MAJANDUS- JA
KOMMUNIKATSIOONI-
MINISTEERIUM

Küberturvalisuse nõuetest ja Eesti infoturbestandardist

Raavo Palu
küberturvalisuse õigusnõunik
Majandus- ja Kommunikatsiooniministeerium
25. november 2022

Mis on küberturvalisus?

Küberturvalisuse määrus (Euroopa parlamendi ja nõukogu määrus nr 2019/881) art 2 punktid 1 ja 8:

- „küberturvalisus“– tegevused, mis on vajalikud, et kaitsta võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid küberohtude eest

- „küberoht“– võimalik asjaolu, sündmus või tegevus, mis võib kahjustada või häirida võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid või neile muul viisil halba mõju avaldada

Küberturvalisuse nõuetest (1/3)

- Põhilisemad küberturvalisuse nõuded tulevad küberturvalisuse seadusest (***KüTS**; jõustus 23.05.2018*)
  - KüTS sätestab ühiskonna toimimise seisukohast oluliste, sealhulgas avaliku sektori võrgu- ja infosüsteemide pidamise nõuded, vastutuse ja järelevalve ning küberintsidentide ennetamise ja lahendamise alused
- Kohaldamisala välistused/erisused: KüTS § 1 lõiked 2-4
- Kohaldub: teenuse osutajatele (*KüTS § 3 lg 1 ehk ETO-d/OTO-d*) ja avalikule sektorile (*KüTS § 3 lg 4, sh KOV-idele ja KOV-i hallatavatele asutustele ja ametiasutustele; neile kohaldatakse teenuse osutaja kohta sätestatut*)

Küberturvalisuse nõuetest (2/3)

- KüTS § 7 lg 1: teenuse osutaja peab rakendama alaliselt turvameetmeid:

  - küberintsidendi ennetamiseks;
  - küberintsidendi lahendamiseks;
  - küberintsidendi tõttu teenuse toimepidevusele või süsteemi turvalisusele avalduva mõju ennetamiseks ja leevendamiseks või teise sõltuva teenuse toimepidevusele või süsteemi turvalisusele avalduda võiva mõju ennetamiseks ja leevendamiseks.

Küberturvalisuse nõuetest (3/3)

- KüTS § 8 lg 1: Teenuse osutaja teavitab Riigi Infosüsteemi Ametit *(RIA)* viivitamata, kuid hiljemalt 24 tundi pärast teada saamist küberintsidendist:

  1) millel on süsteemi turvalisusele või teenuse toimepidevusele oluline mõju *(olulise mõju osas vt sama § lõiget 2);*

  2) mille oluline mõju süsteemi turvalisusele või teenuse toimepidevusele ei ole ilmne, kuid seda võib mõistlikult eeldada.
- Teenuse osutaja peab ka puudutatud isikuid/avalikkust teavitama (*vt KüTS § 8 lg 5*)
- Eraldi teavituskohustus, kui oluline küberintsident on seotud digitaalse teenuse osutajaga, keda teenuse osutaja kasutab *(vt KüTS § 8 lg 9)*

Küberturvalisuse seaduse I muutmine

- KüTS ja teiste seaduste muutmise seadus 531 SE
  - määratleti konkreetsemalt avalik sektor – *varasemalt oli riigi ja kohaliku omavalitsuse üksus*
  - muudatused jõustusid 16.08.2022, v.a. erisustena jõustuvad AvTS-i muudatused 01.01.2023 (***kaob ISKE***) ja ERR-iga seotud muudatused 01.01.2027 (*ERR muutub terve organisatsioonina KüTS-i subjektiks*)
  - lisandus volitusnormina KüTS § 7 lõige 5, mis võimaldab kehtestada Eesti infoturbestandardiga (*E-ITS*) seotud määrused

KüTS § 7 lõike 5 alusel antavatest määrustest

Kavas on kehtestada:

- Vabariigi Valitsuse määrus „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ (eelnõude infosüsteemi toimik 22-0570)
- ettevõtlus- ja infotehnoloogia ministri määrus „Eesti Infoturbestandard“ (eelnõude infosüsteemi toimik 22-0568)

Mõlema määruse

- hetkeseis: VV määrus edastati 17.11 VV-sse ja ministri määrus läheb peatselt MKM-i sisesele kooskõlastusele;
- sihtgrupp: KüTS-i teenuse osutajad (KüTS § 3 lg 1) ja avalik sektor (KüTS § 3 lg 4)

