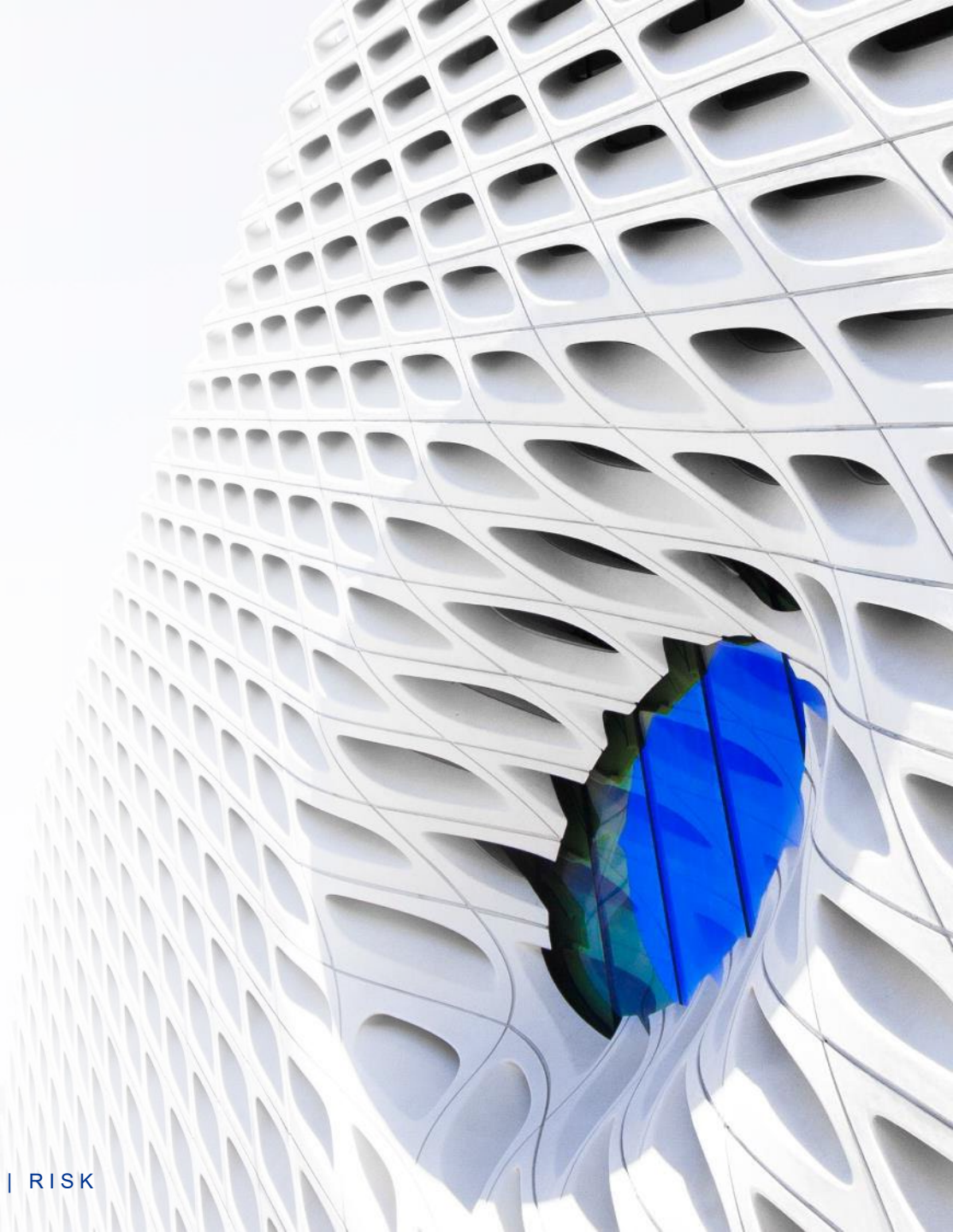
KPMG Cyber

Eesti ettevõtete küberturvalisuse uuring 2022

KPMG Baltics OÜ



DEALS | CYBER | DIGITAL | RISK

Uuringu lühikokkuvõte

Uuringu tulemuste põhjal saame järeldada, et:

01 **Enamus** Eesti suurettevõtete ja tervishoiuettevõtete juhte **teadvustavad intsidentide võimalikku negatiivset mõju.**

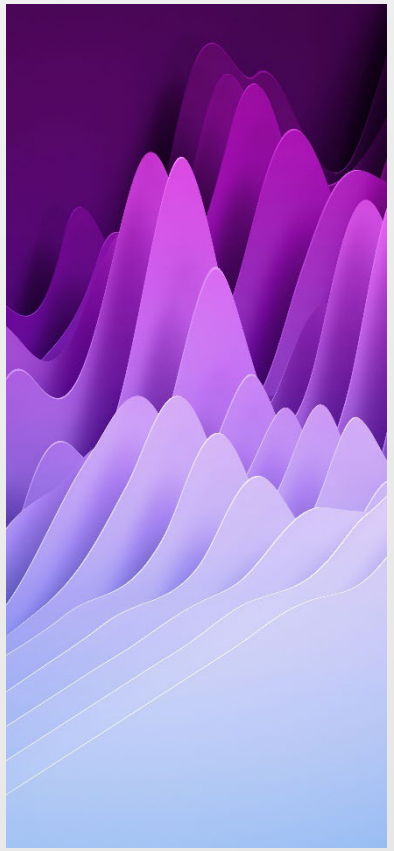
02 **Kolmandik** vastanud juhtidest **mainis infoturbe intsidentide arvu kasvu** viimase aasta jooksul.

03 Peaaegu **iga teine** suurettevõte **on kannatanud** intsidentide tõttu **rahalist kahju**.

04 Infoturbe intsidentide mõju tervishoiuettevõtetele on olnud teiste sektoritega võrreldes **väiksem**. Kuid ka selles sektoris on märgata intsidentide arvu **kasvu**.

05 Ettevõtete seas on **levimas ekslik arusaam, et IT-teenuste väljast tellimisel** (ehk ettevõtte IT-ülesannete delegeerimisel lepingupartnerile) **kaasneb** tellitava teenusega automaatselt ka **küberturvalisuse tagamise kohustus** lepingupartnerile.

06 **Paljudes ettevõtetes puudub strateegiline ametikoht või roll infoturbe ja küberturvalisuse optimaalsemaks juhtimiseks** (nt infoturbejuht). Kui ettevõttes puudub infoturbe tagamiseks keskne lüli, siis puudub ka kõikehõlmav ja sidus ülevaade võimalikest riskidest.

