Küberturvalisuse seadus hakkab mõjutama ka toidutootjat

Keilin Tammepärg

22.01.2026

Teadmised on põllu ramm

Kaasrahastanud Euroopa Liit

Millest täna räägime?

1. Miks tegeleda küberturvalisusega
2. Regulatsoonid: NIS2, KüTS, CRA…
3. Praktilised soovitused

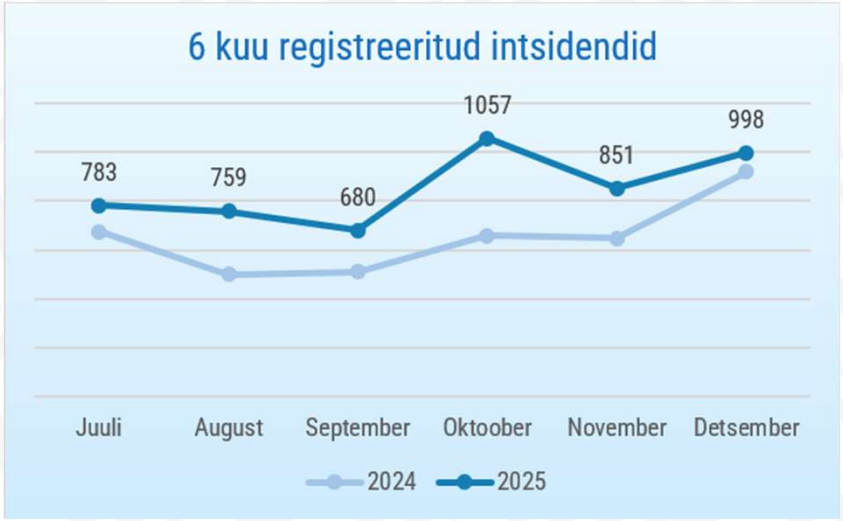
„Küberohud on tihedalt seotud tehnoloogia kiire arenguga. Tehnoloogia ise ei ole halb – vastupidi, see loob majandusele ja ühiskonnale uusi võimalusi. Paraku kasutavad samu tööriistu üha oskuslikumalt ka kurjategijad. Seetõttu ei piisa enam üksnes tehnilisest kaitsest, vaid määravaks saab juhtkonna otsustusvõime, rollijaotus ja valmisolek kriisiolukorras tegutseda.“

ITLi juhatuse liige ja CybExer Technologies OÜ nõukogu esimees Lauri Almann

„Küberruumi toimimine ei ole ammu enam pelgalt IT meeste mure ega tehniline probleem – see on osa majandusest, kriitilisest taristust ja igapäevaelust. „Seetõttu ei saa küberturvalisuse eest vastutada ainult IT-juht või infoturbe spetsialist. Soovitan ettevõtetel käsitleda küberturvalisust pideva juhtimisprotsessina, mitte ühekordse projektina.”

