MentiSec .

# Turvalisus äriettevõttes: mida teha enne, kui audiitor või klient küsib

*Küberturvalisuse seadus enamikule väikeettevõtetest otse ei kohaldu. Nõuded jõuavad kohale hoopis kliendi lepingu ja küsimustiku kaudu. Alates 1. oktoobrist 2025 on Eestis olemas tasuta ametlik miinimum, mille saab neile vastuseks anda.*

ARTIKKEL 17. august 2026 · 10 min lugemist

Enamiku Eesti väikeettevõtete jaoks ei alga küberturvalisus rünnakust. See algab e-kirjast: suur klient saadab mitmekümne reaga turvaküsimustiku, peatöövõtja lisab lepingusse turvalisa auditiõigusega või hankija kirjutab hanketingimustesse ISO 27001 sertifikaadi nõude. Tähtaeg on nädal.

Küsimus, mis siis tekib, on alati sama: **kas me peame seda tegelikult tegema, või on see lihtsalt kellegi mall?** Vastus on enamasti "ei pea, aga vastata tuleb". Alates 2025. aasta oktoobrist on Eestis olemas ametlik, tasuta ja eestikeelne nimekiri, mille saab vastuseks anda.

## Kust see küsimustik õiguslikult tuleb

Kõige levinum arusaam on, et küsimustik tuleb NIS2 direktiivist ja et see "laieneb tarneahelale". Poolik tõde, mis viib vale järelduseni.

Eesti küberturvalisuse seaduses **ei esine sõna "tarneahel" mitte kordagi.** Ei esine ka sõnu "hankija", "alltöövõtt", "mitmikautentimine" ega "varundamine". Nõue jõuab teieni kahe konkreetse sätte kaudu:

**Küberturvalisuse seaduse § 7 lg 3:** "Kui teenuseosutaja volitab süsteemi haldamise teisele isikule või majutab süsteemi teise isiku juures, vastutab teenuseosutaja selle eest, et teine isik tagab süsteemi turvameetmete rakendamise."

**Vabariigi Valitsuse määruse nr 121 lisa punkt 4.2:** teenuse osutaja peab tarnijate, väliste teenuste osutajate **ja partneritega** kirjalikult taasesitatavas vormis kokku leppima **andmete vahetamiseks vajalikud** turvanõuded ning kasutatava teenuse tingimused.

Ehk: seadus ei kohusta teid. Seadus kohustab **teie klienti** teie eest vastutama ja teiega kirjalikult taasesitatavas vormis kokku leppima. Küsimustik on selle kohustuse täitmise viis. See vahe ei ole juriidiline peenutsemine. Sellest sõltub, kas te vastate nõudele või läbirääkitavale soovile.