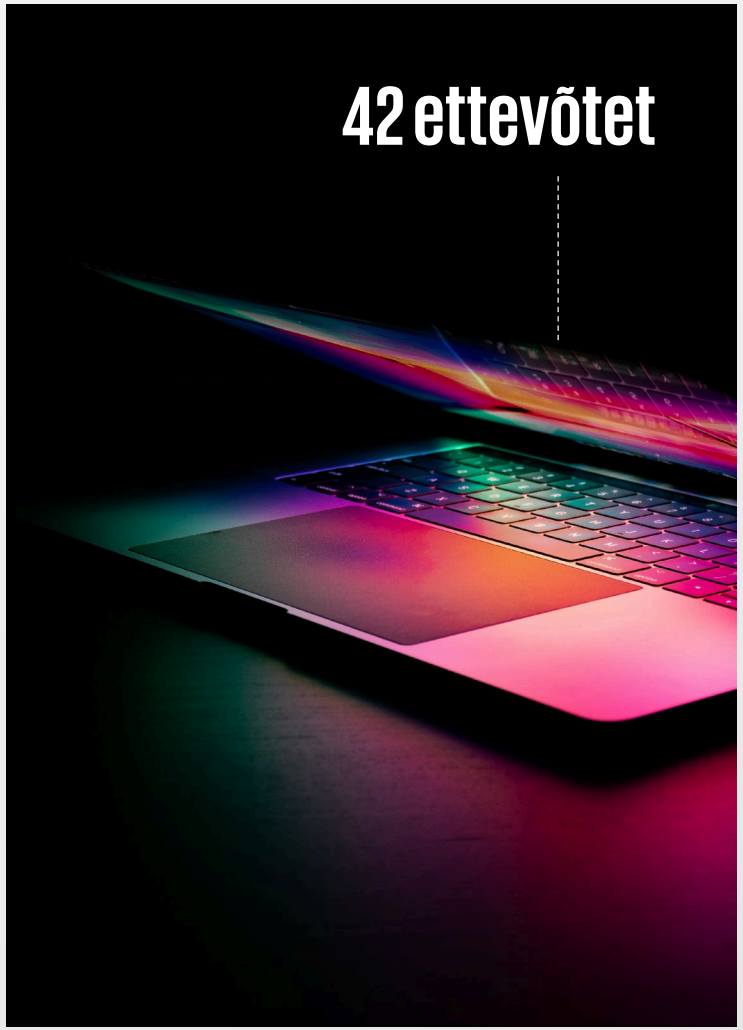


Uuringu taust

KPMG Baltics viis koostöös Äripäevaga **läbi infoturbe ja küberturvalisuse uuringu Eesti juhtivate ettevõtete seas.** Kaardistati Eesti ettevõtete küberturvalisuse taset, infoturbe ülesehitust ja hoiakuid ettevõtete juhtide seas.

Kokku küsitleti 42 ettevõtet.

Uuring viidi läbi kahes etapis 2022. aasta esimeses kvartalis.



Esimene etapp:

- Küsitleti ettevõtete juhte 300 suurima Eesti tööandja hulgast.
- Tulemused peegeldavad infoturbe ning küberturvalisuse seisu Eesti suurtes ettevõtetes.
- Küsitlusele vastas 22 ettevõtet.

Teine etapp:

- Eraldiseisvalt küsitleti ettevõtete juhte tervishoiusektorist.
- Sektoris on kehtestatud kõrgemad infoturbe ja küberturvalisuse nõuded delikaatsete isikuandmete töötlemise tõttu.
- Küsitlusele vastas 20 ettevõtet/organisatsiooni.

Kasutatavad mõisted

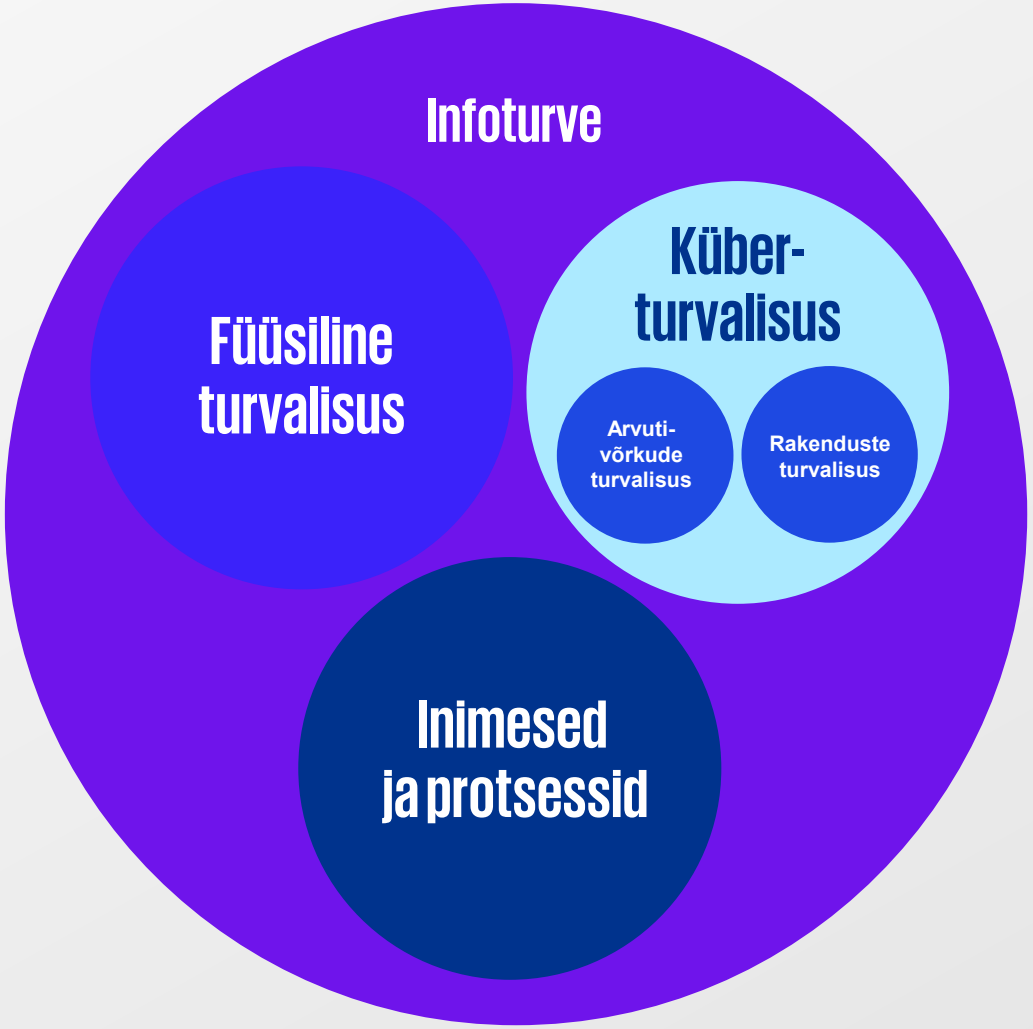
Antud uuringu kontekstis käsitleme mõisteid „infoturve“ ning „küberturvalisus“ alljärgnevalt:

Infoturve

hõlmab infotkandvate andmete konfidentsiaalsuse, terviklikkuse ja käideldavuse kaitsmist, olenemata andmekandja vormist (elektrooniliselt, paberkandjal jm).

Küberturvalisus

hõlmab andmete ja seadmete konfidentsiaalsuse, terviklikkuse ning käideldavuse kaitsmist rünnakute eest küberruumis.