ITLi juhatuse liige ja Telia Eesti AS tegevjuht Andre Visse

Natuke numbreid

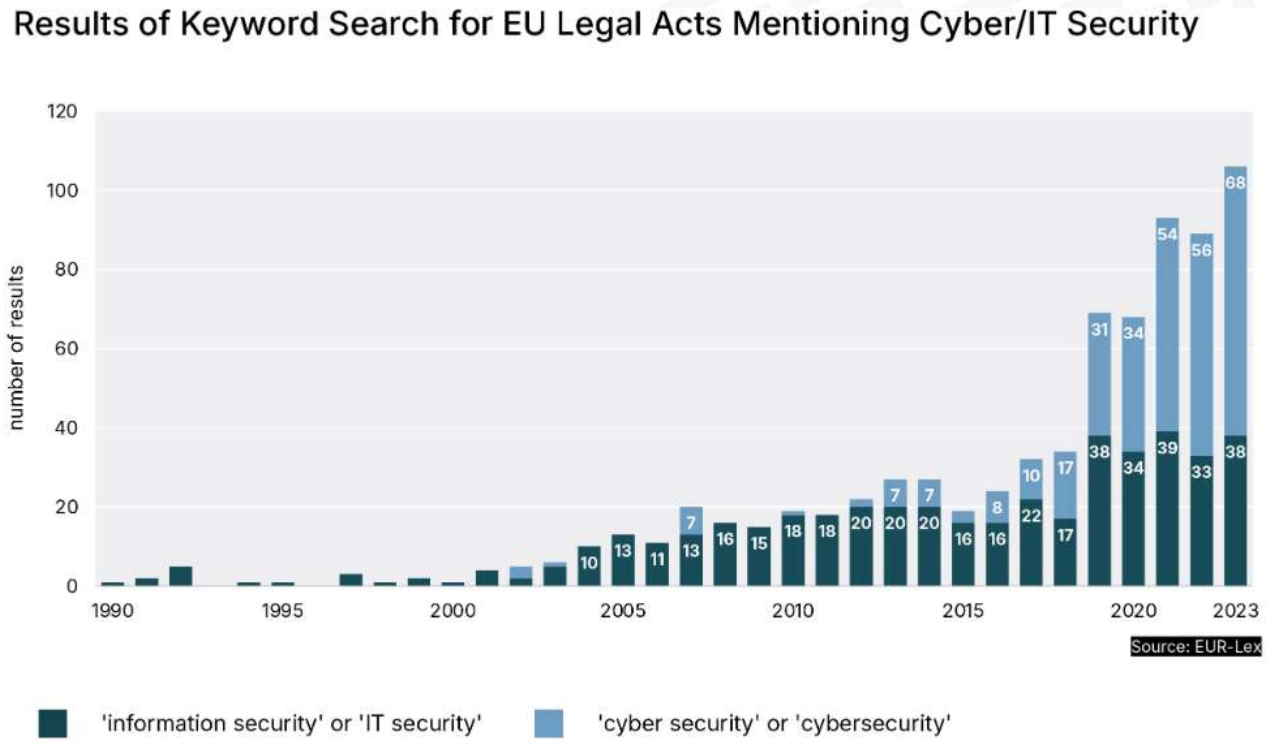


- 2025 toimus Eestis RIA andmetel üle 10 000 mõjuga intsidendi.
- Eestlased kaotasid 2025. a kelmidele ligi 29 miljonit eurot, millest suurima osa moodustasid pangapettused ja õngitsused.
- Iga kuues tööstusettevõte on olnud vähemalt 1 küberrünnaku all
  - Samas hinnatakse küberrünnete riski enda ärile nii: 5 palli skaalal 2,37.
- Ennustuste kohaselt kasutatakse 2027. aastaks tehisintellekti ligi 17% küberrünnakutest.

Graafiku allikas: https://www.ria.ee/olukord-kuberruumis-detsember-2025

Regulatsioonid

Küberturvalisus on EL-is tugevalt reguleeritud valdkond ning regulatsioonide kohaldamisala muudkui laieneb.



Küberturvalisuse valdkonda reguleerivad õigusaktid

Euroopa Liidu regulatsioonid

- NIS1 ja NIS2 (võrgu- ja infosüsteemide turvalisus)
- CSA (küberturvalisuse määrus)
- CRA (küberkerksuse määrus)
- Kübersolidaarsuse määruse ettepanek
- DORA (finantssektori tegevuskerksus)
- 5G küberturvalisuse tööriistakast
- NCCS (elektrivoogude küberturvalisuse eeskiri)
- Sertifitseerimisskeemid (EUCC, EUCS, 5G)
- Küberturvalisuse pädevuskeskuse määrus
- EL-i institutsioonide ja asutuste küberturvalisust puudutavad aktid
- EL-i aktide rakendusaktid ja juhised

Eesti regulatsioonid

- KüTS – küberturvalisuse seadus
- Võrgu- ja infosüsteemide küberturvalisuse nõuded
- E-ITS
- Pilvemäärus
- Küberintsidentide registri põhimäärus
- ESS + Nõuded sideteenuse osutamisele ja sidevõrkude tehnilised nõuded
- HOS-TsiRkS

Seotud õigusaktid: eIDAS2, GDPR, AI Act, CER, masinamäärus, DSA, RED

Miks reguleeritakse?