### Kas seadus kehtib teile?

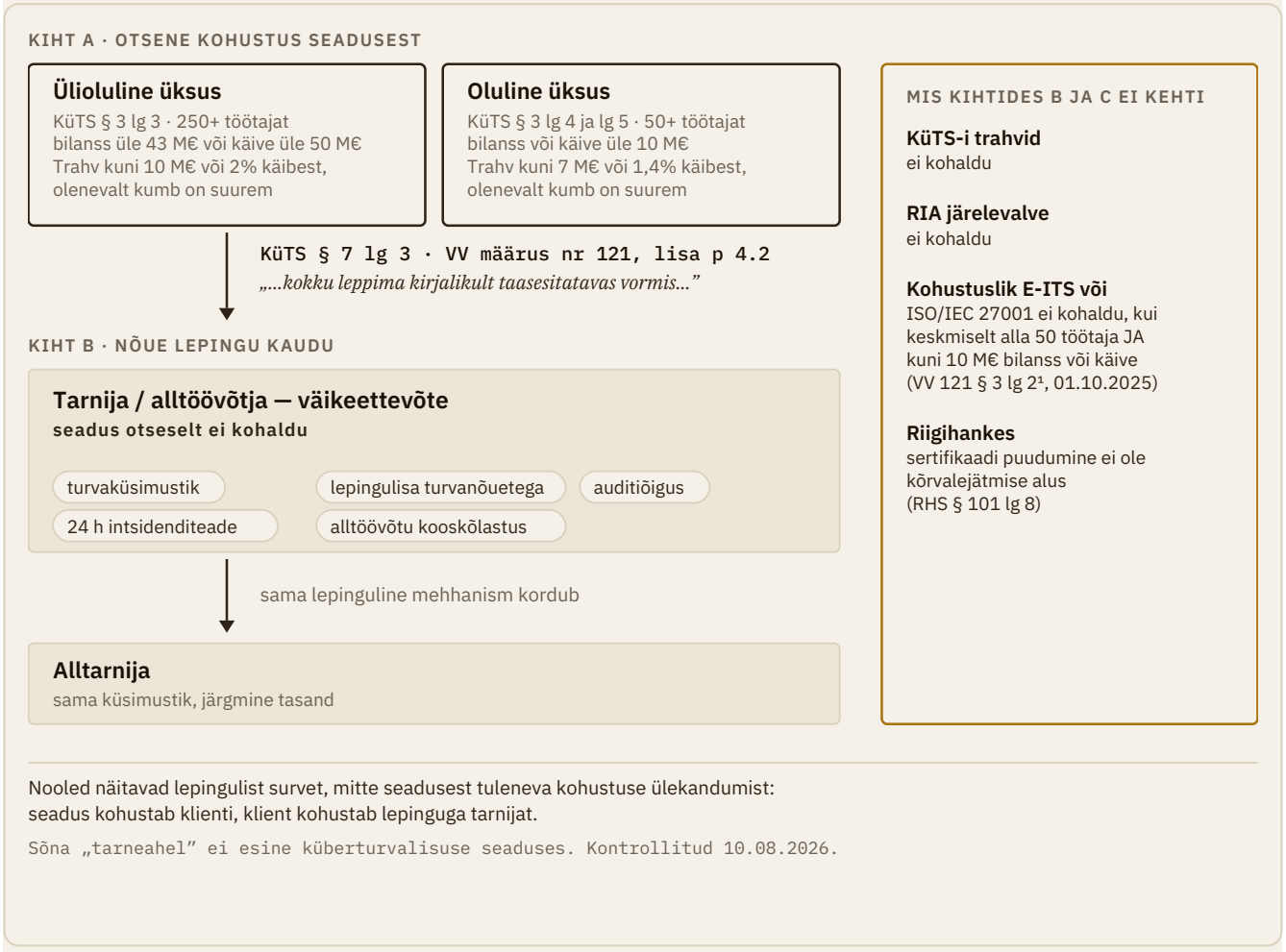
Suure tõenäosusega mitte otse. Küberturvalisuse seaduse NIS2-muudatused jõustusid 1. jaanuaril 2026 ja seaduse subjektide ring kasvas ligikaudu 3500-lt umbes 6500-le. Aga eelnõu seletuskiri ütleb otse: **"Eelnõu kohaldamisalast on välja jäetud mikro- ja väikeettevõtjad"** ning "NIS2-direktiiv võetakse üle minimaalsel võimalikul määral".

Suurusläved on seaduses kirjas:

— **Ülioluline üksus:** üldjuhul 250 või rohkem töötajat ja aastabilansimaht üle 43 miljoni euro või käive üle 50 miljoni euro. Trahvimäär kuni 10 miljonit eurot või 2% eelmise majandusaasta ülemaailmsest kogukäibest, olenevalt sellest, kumb summa on suurem.

— **Oluline üksus:** 50 või rohkem töötajat ja aastabilansimaht või käive üle 10 miljoni euro. Trahvimäär kuni 7 miljonit eurot või 1,4% samast käibest, olenevalt sellest, kumb on suurem.

Mõned tegevusalad on kohaldamisalas suurusest sõltumata: kriitilise tähtsusega sideteenused, kvalifitseeritud usaldusteenused, domeeninimede süsteemi ja tippdomeeni registri teenused, elutähtsa teenuse osutajad ning riigi- ja kohaliku omavalitsuse asutused. Kui te ei ole nende hulgas ja teil on alla 50 töötaja, siis seadus teile otse ei kohaldu.




Kaks eri teed kohustuseni. Ülemises kihis tuleb nõue seadusest, alumistes lepingust. Lepinguline nõue ei kanna endaga kaasa seaduse trahve ega järelevalvet.