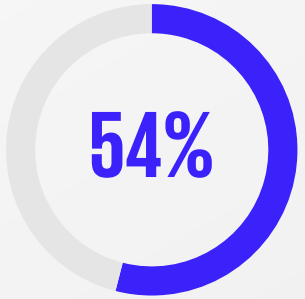
KPMG Cyber

Uuringu tulemused – I etapp*

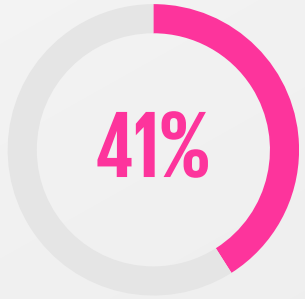
***I. etapi käigus küsitleti 22 ettevõtte juhti 300 suurima Eesti tööandja hulgast.**

Küberintsidentide ohu ja mõju teadvustamine (suurettevõtted)

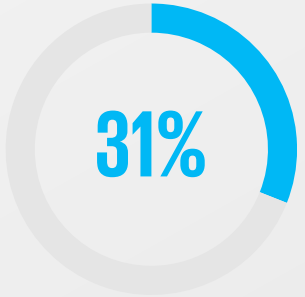
- **Küberintsidentide võimalikku negatiivset mõju** ettevõtete põhitegevusele **teadvustab** valdav **enamus ettevõtete juhte.**
- Ettevõtete juhtid on seisukohal, et **küberintsidentide realiseerumise oht** on täna **pigem tõenäoline.**
- Viimaste aastate küberintsidentide arvu märgatav tõus ning küberintsidentide iseloom viitavad selgelt, et võimalikke **ohvreid valitakse tänapäeval ka juhuslikkuse alusel.**



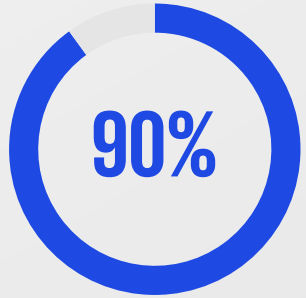
vastanutest on **kannatanud** küberintsidentide tõttu **ajalist kahju.**



vastanutest on **kannatanud** küberintsidentide tõttu **rahalist kahju.**



vastanutest **kinnitasid**, et viimase kahe aasta jooksul on **küberintsidentide arv sagenenud**.



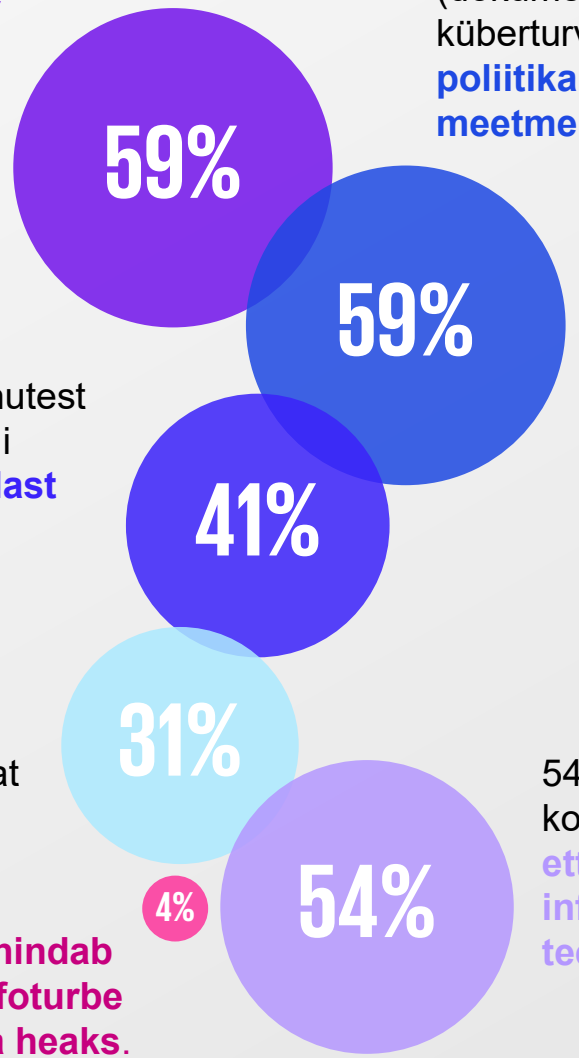
vastanutest **tunneb muret võimalike intsidentide pärast**, mis võivad tulevikus juhtuda.

Küberintsidentideks ettevalmistumine (suurettevõtted)

- **Vähem kui kolmandik** ettevõtetest **omavad** strateegilise **infoturbe eest vastutava töötaja ametikohta/rolli** (nt infoturbejuht).
- **Vaid 4%** küsitletutest **hindas** oma ettevõtte infoturbe võimekust **väga heaks.**
- **Enam kui pooled** vastanutest nentisid, et nende ettevõttes **vastutab infoturbe eest teenuspartner**. KPMG kogemuse kohaselt arvatakse sageli ekslikult, et IT-teenuseid tagavale teenuspartnerile peaks automaatselt kohalduma ka ettevõtte küberturvalisuse tagamise kohustus.

59% vastanutest hindab oma ettevõtte **infoturbe võimekust heaks** (skaalal: väga hea, hea, keskmine, puudulik).

59% on rakendanud enda ettevõttes ametlikult (dokumenteeritul kujul) küberturvalisust tagavaid **poliitikaid, protsesse ning meetmeid.**



41% vastanutest **omab** eraldi **infoturbealast eelarvet**.

31%vastanutest **omab ettevõttes strateegilise infoturbe** eest vastutavat **rolli** (nt infoturbejuht).

54% vastanutest konstateerib, et **ettevõttes tagab infoturvet teenuspartner**.

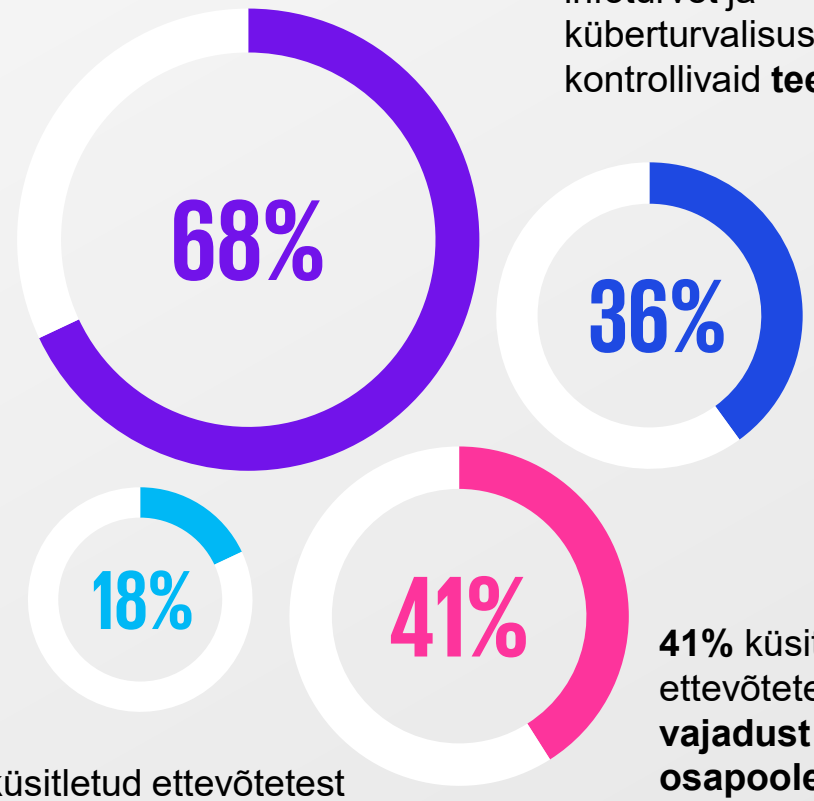
4% vastanutest **hindab** oma ettevõtte **infoturbe võimekust väga heaks**.