Regulatsiooni eesmärgid:

- Suurendada üldist vastupanuvõimet küberohtudele
- Tagada usaldus digitehnoloogiate vastu parandades toodete ja teenuste küberturvalisust
- Ühtlustada riikide küberjulgeolekutase ja parandada EL-i siseturu toimimist

Väljakutsed:

- Aina rohkem ühendunud maailm
- Hübriidohud
- Koostöö intsidentide ennetamiseks ja lahendamiseks
- Oskused

Küberturvalisuse seadus

KüTS

EL NIS2 direktiiv

- Direktiiv (EL) 2022/2555, 14. detsember 2022, meetmete kohta küberturvalisuse ühtlaselt kõrge taseme saavutamiseks kogu liidus;
- Eesmärk on saavutada kogu liidus ühtne kõrge küberturvalisuse tase, et parandada siseturu toimimist;
- See sätestab:
  - liikmesriikide kohustused (vastu võtta riiklik küberturvalisuse strateegia, määrata või luua pädevad asutused);
  - küberturvalisuse riskijuhtimise meetmed ja aruandluskohustused teatud üksustele;
  - küberturvalisuse teabe jagamise eeskirjad ja kohustused;
  - liikmesriikide järelevalve- ja jõustamiskohustused.

Hetkeseis

- Eesti võttis NIS2 direktiivi üle 3 aastat;
- Riigikogu võttis küberturvalisuse seaduse muutmise seaduse vastu 10.12.2025 ja see jõustus 01.01.2026
- Üleminekuaeg 3 aastat
- Töös rakendusaktid ja muudatused

Kellel on kohustus?

- Subjektide arv 3000 vs 6500
  - NB! Ise teab teadma!
- Üliolulised üksused
  - Sõltumata suurusest - elutähtsa teenuse osutajad - toiduga varustamise tagamine
  - Rida suuri: nt elektriettevõtja, infoturbe, pilveandmetöötlus
- Olulised üksused - ka osad sõltumata suurusest ja teised sõltuvad suurusest
  - Keskmise suurusega - ettevõtja, kes tegeleb toidu hulgimüügi, tööstusliku tootmise või tööstusliku töötlemisega või mitmega neist, välja arvatud alkoholi hulgimüügi, tööstusliku tootmise ja tööstusliku töötlemisega EL-I toiduohutuse määruses määratletud ettevõttes ning ühest või mitmest nimetatud tegevusest saadav aastakäive on vähemalt 50 protsenti tema aastakäibest;
  - Toiduvarustuskindluse valdkonna eest vastutav minister kehtestab määrusega KüTS-is nimetatud käitlemisvaldkondade ja toidugruppide täpsustatud loetelu.

Millised on peamised kohustused? (1)

- Esimene kohustus on endast teada anda 3 kuu jooksul seaduse jõustumisest või teenuseosutaja tunnustele vastavuse tekkimisest arvates;
- Järgida järgmisi põhimõtteid:
  - Isiklikkuse põhimõte
  - Tervikliku kaitse põhimõte
  - Kahjuliku mõju vähendamise põhimõte
  - Koostööpõhimõte.
- Määrata vastutav juhatuse liige, kes peab läbima korrapäraselt koolituse.

Millised on peamised kohustused? (2)

- Rakendada alaliselt asjakohaseid ja proportsionaalseid tehnilisi, tegevuslikke ning korralduslikke turvameetmeid:
  - Mis tulevad määrusest "Võrgu- ja infosüsteemide küberturvalisuse nõuded":
    - Esmased turvanõuded kõigile kohuslastele;
    - E-ITS või ISO/IEC 27001 standardi järgimise kohustus alates keskmisest suurusest.
    - Määruses võib võtta arvesse tegevusalasid.
- NB! Kui teenuseosutaja volitab süsteemi haldamise teisele isikule või majutab süsteemi teise isiku juures, vastutab teenuseosutaja selle eest, et teine isik tagab süsteemi turvameetmete rakendamise.

