberintsidentidele reageerimise kava ja teavitusvoogu, mis on kohe pärast intsidendi avastamist käivitamiseks valmis. Selle tähtaja järgimine käsitsi ja killustatult toimivate protsessidega on äärmiselt keeruline.

11. Tarneahela turvalisus

Enamik viimastel aastatel toimunud suurtest küberrünnakutest jõudis sihtorganisatsioonideni tarnijate ja tarkvaratootjate kaudu, mitte organisatsiooni otsese ründamise teel. Seepärast seab direktiiv tarneahela riski riskijuhtimiskohustuste keskmesse.

- Üksused peavad hindama oma tarnijate ja teenuseosutajate toodete/teenuste **kvaliteeti, turvatavad ja turvalise arenduse korda**.
- **Küberturvalisuse nõuded tuleb lisada lepingutesse** otseste tarnijatega.
- **Hallatud turbeteenuse osutajate (MSSP) valimisel** tuleb olla eriti hoolikas; need osutajad on ründajate jaoks kõrge väärtusega sihtmärgid.
- Koostöörühm koos komisjoni ja ENISAga viib läbi **koordineeritud turberiski hindamisi** kriitilise tähtsusega tarneahelate jaoks (nagu tehti 5G-võrkude puhul).
- **Mittetehniline riskitegurid** kuuluvad samuti hindamisalasse, sealhulgas kolmandate riikide võimalik põhjendamatu mõju tarnijatele, varjatud nõrkused/tagauksed ning teenuse osutajast sõltuvus.

12. Juhtorgani vastutus

Direktiiv tagab, et küberturvalisus ei jää ainuüksi tehniliste osakondade teemaks, vaid muutub **tippjuhtkonna otseseks vastutusalaks**. Artikli 20 kohaselt on elutähtsate ja oluliste üksuste juhtorganid kohustatud:

- Vastutama artikli 21 kohaste **riskijuhtimismeetmete heakskiitmise** ja nende rakendamise järelevalve eest;
- Olema võimelised kandma **isiklikku vastutust** nende kohustuste rikkumise eest;
- Läbima korrapäraselt küberturvalisuse koolitust piisavate teadmiste ja oskuste omandamiseks;
- Soodustama samalaadset koolitust oma töötajatele.

> **Oluline:** Elutähtsate üksuste puhul võib pädev asutus nõuda **ajutise juhtimiskeelu** kohaldamist tippjuhtkonna suhtes (nendele, kes tegutsevad tegevjuhi või seadusliku esindaja rollis). See on viimase abinõuna kasutatav meede, mida kohaldatakse alles pärast kõigi muude täitmise tagamise võimaluste ammendamist.

13. ELi tasandi koostööstruktuurid

Direktiiv reguleerib või tugevdab erinevaid struktuure, mis tagavad liikmesriikide tõhusa koostöö:

Struktuur	Ülesanne
Koostöörühm	Toetab koostööd strateegilisel tasandil; koostab kaheaastaseid tööprogramme; avaldab suunisdokumente; viib läbi kriitilise tähtsusega tarneahelate koordineeritud riskihindamisi.
CSIRTide võrgustik	Operatiivtasandi koostöö; intsidentide teabevahetus; vastastikune abi; ühine reageerimine.
EU-CyCLONe	Euroopa küberkriisi kontaktorganisatsioonide võrgustik; ühendab suures ulatuses intsidentide ja kriiside puhul tehnilise ja poliitilise tasandi; koostab mõjuanalüüse.
ENISA	Loob ja haldab Euroopa nõrkuste andmebaasi; pakub tehnilist tuge; arendab suuniseid; jälgib liikmesriikide küberhügieenipoliitikat.
IPCR-korraldused	ELi integreeritud poliitilise kriisireageerimise korraldused (nõukogu rakendusotsus 2018/1993), liidu tasandi kriisijuhtimine ulatuslike kriiside puhuks.
ELi CSIRTide koordinaator CVD jaoks	Igas liikmesriigis määratakse koordinaatoriks CSIRT, kes haldab piiriülest koordineeritud nõrkuste avalikustamist.

Koostöö kolmandate riikidega: EL võib sõlmida rahvusvahelisi lepinguid kolmandate riikide või rahvusvaheliste organisatsioonidega ELi toimimise lepingu artikli 218 alusel. Sellised lepingud võivad, kaitstes liidu huve ja andmekaitset, lubada neil osapooltel osaleda koostöörühma, CSIRTide võrgustiku või EU-CyCLONe tegevustes.

14. Järelevalve ja täitmise tagamine

Direktiiv näeb ette erinevad järelevalvekorrad kahe üksuste kategooria jaoks. **Elutähtsate üksuste** suhtes kohaldatakse nii ex-ante kui ka ex-post järelevalvet, samas kui **olulisi üksuseid** jälgitakse ainult ex-post, tõendite või kaebuse alusel.