Infoturbe ja küberturvalisuse kontroll sõltumatu osapoole poolt (suurettevõtted)

- **Alla poole** vastanutest (41%) on hinnanud enda **iseseisvat võimekust** infoturbe ja küberturvalisuse tagamisel piisavaks**.**
- Jätkuvalt on infoturbe tagamisel nõrgimaks lüliks inimene. Pisut enam kui kaks kolmandikku küsitletud ettevõtetest **(68%) on korraldanud oma töötajatele** viimase aasta jooksul **infoturbealaseid koolitusi**.
- Vaid **väike osa** küsitletud ettevõtetest (18%) **on tellinud tehnilisema iseloomuga teenuseid,** nt läbistustestimine.
- **Populaarseimad sisse ostetavad teenused** on isikuandmete kaitse (vastavus GDPR-ile), ISKE/ISO27001 vastavusauditid, õngitsusrünnaku simuleerimine.

68% küsitletud ettevõtteid on **korraldanud** enda töötajatele viimase aasta jooksul **infoturbealaseid koolitusi**.

36% küsitletud ettevõtetest **on** viimase aasta jooksul **sisse ostnud sõltumatu osapoole** teostatavaid, infoturvet ja küberturvalisust kontrollivaid **teenuseid**.



18% küsitletud ettevõtetest on **soetatud tehnilisema iseloomuga teenuseid** – näiteks arvutivõrkude tehnilise läbistustestimine (ingl k *Penetration Testing*).

41% küsitletud ettevõtetest **ei näe vajadust sõltumatu osapoole** poolt teostatavate **teenuste sisse ostmiseks.**

Uuringu tulemused – I etapp*

Kokkuvõte: 22 ettevõtte juhti 300 suurima Eesti tööandja hulgast

01

Olgugi, et juhid peavad infoturvet ja küberturvalisust oluliseks, viitavad uuringu tulemused sellele, et **arvamus ettevõtte infoturbealasest seisust ei pruugi ühtida reaalse olukorraga.** Seda väidet kinnitavad ka KPMG poolt 2021-2022 aastatel teostatud ettevõtete infoturbe ja küberturvalisuse küpsustaseme hindamiste tulemused – juhtkond kipub alahindama riske ja ülehindama olemasolevat taset.

02

Sageli puudub ettevõttes strateegiline ametikoht infoturbe ja küberturvalisuse optimaalsemaks tagamiseks (nt infoturbejuht). Infoturbejuht mõistab ettevõtet mõjutatavaid riske (sh seoseid tehnoloogia ja äririskide vahel) ning juhib vajalike turvatehnoloogiate ja protsesside kasutuselevõttu, eesmärgiga minimeerida organisatsioonis riskide avaldumist või riskide avaldumisest tulenevaid tagajärgi. Kui ettevõttes puudub infoturbe tagamiseks keskne lüli, siis puudub ka kõikehõlmav ja sidus ülevaade riskidest. Kui infoturbejuhi rolli täidab põhitöö kõrvalt näiteks IT-juht, kasvab oht fookuse hajumisele ja alajuhtimisele.

03

Ettevõtete seas on levimas arusaam, et IT-teenuste sisse ostmisel kaasneb teenusega ka küberturvalisuse tagamine ettevõttes – antud arusaam on tihtipeale ekslik. Kui olemasolev IT-teenuste leping ei kajasta spetsiifiliselt küberturvalisuse tagamise nõuet, siis pole tegelikult lepingupartneril ka vastavat kohustust.

04

Sõltumatu osapoole poolt teostatavaid infoturbe kontrolle tellitakse küsitletud ettevõtete seas pigem vähe (nt IT-audit, IT-riskianalüüs, tehniline läbistustestimine jm). Muuhulgas näeb suur osa küsitletud ettevõtetest, et sõltumatu osapoole teenuste sisse ostmine ei ole vajalik. Samas on just sõltumatud turvalisuse kontrollid need, mis annavad kõige objektiivsema hinnangu ettevõtte infoturbe hetkeolukorrale ning investeeringute asjakohasusele.

KPMG Cyber

Uuringu tulemused – II etapp*

***II. etapi käigus küsitleti 20 ettevõtte juhti Eesti tervishoiusektorist.**

Infoturbe ja küberturvalisuse kontroll sõltumatu osapoole poolt (tervishoid)

Infoturvet peab oluliseks ka valdav enamus tervishoiu ettevõtete juhte.

Kuna infoturbe tagamise eest vastutab kolmel juhul neljast teenuspartner, on tõenäoline, et juhtkond on andmete töötlemisega seotud riskid ja nende ennetamise delegeerinud majast välja. Koostöös majasisese infoturbejuhiga, võib see mudel hästi toimida.

60% küsitletud tervishoiu ettevõtetest on korraldanud enda töötajatele viimase aasta jooksul **infoturbe-alaseid koolitusi**. Seda on 8% vähem, kui uuringu I. etapis kajastatud ettevõtete puhul.

Mudeli puhul, kus infoturbe tagamise eest vastutab teenuspartner, on oluline kontrollida, kas rakendatav infoturbe meetmestik on sobiv ja efektiivne. Selleks sobivad kõige paremini kolmanda osapoole teenused. **On üllatav, et paljud tervishoiu ettevõtted**, kus reeglina kehtivad rangemad nõuded infoturbele (seoses delikaatsete isiku-andmete töötlemisega), **ei näe vajadust sõltumatu osapoole poolt teostatavate infoturbealaste kontrollide järele.**

Kõigest 20%

küsitletud tervishoiu ettevõttetest on viimase aasta jooksul ostnud sisse sõltumatu osa-poole poolt teostatavaid, infoturvet ja küber-turvalisust kontrollivaid teenuseid. See on tervelt 16% vähem, kui uuringu I. etapis kajastatud ettevõtete seas.

Eriti ohtlik on olukord, kus ettevõttes puudub **infoturbejuht** või inimene, kes täidab sarnast rolli, **sõltumatuid osapooli** ei kaasata, **töötajaid** ei koolitata ning juhtkond on seisukohal, et IT teenuspartner katab ka infoturbega seotud vajadused – **kuigi vastavas lepingus seda sätestatud pole**. Delikaatsete isikuandmete töötleja jaoks on võimalikud tagajärjed tõenäoliselt katastroofilised.

50%

küsitletud tervishoiu ettevõtetest **ei näe vajadust** sõltumatu osapoole poolt teostatavate teenuste sisse ostmiseks. Suur osa küsitletavatest ettevõttetest on hinnanud seega enda iseseisvat võimekust infoturbe ja küberturvalisuse tagamisel piisavaks.

