EESTI
CYBERTECH
KLASTER

Küberkerksus juhile

Seminar Eesti Mööblitööstuse Liidule

19.11.2026

26 aastat tehnoloogiasektori edendaja

SISERIIKLIKUD KOOSTÖÖPARTNERID

- Ministeeriumid
  Riigiasutused
- Kutse- ja kõrgkoolid
- SA — Valdkondlikud sihtasutused
- Teised erialaliidud
- Startup kogukond

131 liiget

70% sektori käibest

Tööjõud ja haridus

Poliitika ja ärikeskkond

Äriarendus ja eksport



Ekspertide tutvustus



Kalmer Päts
SOCaaS tootejuht

Telia

Ekspert



Jaan Vahtre
Küberturvalisuse valdkonna juht

KPMG

Ekspert



Livio Nimmer
Juhtivaudiitor

OIXIO

Ekspert



Anett Numa
Rahvusvaheliste suhete juht

NEVERHACK ESTONIA

Ekspert



Markus Ilmar Münzer
Tegevjuht

risksight

Moderaator

Seminari põhisõnumid

01 Küberrisk on äririsk

Küberintsident mõjutab eelkõige tootmist, tarneid ja kliendisuhteid. Seetõttu on see juhtkonna teema.

02 Esmalt äri, seejärel turvalisus

Hea küberturvalisuse taseme saavutamiseks peab olema hea ülevaade ärist endast – varadest, äriprotsessidest, prioriteetidest jne.

03 Nõuete täitmine ei taga kaitset

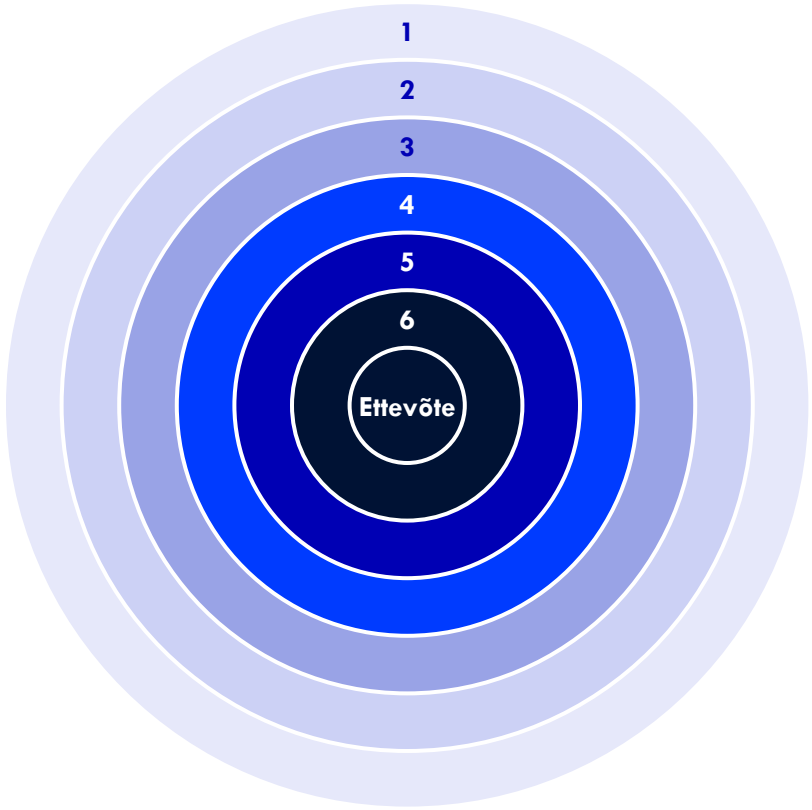
Dokumendid ja turvalahendused on vajalikud, kuid nende toimimist tuleb kontrollida.

04 Samm-sammult areng

Esmalt tasub ette võtta kõige odavamad, kuid tõhusamad meetmed.