„Võrgu- ja infosüsteemide küberturvalisuse nõuded“ (1/3)

- Kooskõlastusringi versioonis olid ka nõuded pilvede kasutamiseks – need võeti hetkel välja, kuid lisanduvad hiljem muudatustena
- tekitab volituse ettevõtlus- ja infotehnoloogiaministrile E-ITS’i kehtestamiseks
- E-ITS asemel saab kasutada ISO/IEC 27001 standardit
- määratleb E-ITS’i auditeerimise sisu + need teenuse osutajad, kes ei pea E-ITS auditit tegema:
  - majandusaasta jooksul keskmiselt alla 10 töötaja + aasta bilansimaht/käive ei ületa 2 MEUR (nt perearstid)
  - loetelu konkreetsematest asutustest/isikutest: nt muuseumid
  - isikud, kes on teinud ISO/IEC 27001 + edastanud ISO/IEC 27001 vastavussertifikaadi Riigi Infosüsteemi Ametile

„Võrgu- ja infosüsteemide küberturvalisuse nõuded“ (2/3)

Määratleb turvameetmete üldnõuded

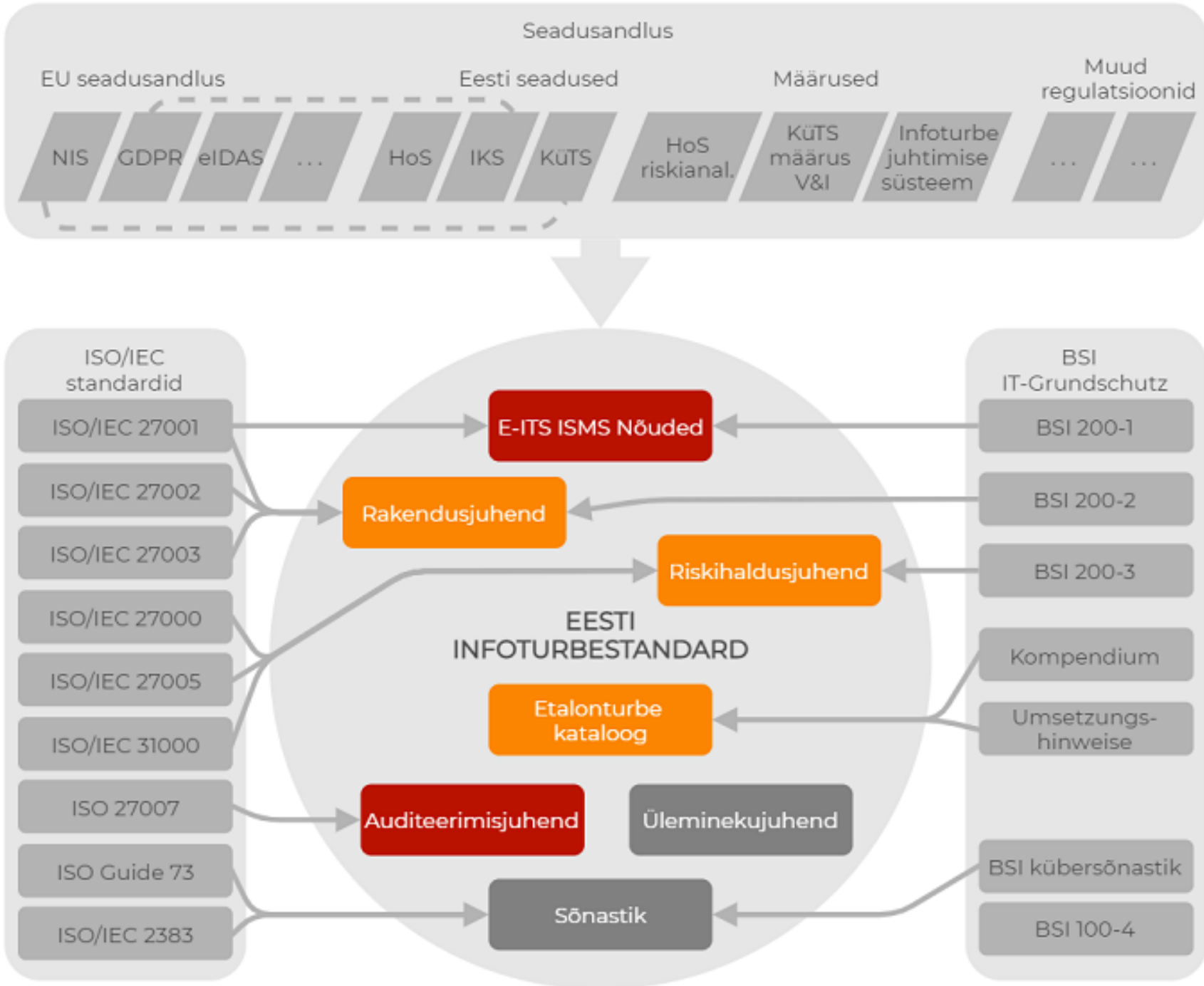
- süsteemide ja seotud teenuste või protsesside kaardistamine ning dokumenteerimisnõue rakendatavatele süsteemidel rakendatavate turvameetmete ja riskianalüüsi osas
- dokumentatsiooni säilitamiskohustus vähemalt 7 aastat selle koostamisest + vajadusel tehakse RIA-le kättesaadavaks
- säilib nõue: dokumentatsiooni võib koostada muu õigusakti alusel koostatava dokumendi osana
- paneb paika riskianalüüsi ajakohastamise aja