Küberintsidentide ohu ja mõju teadvustamine (tervishoid)

Tervishoiu sektori ettevõtete ründamine on ründajatele tihtipeale eetika küsimus –

on kurjategijaid, kes hoiduvad tervishoiu ettevõtete ründamisest ja ka neid, keda eetika jätab külmaks. Maailmas tõusuteel olev intsidentide arv peegeldub selgelt ka tervishoiu-sektori ettevõtete seas, kuid veidi väiksemas ulatuses.

Küberintsidentide võimalikku negatiivset mõju

tervishoiu ettevõtete põhitegevusele **teadvustab** valdav **enamus** tervishoiu-ettevõtete **juhte. GDPR raames** on isikuandmete varguse korral võimalik trahv märkimisväärselt suur.

10%

vastanud tervishoiu ettevõtetest on **kannatanud** küberintsidentide tõttu **ajalist kahju.**

Ükski vastanud

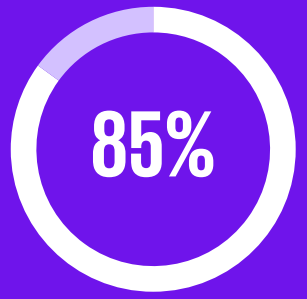
Eesti tervishoiuettevõtete

pole kannatanud

küberintsidentide tõttu **rahalist kahju.**

Tervishoiu ettevõtete seas on

küberintsidentide realiseerumine ning mõju olnud **tunduvalt tagasi-hoidlikum**, kui uuringu I. etapis kajastatud ettevõtete seas.



vastanutest tunneb muret võimalike intsidentide pärast, mis võivad tulevikus juhtuda.

20%

vastanutest **kinnitasid**, et viimase kahe aasta jooksul on **küber-intsidentide arv sagenenud**.

Küberintsidentideks ettevalmistumine (tervishoid)

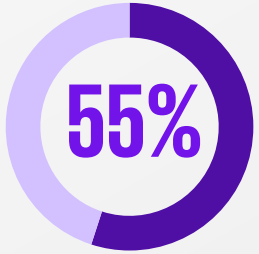
Tervishoiu ettevõtted on oma ette-valmistust puudutavates hinnangutes tagasihoidlikumad kui uuringu I. etapis kajastatud ettevõtted – ligi **2/3** hindab oma organisatsiooni infoturbe võimekust keskmiseks.

65% vastanutest hindab oma ette-võtte infoturbe võimekust **keskmiseks, 30%** hindab võimekust **heaks** ning **5% väga heaks** (skaalal: väga hea, hea, keskmine, puudulik).

Tervishoiu ettevõtete hulgas on infoturbejuhi roll levinum kui teiste sektorite ettevõtete seas. Delikaatsete isikuandmete töötlejatena kohanduvad neile ka rangemad nõuded. Seega on tervishoiu valdkonna organisatsioonid rohkem motiveeritud riske maandama.

35% vastanutest omab eraldi **infoturbealast eelarvet**, mis on 6% vähem, kui I. etapis kajastatud ettevõtete seas.

Enamus tervishoiuettevõtteid vastas, et ettevõttes tagab infoturvet teenuspartner. KPMG on küber-turvalisuse teenuste osutamisel täheldanud ettevõtete juhtide seas **laialt levinud arusaama**, et IT-teenuseid tagavale teenuspartnerile peaks automaatselt kohalduma ka ettevõtte **küberturvalisuse tagamise kohustus**. Kahjuks on see arvamus ekslik (välja arvatud juhul kui leping ei sätesta teisiti). **Lõplik vastutus ettevõtte turvalisuse tagamisel lasub alati ettevõtte juhtkonnal, mitte teenuspartneril.**



küsitletud tervishoiuettevõttetest on rakendanud enda ettevõttes ametli-kult (dokumenteeritud kujul) küber-turvalisust tagavaid **poliitikaid**, **protsesse** ning **meetmeid**.

40% vastanutest omab ettevõttes strateegilise infoturbe eest vastutava **töötaja ametikohta/rolli** (nt infoturbejuht) – so. 9% rohkem kui I. etapis kajastatud ettevõtete puhul.

75% vastanutest konstateerib, et **ettevõttes tagab infoturvet teenuspartner.**

Uuringu tulemused – II etapp*

Kokkuvõte (1/2): 20 ettevõtte juhti Eesti tervishoiusektorist

01

Olgugi, et juhid peavad infoturvet ja küberturvalisust oluliseks, viitavad uuringu tulemused sellele, et **arvamus ettevõtte infoturbealasest seisust ei pruugi ühtida reaalse olukorraga.** Seda väidet kinnitavad ka KPMG poolt 2021-2022 aastatel teostatud ettevõtete infoturbe ja küberturvalisuse küpsustaseme hindamiste tulemused – juhtkond kipub alahindama riske ja ülehindama olemasolevat taset.

02

Küberintsidentide mõju on tervishoiu-ettevõtetele olnud tunduvalt väiksem – teadaolevalt on intsidente toimunud vähe ning toimunud intsidentide mõju on olnud tagasihoidlik. Siinkohal jääb aga lahtiseks asjaolu, kas ning kui palju on tervishoiu ettevõtteid mõjutavaid avastamata intsidente (nt lekkinud andmeid), sest suurem osa tervishoiuettevõtted ei teosta sõltumatute kolmandate osapoolte poolt infoturbe kontrolle.

03

Ettevõtete seas on levimas arusaam, et IT-teenuste sisse ostmisel kaasneb teenusega ka küberturvalisuse tagamine ettevõttes – antud arusaam on tihtipeale ekslik. Kui olemasolev IT-teenuste leping ei kajasta spetsiifiliselt küberturvalisuse tagamise nõuet, siis pole tegelikult lepingupartneril ka vastavat kohustust.

Uuringu tulemused – II etapp*

Kokkuvõte (2/2): 20 ettevõtte juhti Eesti tervishoiusektorist

04

Sõltumatu osapoole poolt teostatavaid infoturbe kontrolle (IT-audit, IT-riskianalüüs, tehniline läbistustestimine jm) teostatakse küsitletud tervishoiuettevõtete seas **väga vähe – tervelt 16% vähem**, kui uuringu 1. etapis kajastatud ettevõtete puhul.

05

Pooled küsitletutest ei pea vajalikuks sõltumatu osapoole poolt teostatavate teenuste sisseostu – mis on märgiline: see osakaal on suurem (tervelt 9% võrra), kui uuringu I. etapis kajastatud ettevõtete puhul, kes erinevalt tervishoiusektor-i ettevõtetest, ei töötle reeglina delikaatseid isikuandmeid.