Telia KPMG OIXIO NEVERHACK ESTONIA risksight

Seminari ülesehitus



TEEMA	KAITSEKIHT	
01 Juhtimine ja riskid	1 2	Juhtimine Tuvastamine
02 Inimesed ja kultuur	3	Kaitsmine
03 Intsident ja talitluspidevus	4 5 6	Avastamine Reageerimine Taastamine
04 Kaitsemeetmed ja investeeringud	3	Kaitsmine

IGAS TEEMAS

1 Olukord	2 Hääletus	3 Ühisarutelu	4 ITL'i soovitus

EESTI
CYBERTECH
KLASTER

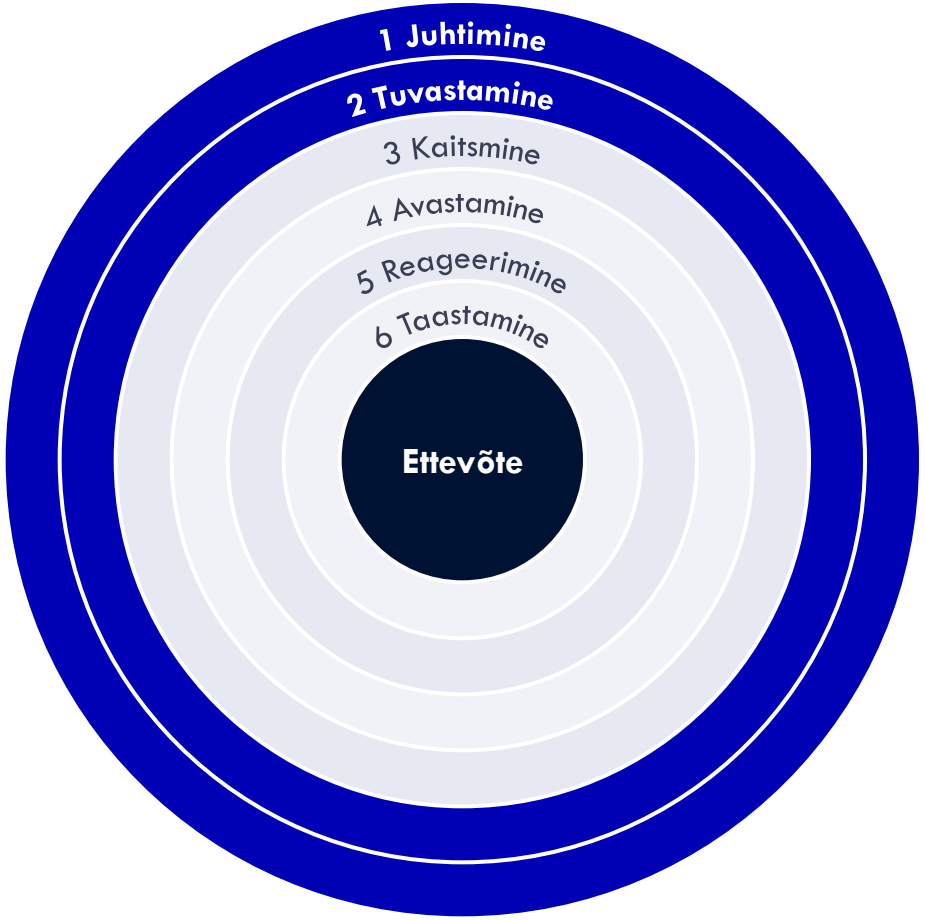
01

Juhtimine ja riskid

Ettevõtte suurim klient saadab tarnijatele küberturvalisuse küsimustiku ja ootab vastust 2 nädala jooksul.

ITL soovitus

Küberturvalisuse eest vastutab juhtkond. Esimese sammuna koostatakse ülevaade IT-varadest ja sõltuvustest ning lepitakse kokku vastutaja.