Sellel vahel on praktilised tagajärjed, mida tasub teada:

— **Trahvid ei kohaldu teile.** Kui te ei ole seaduse subjekt, ei saa RIA teid trahvida. Alles jääb lepinguline risk, mitte riiklik sanktsioon.

— **Kontserni kuulumine ei tõmba teid automaatselt sisse.** Küberturvalisuse seaduse § 3 lg 7 ütleb, et partner- ja sidusettevõtete andmeid ei arvestata, kui üksus on teenuse osutamiseks kasutatavates süsteemides iseseisev. See on Eesti enda valik ja selle kohta ei ole veel kohtupraktikat.

— **Küberkerksuse määrus (CRA) ei kohaldu SaaS-ile.** Kui müüte teenust pilvest, hinnatakse teid NIS2 loogika, mitte CRA järgi. Väikeettevõtte puhul tähendab see enamasti, et kumbki otse ei kohaldu. CRA puudutab paigaldatavaid tooteid ja seadmeid; selle põhikohustused hakkavad kehtima

11. detsembrist 2027, kuid nõrkustest teavitamise kohustus juba 11. septembrist 2026.

— **DORA ei kohaldu väiksele IT-tarnijale otse.** Otsesed kohustused tekivad ainult kriitiliseks määratud teenusepakkujale. Küll aga jõuab DORA teieni lepingu kaudu, kui teie klient on finantssektoris. Selle artikkel 30 loetleb kohustuslikud lepingutingimused.

### Eesti ametlik miinimum, mille saab lauale panna

Siin on artikli kõige praktilisem osa ja fakt, mida enamik Eesti turvatekstidest ei maini.

**25. septembril 2025 leevendas valitsus nõudeid ligikaudu 1200 Eesti organisatsiooni jaoks.** Alates 1. oktoobrist 2025 ei pea teenuseosutaja, kellel on majandusaasta jooksul **keskmiselt** alla 50 töötaja ja kelle aastane bilansimaht või käive ei ületa 10 miljonit eurot, rakendama täismahus Eesti infoturbestandardit ega ISO/IEC 27001-t. Asemele tuli lühike nimekiri nimega **esmased turvameetmed** — üheksa valdkonda, umbes 50 punkti, eestikeelne, tasuta, otse Vabariigi Valitsuse määruse lisas.

Üheksa valdkonda on:

1. Infoturbe korraldus — vastutav isik, reeglid, IT-varade nimekiri
2. Kasutajate teadlikkus ja kasutajaõigused — sh **mitmeastmeline autentimine**
3. Andmete turve — sh **regulaarne varundus, varukoopiad töösüsteemist eraldi, taaste testitud**
4. **Tarnijate, väliste teenuste osutajate ja partnerite haldus**
5. Küberintsidentide haldus — nimeline koordinaator ja kontakt
6. Pilvteenuste ja veebirakenduste kaitse — sh kasutatavate pilvteenuste nimekiri
7. Infotehnoloogiaseadmete kaitse — 14 punkti, paikamisest kettakrüpteerimiseni
8. Sideühenduste ja võrgu kaitse
9. Füüsiline turve

Kaks asja teevad selle nimekirja väikeettevõtte jaoks eriti kasutatavaks, ja mõlemad on määruse enda tekstis:

> *"Teenuse osutaja võib käesolevas lisas sätestatud meetmete asemel võtta kasutusele mõne muu samaväärse meetme riskide vähendamiseks."*

> *"Teenuse osutaja ei pea käesolevas lisas sätestatud meedet rakendama, kui meede ei ole asjakohane või rakendatav ning kui ta on rakendamata jätmisega kaasnevad riskid teadvustanud."*

Ehk proportsionaalsus on sisse kirjutatud. "Ei kohaldu meile, ja siin on põhjus" on lubatud vastus — kui põhjus on kirjas.

See ei ole Eesti leiutis. Maailma suurima tarkvaraostja Microsofti tarnijaprogramm SSPA nõuab tavatarnijalt **iga-aastast enesedeklaratsiooni**, mitte auditit. Sõltumatut kinnitust küsitakse alles siis, kui tarnija on alltöötleja või pakub SaaS-i, majutust või kasutab ise alltöövõtjaid. Ja Microsoft lubab sõnaselgelt vastata "ei kohaldu" koos põhjendusega. Kui suurim ostja lubab põhjendatud "ei kohaldu", võib seda vastust pakkuda ka väiksema kliendi küsimustikus.