06

Sõltumatud turvalisuse kontrollid need annavad reeglina kõige objektiivsema hinnangu ettevõtte infoturbe hetkeolukorrale ning investeeringute asjakohasusele. Tervishoiuettevõtetes töödeldakse **delikaatseid isikuandmeid**, mistõttu võib eeldada, et tervishoiuettevõtted panustavad infoturbesse rohkem ressursse, kui uuringu I. etapis küsitletud Eesti ettevõtted. Paraku viitavad uuringu tulemused asjaolule, et reaalne seis on hoopis vastupidine – **tervishoiu ettevõtted panustavad infoturbesse keskmiselt vähem ressursse kui uuringu I. etapis küsitletud ettevõtted.**

KPMG Cyber

Avastatud kitsaskohad– KPMG soovitused

Mida teha uuringus avastatud kitsaskohtade parandamiseks?

KPMG soovitused

uuringus avastatud kitsaskohtadest tingitud olukorra parandamiseks

A

Soovitame regulaarselt teostada ettevõtteüleseid IT-auditeid.

IT-audit tuvastab **infoturbealaseid kitsaskohti** ettevõtte **IT ülesehituses** ning **IT halduse korralduses**. Soovitame kaasata antud kontrollide teostamisse sõltumatut ning vastava töökogemuse ja kvalifikatsiooniga kolmanda osapoole esindajat, kuna esineb risk, et enda asutuse töötajad ei oma kvaliteetsete kontrollide teostamiseks vajalikku pädevust. Lisaks võivad töötajad tahtlikult või tahtmata varjata ettevõtte IT infrastruktuuris esinevaid puudusi. IT-auditi käigus soovitame kriitilise pilguga kontrollida kõik **kolmandate osapooltega sõlmitud lepingud** – eelkõige tuleb kontrollida, kas lepingud vastavad IT turvalisuse seisukohast ettevõtte juhtkonna ootustele.

B

Soovitame luua infoturbejuhi ametikoht/roll või kaasata antud rolli täitmisel välist partnerit.

Infoturbejuhi ametikoha loomine, koos kvalifitseeritud inimese värbamise ning vastavate ülesannete määramisega, on suurepärane viis **tugevdada enda ettevõtte infoturbealast olukorda**. Samas ei ole iga ettevõtte puhul otstarbekas luua eraldiseisvalt ametikohta. Infoturbejuhi rolli saab hoolika planeerimise tulemusena delegeerida ka teatud olukordades teistele ettevõtte töötajatele. Tänapäeval on võimalik ka **infoturbejuhi kompetentsi sisse osta** vajalikus ulatuses väliste partnerite kaudu – see on parim võimalik kombinatsioon finantsiliste ressursside kokkuhoiust ning kvalifitseeritud, infoturbealase spetsialisti kaasamisest.

C

Soovitame regulaarselt teostada tehnilisi IT infrastruktuuri turvalisuse teste.

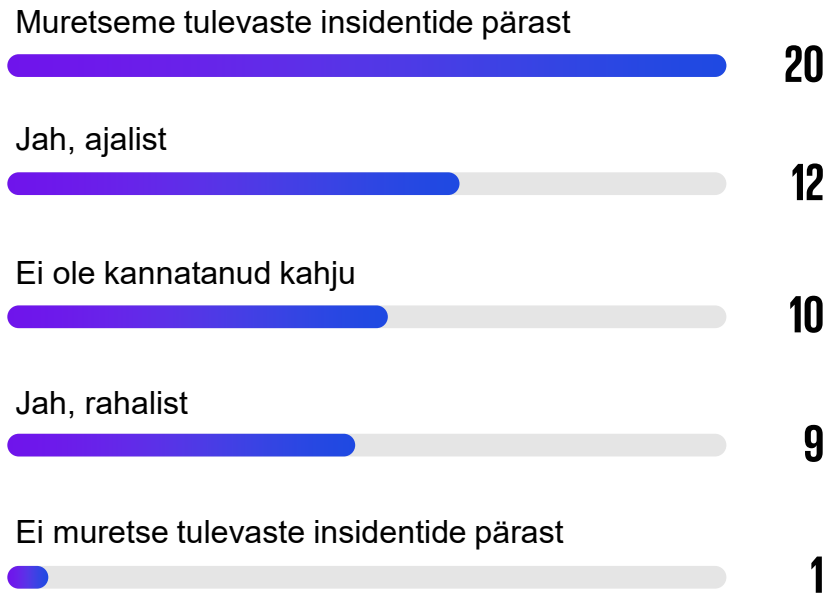
Soovitame IT-auditi käigus teostatavaid toiminguid täiendada tehniliste turvalisuse testidega. Tehniliste kitsaskohtade avastamiseks soovitame teostada ettevõtte IT infrastruktuurile **läbistusteste**. Kui ettevõttel läbistustestide soetamiseks rahalisi vahendeid napib, võib alternatiivina teostada ka **turvanõrkuste skanneerimist**. Mainitud tehnilised testid võimaldavad saada aimu, kas ja kuidas ettevõttes rakendatud tehnilised kaitsemeetmed reaalsuses kasutatavatele ründevektoritele vastu peavad.

KPMG | KPMG Cyber

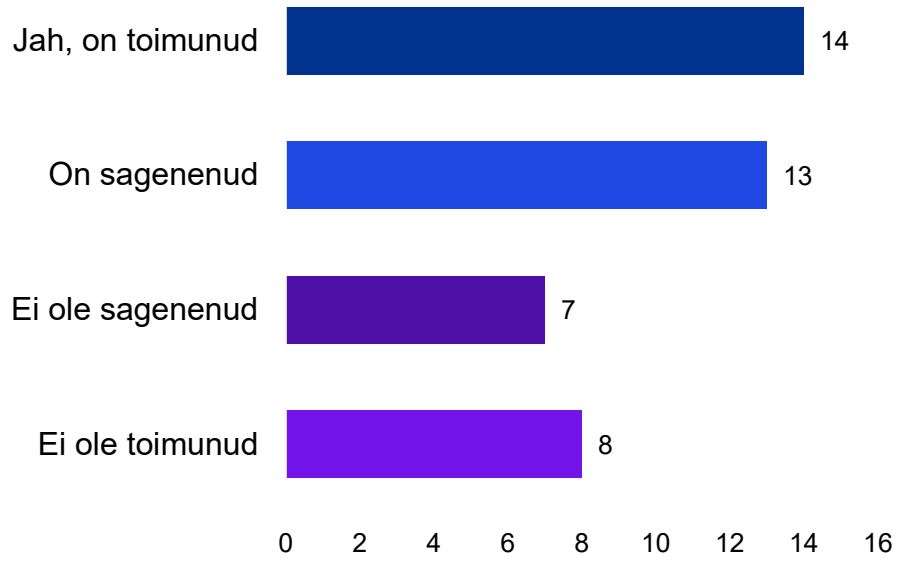
Lisad

Uuringu tulemused – I etapp*

Kas teie ettevõte on kannatanud kunagi ajalist või rahalist kahju seoses küberintsidentidega? Kas muretsete ka täna nende riskide pärast?