Sinised kihid: seda tugevdab soovitus

EESTI
CYBERTECH
KLASTER

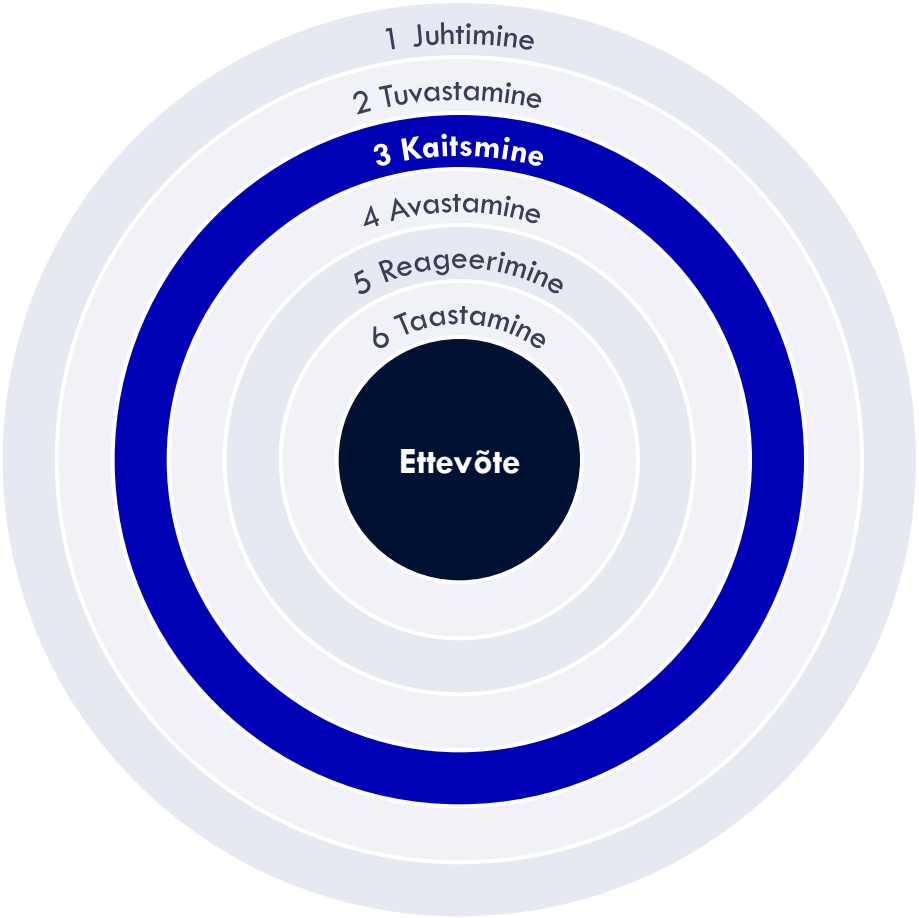
02

Inimesed ja kultuur

Ettevõttes korraldati 2 aastat tagasi ühekordne küberturvalisuse koolitus. Vahepeal on lisandunud uusi töötajaid ja petukirjad on muutunud usutavamaks. Eelmisel nädalal sisestas üks töötaja oma parooli võltslehele.

ITL soovitus

Küberteadlikkus kujuneb järjepideva koolituse, õppuste ja juhtkonna eeskuju kaudu. Ühekordne koolitus töötajate käitumist püsivalt ei muuda.