Ja veel üks kokkulangevus, mis teeb sellest hea vastuse just küsimustikule: **valdkond 4 puudutab sedasama teemat, mida NIS2 tarneahela nõue.** See on meie hinnang, mitte määruse sõnastus. Rahvusvaheline küsimustik küsib tarnijate kohta rohkem (auditiõigus, taustakontroll, alltöövõtt, lepingu lõpetamine). Aga punktid 4.1 ja 4.2 annavad vastamiseks lähtekoha.

### Mida küsitakse ja mille saate lauale panna

Rahvusvahelised küsimustikud on suured. Shared Assessmentsi SIG Core katab umbes 800–850 küsimust 21 riskivaldkonnas, pilvteenuste CAIQ 17 valdkonda, ISO/IEC 27001:2022 lisa A umbes 93 turvameedet. Aga teemasid, mis tegelikult korduvad, on kaksteist: infoturbe korraldus, vastavus ja tõendid, ligipääsuhaldus ja mitmeastmeline autentimine, töötajate teadlikkus, varade nimekiri, krüpteerimine, seadmete ja võrgu kaitse ning paikamine, turvaline arendus, logimine ja seire, intsidendihaldus, talitluspidevus ja varundus, ning alltöövõtjad.

Vastamise saladus ei ole hea sõnastus, vaid see, et **iga küsimuse taga on üks konkreetne dokument**, mille saab lihtsalt üle anda.

Üks lisanipp neile, kes müüvad pilve- või tarkvarateenust: CAIQ küsimustiku saab täita üks kord ja avaldada **tasuta** CSA STAR registris (Level 1 enesehinnang). Esitamine käib Exceli failina, kirje ilmub üldjuhul ühe tööpäevaga ja edaspidi saab iga järgmise kliendi küsimustikule vastata lingiga. Tasuline on alles vabatahtlik valideering ja Level 2 audit — esimeseks sammuks pole kumbagi vaja.

| KÜSIMUS, MIS TULEB | | ARTEFAKT, MILLE ANNATE | KLASS | ALUS |
|---|---|---|---|---|
| *„Kas teil on infoturbe eest vastutav isik?”* | → | **Nimeline vastutaja + kirjapandud reeglid** | A | esm. tm 1.1–1.2 |
| *„Milliseid süsteeme ja seadmeid kasutate?”* | → | **IT-varade nimekiri koos omanikega** | B | esm. tm 1.4–1.5 |
| *„Kas kasutate mitmeastmelist autentimist?”* | → | **Ligipääsu- ja MFA-kord + tõend, et MFA on sees** | C | esm. tm 2.5 |
| *„Kas varundate?”* | → | **Varunduskord + taastetesti protokoll** | C | esm. tm 3.6 |
| *„Kes on teie alltarnijad?”* | → | **Oluliste tarnijate nimekiri koos taustaga** | B | esm. tm 4.1 |
| *„Milliseid pilvteenuseid kasutate?”* | → | **Pilvteenuste nimekiri, otstarve ja risk** | B | esm. tm 6.6 |
| *„Kuidas käitute intsidendi korral?”* | → | **Intsidendi kontakt + käsitlusprotsess** | A | esm. tm 5.2–5.3 |
| *„Kuidas te isikuandmeid töötlete?”* | → | **Töötlemisülevaade + andmetöötluslepingud** | B | IKÜM art 30/28 |

A kirjapanek — info on olemas, tuleb kirja panna

B kogumine — info tuleb esmalt kokku koguda

C tõendamine — nõuab tegevust, mille tulemus jääb kirja

Klassid kirjeldavad ülesande laadi, mitte ajakulu.
Kaitstavaid avalikke ajakuluandmeid ei ole.
Kontrollitud 10.08.2026.