„Võrgu- ja infosüsteemide küberturvalisuse nõuded“ (3/3)

Rakendussätted: süsteemi turvalisuse tagamiseks rakendatud meetmete vastavust E-ITS’le eeldatakse, kui:	
• teenuse osutaja **haldab** riigi või kohaliku omavalitsuse üksuse süsteemi ning • nimetatud süsteemi turvalisuse tagamiseks **ISKE määruse nõudeid**. Erand kehtib kuni **31.12.2022** (seotud ISKE määruse kehtivusega)	• teenuse osutaja **ei halda** riigi või kohaliku omavalitsuse üksuse süsteemi ning • teenuse osutaja rakendab, seirab ja ajakohastab teatavaid turvameetmeid (6 punktine loetelu). Erand kehtib kuni ~~31.12.2022~~ 30.06.2023

“Eesti infoturbestandard“

- igal aastal kehtestatakse uuendatud versioon E-ITS’ist (*versiooni uuendamist teostab RIA; MKM vormistab ministri määruse lisaks*)
- sisaldab loetelu dokumentidest (saadaval ka E-ITS portaalis), milledest tuleb lähtuda E-ITS’i puhul ehk neil dokumentidel on ministri määruse jõud:
  - näiteks: organisatsiooni infoturbe halduse süsteemi nõuded, etalonturbe kataloog ja auditeerimise juhend/eeskiri
  - avalikul kooskõlastusel olnud versioonis oli loetelus ka rakendusjuhend – sellest teatud osad tulevad eelnimetatud dokumenti(desse) 2023 versioonis
- ministri määrusega kinnitatakse E-ITS 2022 versioon
- Kui E-ITS’i dokumentide osas on tagasisidet, siis edastada RIA-le aadressil **standard@ria.ee**


Seadusandlus
EU seadusandlus
Eesti seadused
Määrused
Muud regulatsioonid
NIS
GDPR
eIDAS
...
HoS
IKS
KüTS
HoS riskianal.
KüTS määrus V&I
Infoturbe juhtimise süsteem
...
...
ISO/IEC standardid
ISO/IEC 27001
ISO/IEC 27002
ISO/IEC 27003
ISO/IEC 27000
ISO/IEC 27005
ISO/IEC 31000
ISO 27007
ISO Guide 73
ISO/IEC 2383
E-ITS ISMS Nõuded
Rakendusjuhend
Riskihaldusjuhend
EESTI INFOTURBESTANDARD
Etalonturbe kataloog
Auditeerimisjuhend
Üleminekujuhend
Sõnastik
BSI IT-Grundschutz
BSI 200-1
BSI 200-2
BSI 200-3
Kompendium
Umsetzungs-hinweise
BSI kübersõnastik
BSI 100-4

Küsimused?

MAJANDUS- JA
KOMMUNIKATSIOONI-
MINISTEERIUM

Aitäh!

Raavo Palu
küberturvalisuse õigusnõunik
riikliku küberturvalisuse osakond
Majandus- ja Kommunikatsiooniministeerium
raavo.palu@mkm.ee