Millised on peamised kohustused? (3)

- Teavitada (olulise mõjuga) küberinsidendist RIA-t viivitamata, kuid hiljemalt 24h pärast teada saamist;
- Edastada viivitamata, kuid hiljemalt 72 tundi pärast olulise mõjuga küberintsidendist teada saamist intsidenditeade;
- Esitada RIA taotlusel vahearuanne olulise mõjuga küberintsidendi lahendamise seisu kohta;
- Teavitada mõistliku aja jooksul isikut, keda olulise mõjuga küberintsident või oluline küberoht võib mõjutada, või avalikkust, kui mõjutatud isikuid ei ole võimalik eraldi teavitada;
- Esitada ühe kuu jooksul RIA-le lõppraport.
- + Vabatahtlik teavitamine

Järelevalve

- Teostab Riigi Infosüsteemi Amet
- Eel- ja järelkontroll
- Võib teatud tingimustel võib küberintsidendi korral vahetu kõrgendatud ohu tõrjumiseks või korrarikkumise kõrvaldamiseks süsteemi kasutamist või süsteemile juurdepääsu piirata
- Kohapealne kontroll ja kaugjärelevalve, s.h pisteline järelevalve
- Sihipärased turvaauditid (kulu!)
- Turvalisuse kontrollid
- Hoiatused ja ettekirjutused

Tagajärjed ja karistused

- RIA-l õigus nõuda:
  - loa väljastajalt teenuse või tegevuse sertifikaadi või loa ajutist peatamist;
  - üliolulilselt üksuselt juhatuse liikme volituste ajutist peatamist.
- Sunniraha igakordse ülemmääraga 70 000 eurot.
- Trahvid:
  - Üliolulisel üksusel kuni 10 000 000 eurot või kuni 2 protsenti üliolulise üksuse eelmise majandusaasta ülemaailmsest aastasest kogukäibest;
  - Olulisel üksusel kuni 7 000 000 eurot või kuni 1,4 protsenti olulise üksuse eelmise majandusaasta ülemaailmsest aastasest kogukäibest.

EL-I küberkerksuse määrus

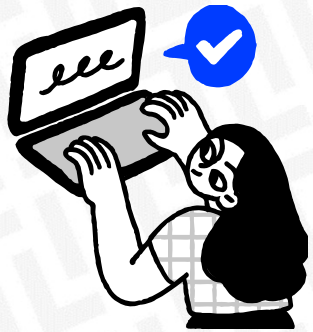
- Määrus (EL) 2024/2847, 23. oktoober 2024, digielemente sisaldavate toodete horisontaalsete küberturvalisuse nõuete kohta.
- Eesmärk on tagada toodete küberturvalisus kogu tarneahelas ja kogu nende elutsükli vältel.
- See sätestab:
  - digitaalsete elementidega toodete turul kättesaadavaks tegemise eeskirjad;
  - digitaalsete elementidega toodete kavandamise, arendamise ja tootmise olulised küberturvalisuse nõuded;
  - haavatavustega tegelemise protsesside olulised küberturvalisuse nõuded;
  - turujärelevalve, sealhulgas seire ja jõustamise eeskirjad.

Mõju ettevõtetele

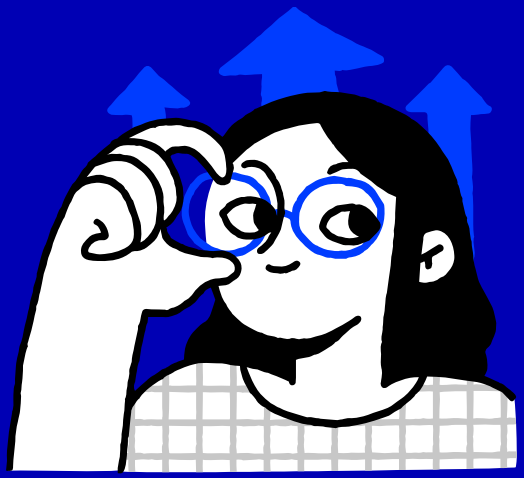
- Ettevõtted peavad suutma kõik selle ära rakendada
- Palju regulatsiooni on otsekohalduv
- Samal ajal kohalikud eripärad
- Otsekohalduvad rakendusaktid
- Topeltkohustused
- Järelevalve asutuste paljusus
- Tarneahela osapoolte vastutus
- Standardid ei jõua järgi

Mis järgmiseks?