Pädevate asutuste järelevalvevolitused

- Viia läbi kohapealseid kontrolle ja kaugseire;
- Nõuda sihipäraseid turvaauditeid (üksus võib kandma kulud);
- Tellida turvaskaneerimisi;
- Nõuda riskijuhtimismeetmetele vastavust tõendavaid dokumente;
- Nõuda teavet direktiivi rikkumises kahtlustatavate tegude kohta;
- Nõuda vajaduse korral isikuandmetele ja liikluse andmetele juurdepääsu võimaldavat teavet.

Kohaldatavad täitmise tagamise meetmed

- Anda hoiatusi ja siduvaid juhiseid;
- Nõuda konkreetsete meetmete rakendamist või nõrkuste kõrvaldamist täpsustatud tähtaja jooksul;
- Tellida sõltumatu audit riskijuhtimismeetmete kontrollimiseks;
- Nõuda, et üksused teavitaksid teenuse kasutajaid rikkumise laadist;
- Teha avalikke avaldusi (avalikustades üksuse nime ja rikkumise laadi);
- Elutähtsate üksuste puhul (viimase abinõuna): sertifikaatide või lubade ajutine peatamine ja tippjuhtkonnale ajutiste juhtimiskeeldude kohaldamine;
- Määrata või taotleda haldustrahvide kohaldamist.

15. Haldustrahvid

Direktiiv kehtestab **ELi ülese ühtlustatud maksimumpiirid** liikmesriikide kohaldatavatele haldustrahvidele. Need piirid on seotud üksuse ülemaailmse käibega, sarnaselt GDPRiga.

Üksuse liik	Maksimumsumma (kohaldatakse kõrgemat)
Elutähtsad üksused	10 000 000 eurot või 2% ülemaailmsest aastasest käibest
Olulised üksused	7 000 000 eurot või 1,4% ülemaailmsest aastasest käibest

Trahvisuuruse määramise tegurid

- Rikkumise laad, raskusaste ja kestus;
- Tekitatud materiaalne või mittemateriaalne kahju;
- Kas rikkumine oli tahtlik või hooletu;
- Kahju ennetamiseks või leevendamiseks võetud meetmed;
- Vastutuse määr ja varasemad rikkumised;
- Koostöö aste pädeva asutusega;
- Muud raskendavad või kergendavad asjaolud.

Trahvid peavad olema **proportsionaalsed** ning nende kohaldamisel tuleb järgida põhiõigusi, nagu kaitseõigus, süütuse presumptsioon ja õigus tõhusale õiguskaitsevahendile. Liikmesriigid võivad ette näha ka kriminaalkaristused riigisisese õiguse rikkumiste eest; kuid ühtki isikut ei tohi karistada kaks korda sama teo eest, rikkudes **ne bis in idem** põhimõtet.

16. Rakendamise ajakava ja üleminek

Kuupäev	Sündmus
14. detsember 2022	Direktiivi vastuvõtmine Euroopa Parlamendi ja nõukogu poolt
27. detsember 2022	Avaldamine Euroopa Liidu Teatajas (ELT L 333/80)
16. jaanuar 2023	Direktiivi jõustumine (20 päeva pärast avaldamist)
17. oktoober 2024	Direktiivi riiklikku õigusse ülevõtmise tähtaeg liikmesriikidele
18. oktoober 2024	Direktiivi kohaldamise algus
18. oktoober 2024	Direktiivi (EL) 2016/1148 (NIS1) kehtetuks tunnistamine
17. aprill 2025	Tähtaeg liikmesriikidele elutähtsate ja oluliste üksuste loetelu edastamiseks komisjonile
Alates 17. oktoobrist 2027	Direktiivi rakendamise korrapärane läbivaatamine komisjoni poolt (iga 36 kuu järel)

Oluline: NIS2 on direktiiv ega kehti otse. Iga liikmesriik peab direktiivi oma riigisisesesse õigusse üle võtma. Seetõttu sõltuvad üksusele kohaldatavad täpsed kohustused ja karistused selle liikmesriigi poolt vastu võetud riiklikust ülevõtmisaktist, kus ta tegutseb.