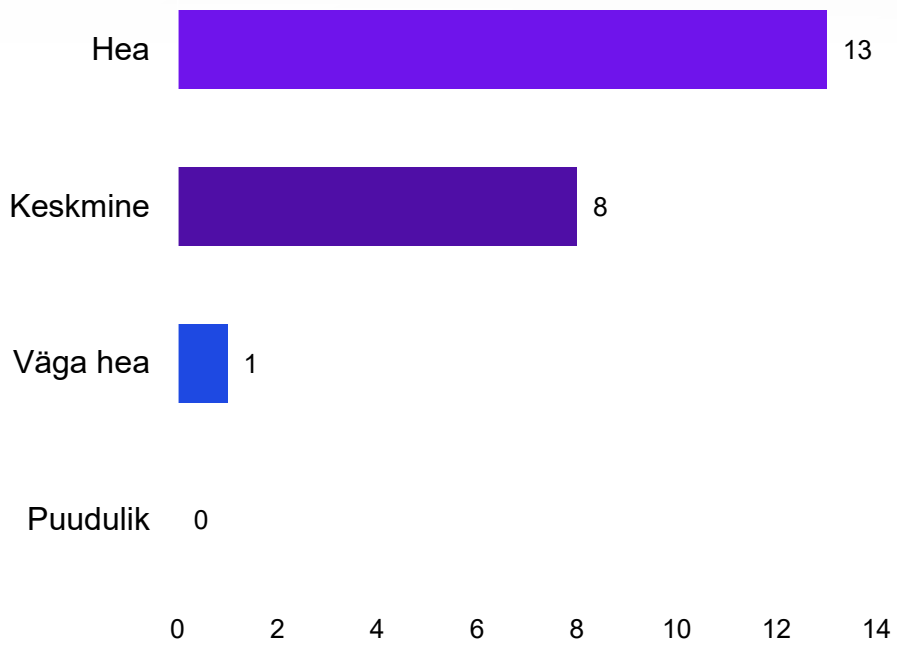
Kas viimase aasta jooksul on teie ettevõttes esinenud infoturbe intsidente? Kas intsidentide arv on sagenenud?



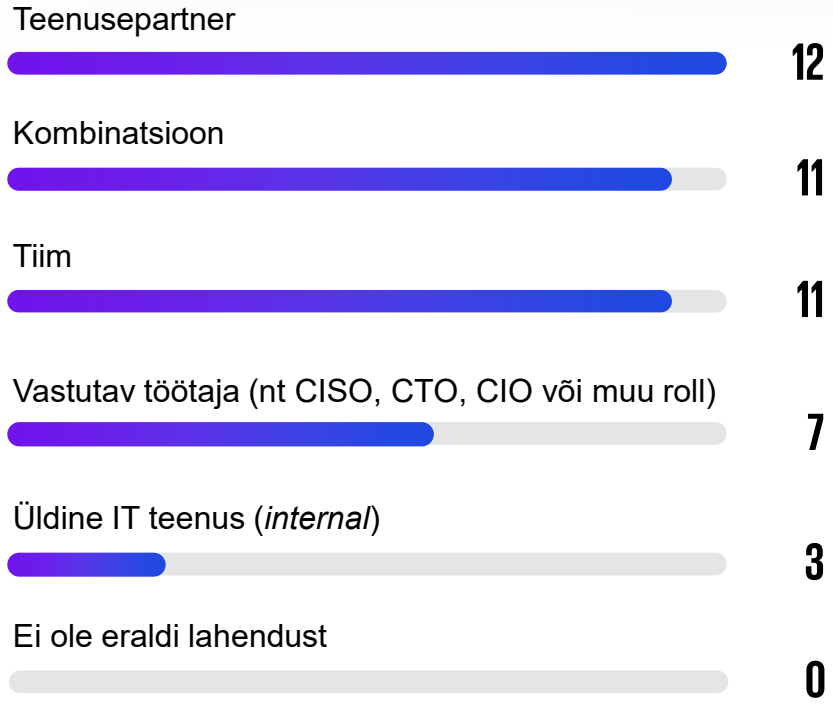
*I. etapi käigus küsitleti 22 ettevõtte juhti 300 suurima Eesti tööandja hulgast.

Uuringu tulemused – I etapp*

Kuidas hindate oma ettevõtte infoturbe võimekust?



Kuidas on teie ettevõttes lahendatud infoturbe tagamine?



*I. etapi käigus küsitleti 22 ettevõtte juhti 300 suurima Eesti tööandja hulgast.

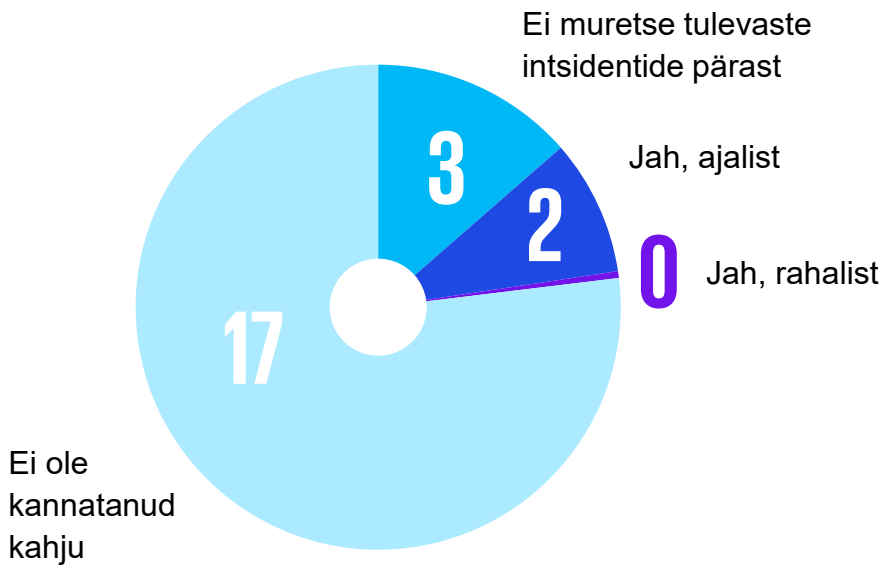
Uuringu tulemused – I etapp*

Kas olete viimase aasta jooksul ostnud küberturvalisuse valdkonna teenuseid? Kui jah, siis milliseid?

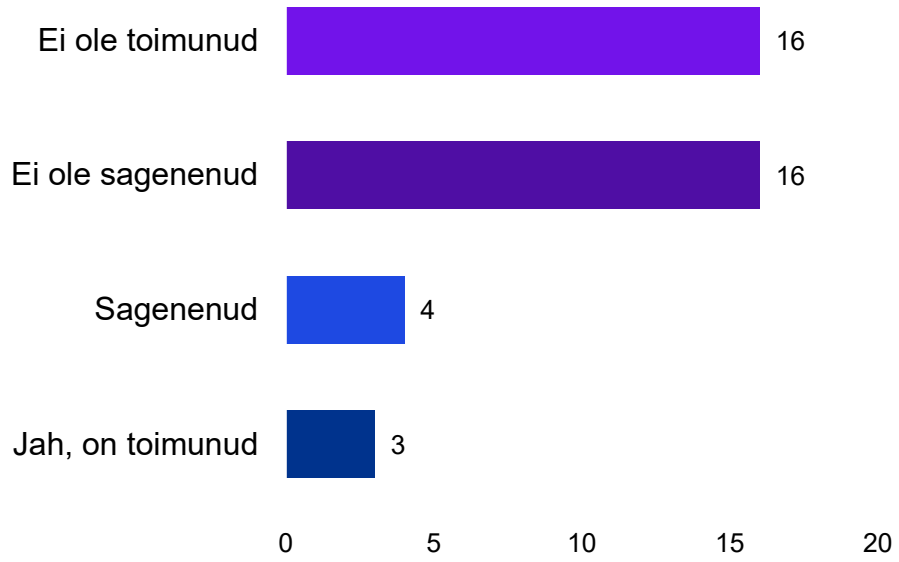
*I. etapi käigus küsitleti 22 ettevõtte juhti 300 suurima Eesti tööandja hulgast.