Sinised kihid: seda tugevdab soovitus

EESTI
CYBERTECH
KLASTER

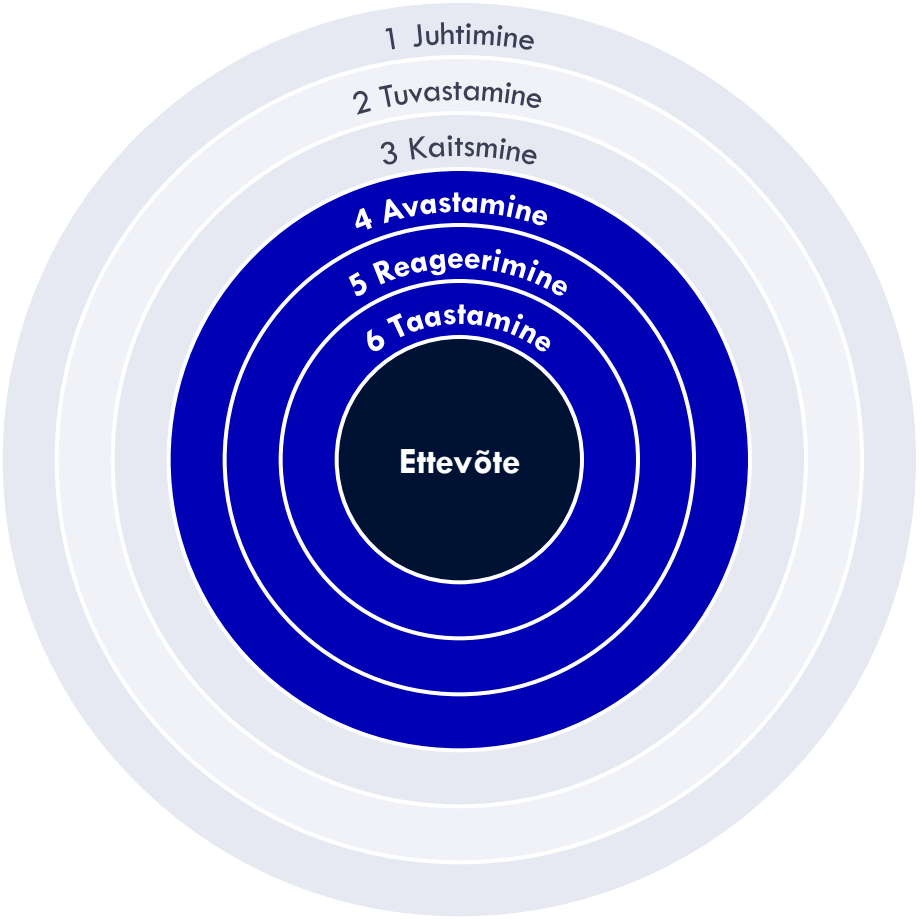
03

Intsident ja talitluspidevus

Esmaspäeva hommikul tootmine seisab. Seadmed ei saa tööülesandeid, ERP ei avane ja ekraanile on ilmunud lunarahanõue. Reedel on kokku lepitud suur tarne.

ITL soovitus

Tegevused intsidendi esimestel tundidel lepitakse kokku enne intsidenti. Taastumine võib kesta nädalaid, mistõttu varuplaan koostatakse aegsasti.