17. Mõju ELi-välistele ettevõtetele

Kuigi NIS2 on ELi direktiiv, on sel olulised mõjud ELi-välistele ettevõtetele, eriti neile, kes teenindavad ELi turgu või tarnivad ELi-põhistele kriitiliste sektorite üksustele:

Otseselt mõjutatud ELi-välised ettevõtted

- ELi-välised **DNS-teenuse osutajad, pilveteenuse osutajad, andmekeskuste operaatorid, CDN-pakkujad, hallatud teenuse ja hallatud turbeteenuse osutajad, veebipõhised kauplemiskohad, otsingumootorid ja sotsiaalvõrguplatvormid**, kes pakuvad teenuseid ELis, peavad määrama ELi esindaja ja järgima direktiivi kohustusi;
- ELi tütarettevõtete või filiaalidega ELi-välistele ettevõtetele võib direktiiv kohalduda nende üksuste kaudu;
- ELi elutähtsatele või olulistele üksustele tooteid/teenuseid pakkuvad ELi-välised tarnijad alluvad nende klientide kehtestatud **tarneahela turvalisuse lepingulistele nõuetele** (artikkel 21(2)(d));
- ELi digitaristu- või finantssektori üksuseid teenindavad ELi-välised MSP-d/MSSP-d võivad kuuluda otseselt kohaldamisalasse.

Kaudsed mõjud

- ELi klientide tarneahela riskihindamised sunnivad ELi-väliseid tarnijaid tõstma oma küberturvalisuse standardeid;
- Direktiivi poolt kehtestatud standardid (ISO/IEC 27001, ENISA suunised jne) muutuvad **de facto viitepunktideks** globaalsel turul;
- ELi-välised jurisdiktsioonid kasutavad üha enam NIS2-i viitena oma küberturvalisuse seadusandluse väljatöötamisel.

18. Praktiline vastavustegevuse kava (10 sammu)

Järgnev 10-sammuline kava on praktiline juhend nii ELis tegutsevatele ettevõtetele kui ka neile, kes soovivad vabatahtlikult NIS2 standarditega kooskõlas olla.

Samm	Tegevus
1. Kohaldamisala määramine	Selgitada välja, kas ettevõte kuulub I või II lisa sektoritesse, vastab suuruse kriteeriumidele, ja tuvastada kategooria (elutähtis/oluline).
2. Lünkade analüüs	Hinnata olemasolevat infoturbe juhtimissüsteemi artikli 21 10 meetmete kategooria suhtes; kaardistada lüngad.
3. Juhtimisstruktuur	Kehtestada vastutused, aruandlusliinid ja heakskiitmisprotsessid juhatuse/tippjuhtkonna tasandil; luua korrapärane koolitusprogramm.
4. Poliitikad ja dokumentatsioon	Koostada või uuendada infoturbepoliitikat, riskijuhtimispoliitikat, intsidentidele reageerimise poliitikat, vastuvõetava kasutuse poliitikat ja muid dokumente.
5. Riskihindamine	Koostada varade inventuur, ohuanalüüs ja riskihindamine kõiki ohte hõlmava lähenemisviisiga; kehtestada riskide aktsepteerimise kriteeriumid.
6. Tehniliste kontrollmeetmete rakendamine	Rakendada mitmikautentimine, krüpteerimine, võrgu segmenteerimine, null-usalduse arhitektuur, logihaldus, SIEM, EDR/XDR, varundus- ja avariitaaste lahendused.
7. Intsidentidele reageerimise võimekus	Dokumenteerida intsidentidele reageerimise kava; määrata rollid/vastutused; luua 24-tunnine varajase hoiatuse teavitusvoog; korraldada lauaõppused.
8. Tarneahela haldus	Inventeerida tarnijad; liigitada nad riskitaseme järgi; lisada küberturvalisuse sätted lepingute mallidesse; korraldada korrapäraseid auditeid.
9. Koolitus ja teadlikkuse tõstmine	Korraldada kõigile töötajatele iga-aastane küberhügieeni koolitus; pakkuda spetsialiseeritud koolitust juhtorganile; korraldada andmepüügisimulatsioone.
10. Pidev täiustamine	Viia läbi sise- ja välisauditeid; jälgida KPI-sid; õppida igast intsidendist; uuendada riskihindamist kord aastas; taotleda sertifitseerimist (ISO/IEC 27001, ELi küberturvalisuse sertifitseerimine).

19. Kokkuvõte ja hinnang

NIS2 direktiiv tõstab oluliselt Euroopa Liidu küberturvalisuse lähtetaset. See ei kehtesta ainult tehnilisi nõudeid, vaid muudab küberturvalisuse **ettevõtete juhtimisstruktuuri ja äritegevuse lahutamatuks osaks**.

Direktiivi tugevused

- **Lai haare**: kohaldamisalas umbes 18 sektorit ja üle 100 000 üksuse kogu EL-27 piires;
- **Ühtlustamine**: ühetasane mänguplats siseturul tänu ühtsetele kriteeriumidele ja täitmise tagamise korrale kogu ELis;
- **Juhtimisele keskendumine**: tippjuhtkonna vastutusele võtmise kaudu tagatakse küberturvalisuse levik kõigil ettevõtte tasanditel;
- **Tarneahelale rõhuasetamine**: vastab reaalsusele, et enamik tänapäevaseid rünnakuid tuleb tarneahela kaudu;
- **Koostööstruktuurid**: mitmekihiline ELi tasandi koordineerimine koostöörühma, CSIRTide võrgustiku ja EU-CyCLONe kaudu.