Uuringu tulemused – II etapp*

Kas teie ettevõte on kannatanud kunagi ajalist või rahalist kahju seoses küberintsidentidega? Kas muretsete ka täna nende riskide pärast?



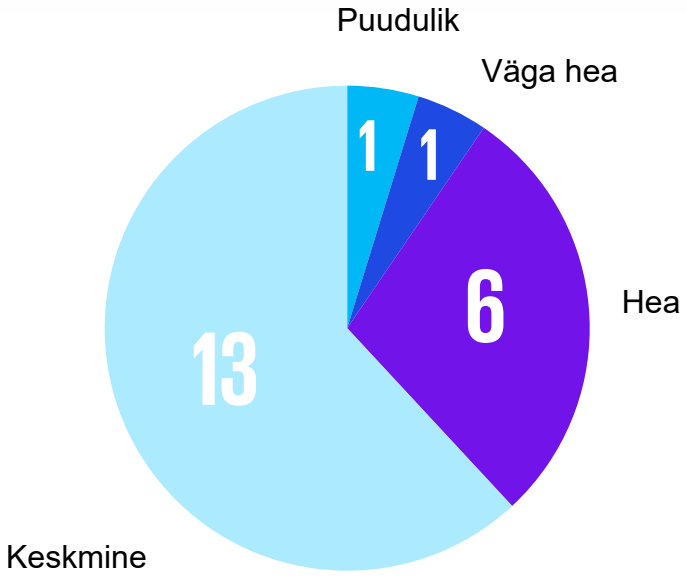
Kas viimase aasta jooksul on teie ettevõttes esinenud infoturbeintsidente? Kas intsidentide arv on sagenenud?



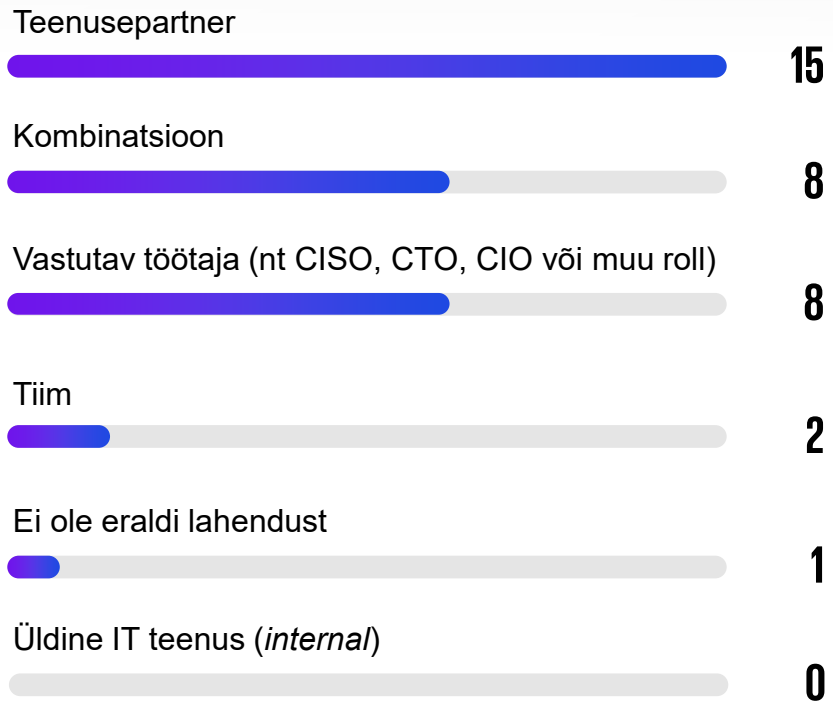
*II. etapi käigus küsitleti 20 ettevõtte juhti tervishoiusektorist.

Uuringu tulemused – II etapp*

Kuidas hindate oma ettevõtte infoturbe võimekust?



Kuidas on teie ettevõttes lahendatud infoturbe tagamine?



*II. etapi käigus küsitleti 20 ettevõtte juhti tervishoiusektorist.

Uuringu tulemused – II etapp*

Kas olete viimase aasta jooksul ostnud küberturvalisuse valdkonna teenuseid? Kui jah, siis milliseid?

*II. etapi käigus küsitleti 20 ettevõtte juhti tervishoiusektorist.

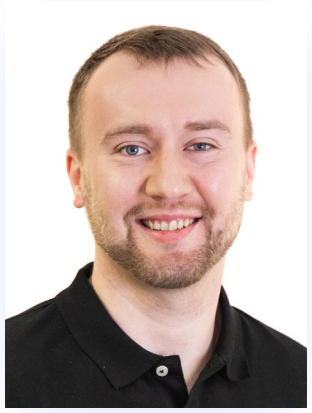
Küsitluse küsimused

Uuringu käigus esitati küsitletavatele ettevõtetele 10 küsimust:

1	Kas teie ettevõttel on sõnastatud IT strateegilised eesmärgid või IT strateegia? Kui jah, siis kas strateegias sisaldub küberturbe meetmestik?
2	Kuidas on teie ettevõttes lahendatud infoturbe tagamine?
3	Kas viimase aasta jooksul on teie ettevõttes esinenud infoturbe intsidente? Kas intsidentide arv on sagenenud?
4	Kas olete viimase aasta jooksul ostnud küberturvalisuse valdkonna teenuseid? Kui jah, siis milliseid?
5	Kas vajate abi küberturvalisuse valdkonna riskide juhtimisel, maandamisel? Nt. kas teie ettevõtel on plaanis lähiajal (2022. aastal) tellida mingeid infoturbe teenuseid? Mis teenuseid?
6	Kas ettevõttes on läbi viidud infoturbe alaseid koolitusi? Milliseid?
7	Kuidas hindate oma ettevõtte infoturbe võimekust?
8	Kas teie ettevõte on kannatanud kunagi ajalist või rahalist kahju seoses küberintsidentidega? Kas muretsete ka täna nende riskide pärast?
9	Kas pandeemia on teie ettevõttes kiirendanud digimuutusi? Sh. kas teie töötajad omavad ettevalmistust infoturbe vallas ja oskavad levinumaid riske maandada?
10	Kas teie ettevõttes on olemas infoturbealane eelarve? Võimalusel täpsustada eelarvet.

KPMG Cyber

Aitäh!



Igmar Ilves

Cyber Security Manager, GPEN, GWAPT, CISA, ITSRM²

Mobile +372 5684 5435
iilves@kpmg.com

KPMG Baltics OÜ
Narva mnt 5
Tallinn 10117, Estonia