Sinised kihid: seda tugevdab soovitus

EESTI
CYBERTECH
KLASTER

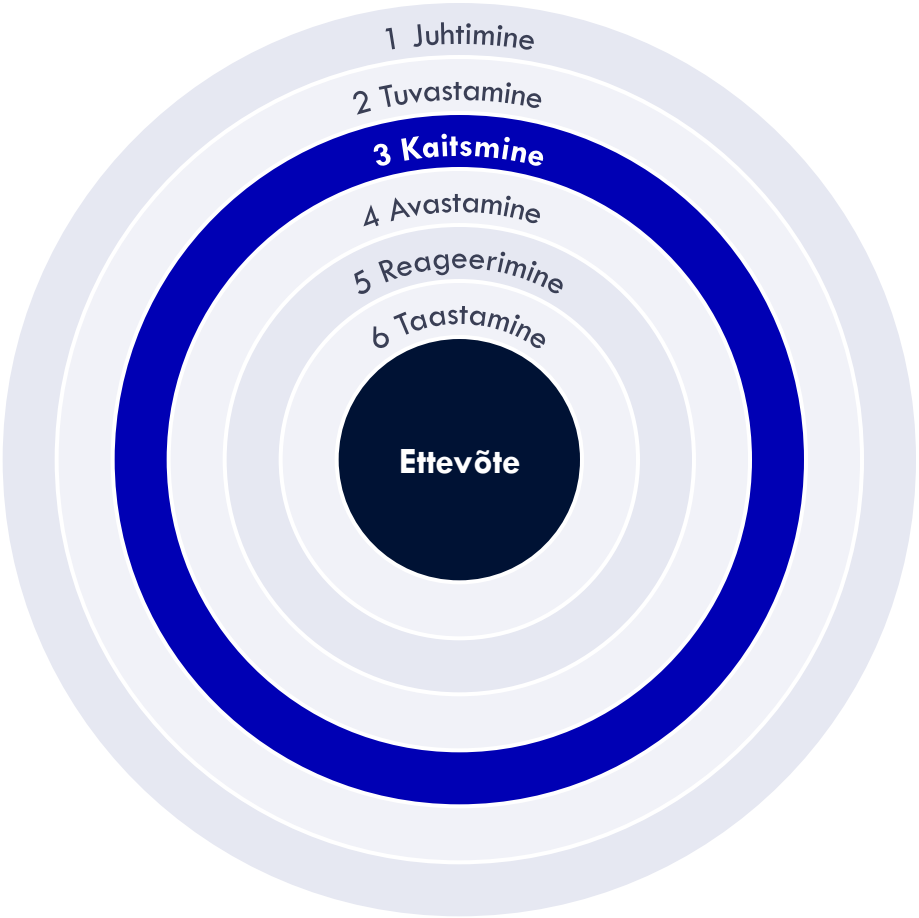
04

Kaitsemeetmed ja investeeringud

IT-teenusepakkuja kinnitusel on kõik nõuded täidetud. Juhatus on eraldanud eelarve ühele uuele meetmele, milleks võib olla turvatarkvara, küberkindlustus või koolitus.

ITL soovitus

Investeeringu valikul lähtutakse riskist ja ettevõtte võimekusest meedet hallata.
Meetmete toimimist kontrollitakse regulaarselt.



Sinised kihid: seda tugevdab soovitus

Kokkuvõte



JUHTIMINE

Varad, sõltuvused ja vastutus on teada.



INIMESED

Teadlikkust arendatakse järjepidevalt.



INTSIDENT

Esimesed sammud ja varuplaan on kokku lepitud.



INVESTEERINGUD

Meetmed valitakse riski alusel ja nende toimimist kontrollitakse.

Telia KPMG OIXIO NEVERHACK ESTONIA risksight

Kontrollnimekiri

01

Hinnake oma riskitaset

- ☐ Millised IT-varad ettevõttel on ja kus need asuvad?
- ☐ Millised 3 süsteemi või partnerit on tootmisele ja müügile kriitilised?
- ☐ Mis juhtuks, kui need oleksid nädal aega kasutamatud?

02

Määrake vastutaja

- ☐ Kes juhtkonnas vastutab küberriskide eest ja kas ta teab seda?
- ☐ Kes on IT-poolne kontaktisik?
- ☐ Millal arutas juhtkond küberriske viimati?

03

Arendage teadlikkust järjepidevalt

- ☐ Kas töötajaid, sh uusi töötajaid, koolitatakse regulaarselt?
- ☐ Kas koolitus ja õppused lähtuvad tegelikest riskidest?
- ☐ Kas kahtlusest ja eksimusest teatamine on lihtne?

04

Koostage intsidendiplaan

- ☐ Kellele helistatakse esimesena, ka väljaspool tööaega?
- ☐ Kes otsustab ja kuidas jätkatakse tootmist ilma IT-ta?
- ☐ Kas varukoopiate taastamist on proovitud?

05

Esitage IT-le õiged küsimused

- ☐ Mida IT-leping intsidendi korral katab?
- ☐ Kuidas kontrollitakse, et kaitsemeetmed töötavad?
- ☐ Mis valdkonnas oleks vaja kõige rohkem tähelepanu turvalisuse vaates?

Telia KPMG OIXIO NEVERHACK ESTONIA risksight

ITLi sari TOP 5 küberohtu 2026. aastal

Mis see on?

- ITLi seminaride sari, mis avab ettevõtete juhtidele ja spetsialistidele 2026. aastal olulisemaid küberohte süvitsi.
- Sai alguse ITLi liikmete tippjuhtide arutelust ja jätkub praktiliste veebiseminaridena.
- Veebinaride järelevaatamine:

Veebinaride järelevaatamine:

- https://itl.ee/uudised/top-5-kuberohtu-seminaride-sari/



EESTI
CYBERTECH
KLASTER

Aitäh!

Kontaktid:
Doris Põld, tegevjuht
doris.pold@itl.ee

Grete Soares de Camargo
CyberTech klastri juht
grete.s.camargo@itl.ee
+372 5800 9836

Abimaterjalid:
Kübertugi: https://itl.ee/kybertugi/
Eesti CyberTech klaster: https://itl.ee/cybertech/