- Eesti KüTS-i muutmine
- Lihtsustamine: digivaldkonna omnibuss töös, s.h ühtne intsidentide teavituspunkt
- Muudatused seoses EL-I küberturvalisuse määruse läbivaatamisega
- NIS3?

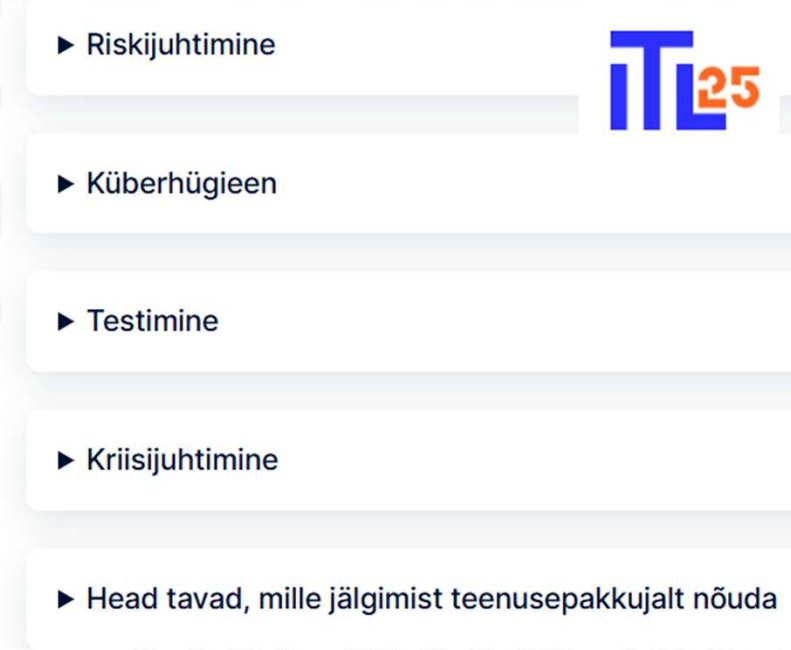


Praktilist



Kust leida tuge?

- ITL-i kübertugi:
  - Soovitused ettevõtjatele
  - Head tavad
- RIA materjalid
  - Nõuanded
  - Portaal ITvaatlik
- Küberturvalisuse tooteid ja teenuseid pakkuvad ettevõtted
- Digiriigi Akadeemia https://digiriigiakadeemia.ee/



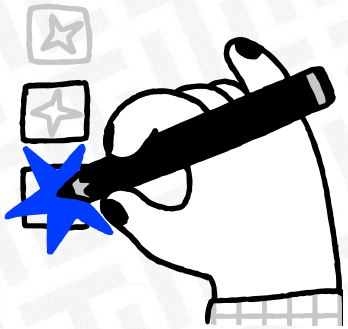
Eesti CyberTech klaster

ESTONIAN CYBERTECH CLUSTER

- Küberturvalisuse klaster ITL-i all alates 2024. aastast
- Esindab enam kui 20 küberturvalisuse ettevõtet
- Rahvusvahelistumisele orienteeritud: keskendunud rahvusvahelisele koostööle ja skaleeritavatele küberturvalisuse lahendustele.
- Platvorm piiriüleste pilootprojektide, oskuste arendamise ja kiire innovatsiooni jaoks.

https://itl.ee/cybertech/

Soovitused



- Hakata otsast pihta:
  - Kas olete subjekt;
  - Välja töötada ja rakendada küberturvalisuse ja intsidendi halduse korrad;
  - Määrata juhatuse liige.
- Vajalik on:
  - tõsta töötajate teadlikkust ja oskusi;
  - luua ja regulaarselt harjutada kriisiplaane;
  - investeerida andmete varundamisse ja turvalisse autentimisse;
  - teha koostööd usaldusväärsete tehnoloogiapartneritega.
- Andke julgelt teada muredest.
  - S.h KüTS küsimused!

Aitäh!

Keilin Tammepärg

ITL-i õigus- ja poliitikavaldkonna juht

keilin.tammeparg@itl.ee

5060113

www.itl.ee