Kriitika ja väljakutsed

- Viivitused ja erinevused liikmesriikide ülevõtmisel; praktikas on ühtne rakendamine kogu EL-27 ulatuses ebaühtlane;
- Eriti keskmise suurusega ettevõtjate jaoks kujutab vastavuse maksumus ja tehnilise võimekuse lõhe sulgemine tõsist väljakutset;
- 24-tunnise varajase hoiatuse tähtaja rakendamine enne piisava küpsuse saavutamist võib viia pealiskaudsete või vigaste teavitusvoogudeni;
- Kattuvusvaldkonnad valdkondlike määrustega (DORA, rahandus; eIDAS, usaldusteenused; sektoripõhised lennundusreeglid jne) võivad tekitada üksustele keerukust.

Üldine hinnang

NIS2 raamib küberturvalisuse ümber tehnilisest mureküsimusest **äritegevuse järjepidevuse, ettevõtte juhtimise ja klientide usalduse küsimuseks**. ELis tegutsevate või ELiga suhtlevate üksuste jaoks on vastavus nii seaduslik kohustus kui ka tegevuse vastupidavusvõime tugevdamise vahend.

ELi-välistele ettevõtetele kehtestab NIS2 uue **de facto standardi** ELi turule juurdepääsuks ning tõstab küberturvalisuse ootusi globaalselt. Varajane vastavusse viimine hõlbustab lepinguliste kohustuste täitmist ja parandab üldist küberturvalisuse vastupidavusvõimet.

> **Lõpumärkus:** Käesolev dokument võtab kokku direktiivi peamised sätted eestikeelsetele lugejatele. Teie organisatsioonile kohaldatavate vastavusnõuete jaoks vaadake ametlikku teksti (ELT L 333/80, 27.12.2022), oma liikmesriigi riiklikku ülevõtmisakti ning valdkondlikke regulatsioone; vajaduse korral kaasake õigus- ja küberturvalisuse nõustajad.

Allikad

- Direktiiv (EL) 2022/2555, EUR-Lex CELEX number 32022L2555
- Euroopa Liidu Teataja L 333/80, 27. detsember 2022
- ENISA, Euroopa Liidu Küberturvalisuse Amet (www.enisa.europa.eu)
- Euroopa Komisjoni digistrateegiaportaal (digital-strategy.ec.europa.eu)

Rohkem NIS2-st Rediaccilt

See kokkuvõte kaardistab direktiivi struktuuri ja kohustused. Rediacc.com-i kaasnevad juhendid tõlgivad need kohustused konkreetseteks operatiivseteks ja hankeotsuseteks.

Kolm kaasnevat juhendit

- **Artikkel 21(2)(d) ja omahosting.** Miks kolmanda osapoole IKT-register väheneb, kui andmetasand ei lahku kunagi teie rentnikust. CISO-dele ja hankevedajatele, kes läbirääkivad 2026. aastal DPA-sid ümber.
- **Pidev tõhusus ilma teatrita.** Artiklid 21(2)(e), (f) ja 23 koos loetuna. Konstantse ajaga fork, mis muudab iganädalased harjutused realistlikuks, ja artikli 23 teatamise ajakava, mida ei ole võimalik täita ilma kohtueksperti-tasemel artefaktideta. SRE ja operatiivjuhtidele.
- **NIS2 vastavuse struktuurne maksumus.** Viie tööriista komplekt, mida keskmise suurusega elutähtsad üksused koosstavad vaikides, mida omahostitav juhtimistasand kokku surub, ja kuluread, mis jäävad teie kanda mõlemal juhul. CFO-dele ja ostjatele, kes suunduvad uuendustsüklisse.

Kust neid leida

Kõik kolm juhendit koos selle kokkuvõttega allalaaditava PDF-ina on saadaval:

rediacc.com/resources/nis2-directive-summary

Rediacc OÜ on Eestis registreeritud omahostitava infrastruktuuri platvorm (registrikood 17363830, KMKR EE102920091). Toode ei asenda turbeprogramme; see on tööriistakiht, mis eemaldab andmetasandi hankijariski, mida traditsioonilised varundus-, avariitaaste- ja testandemete tööriistad ei suuda eemaldada. Tasuta Community tase ja tasulised tasemed alates 349 $/kuus.

> Käesolev dokument ja selle kaasnevad juhendid on haridusmaterjal. Teie organisatsioonile kohaldatavad vastavusotsused nõuavad õigusnõustamist ja viitamist teie jurisdiktsiooni riiklikule ülevõtmisaktile.