Igale korduvale küsimusele vastab üks artefakt. Töömahuklassid kirjeldavad ülesande laadi, mitte ajakulu.

| KÜSIMUS, MIS TULEB | ARTEFAKT, MILLE ANNATE | ALUS |
|---|---|---|
| "Kas teil on infoturbe eest vastutav isik?" | nimeline vastutaja + kirjapandud reeglid | esmased turvameetmed p 1.1–1.2 |
| "Milliseid süsteeme ja seadmeid te kasutate?" | IT-varade nimekiri koos omanikega | p 1.4–1.5 |
| "Kas kasutate mitmeastmelist autentimist?" | ligipääsu- ja MFA-kord | p 2.5 |
| "Kas varundate?" | **varunduskord + taastetesti protokoll** | p 3.6 |
| "Kes on teie alltarnijad?" | oluliste tarnijate nimekiri koos taustaga | p 4.1 |
| "Milliseid pilvteenuseid kasutate?" | pilvteenuste nimekiri koos otstarbe ja riskihinnanguga | p 6.6 |
| "Kuidas käitute intsidendi korral?" | intsidendi kontakt + käsitlusprotsess | p 5.2–5.3 |
| „Kuidas te isikuandmeid töötlete?” | isikuandmete töötlemisülevaade + andmetöötluslepingud | IKÜM art 30, art 28 |

Viimane rida väärib eraldi tähelepanu, sest siin eksitakse kõige sagedamini. Isikuandmete kaitse üldmääruse (IKÜM) artikkel 30 lõige 5 näib vabastavat alla 250 töötajaga ettevõtted töötlemisülevaate koostamisest. Andmekaitse Inspektsioon ütleb otse, et see mulje on väär: kui ettevõttel on vähemalt üks töötaja või vähemalt üks füüsilisest isikust klient, ei ole töötlemine juhuslik ja ülevaade tuleb koostada. **Erinevalt küberturvalisuse seadusest kehtib see teile kindlasti.**

### "Meil ei ole ISO 27001." Kas see lõpetab jutu?

Riigihankes mitte. Riigihangete seaduse § 101 lõige 8 ütleb, et kui pakkujal ei ole temast mitteolenevatel põhjustel võimalik nõutud sertifikaati esitada, **aktsepteerib hankija muud tõendusmaterjali samaväärsete kvaliteedi tagamise meetmete kohta, kui need meetmed vastavad hankija nõutud kvaliteedi tagamise standarditele.**

See ei ole teoreetiline. Tarbijakaitse ja Tehnilise Järelevalve Amet on selle oma 2025. aasta hankekorda sõna-sõnalt sisse kirjutanud: kui pakkujal puudub E-ITS-i auditi järeldusotsus või kehtiv ISO/IEC 27001 sertifikaat, peab amet ise enne kvalifitseerimisotsust veenduma, et nõutud infoturbemeetmed on rakendatud.

Erakliendi puhul on see läbiräägitav. Mõistlik vastus ei ole sertifikaadi kiirkorras ostmine, vaid rakendatud meetmete näitamine. Eestis on selleks olemas riigi enda kehtestatud nimekiri.

Sertifikaadi kohta veel üks aus tähelepanek: **Eesti Akrediteerimiskeskus ei ole akrediteerinud ühtegi ISO 27001 sertifitseerijat.** Sertifikaat tuleb osta välismaise akrediteerimisasutuse alt ja avalikku Eesti hinnastatistikat selle kohta ei ole. Kui keegi lubab teile numbri, küsige allikat. Meie ei paku siin numbrit, sest kaitstavat allikat ei ole.

### Kui klient on Rootsist, Soomest, Norrast või Ühendkuningriigist

Eesti väikeettevõtte välisklient on enamasti põhjamaine või briti. Sealgi on pilt sama, mitte karmim.

Nõue aktsepteerida samaväärset tõendust ei ole Eesti eripära: RHS § 101 lg 8 võtab üle ELi hankedirektiivi sätte, mis kehtib ka Rootsi, Soome ja Taani hankijale. Rootsi riigihankeamet läheb kaugemale ja tunnistab ise, et ISO 27001 nõudmine kvalifitseerimistingimusena on õiguslikult ebaselge, sest kohus ei ole seda hinnanud. Nõue peab olema "otstarbekas ja proportsionaalne".

Briti küberkeskus NCSC soovitab oma tarneahela juhendis (detsember 2025) ostjatel esitada eri suurusega tarnijatele **eri nõuded**, et need oleksid "realistlikud, pragmaatilised ja riskiga proportsionaalsed". Ja välisriigi tarnija kohta ütleb sama juhend otse: ostja peaks küsima **meetmete olemasolu, mitte Briti sertifikaati**. See lause tasub meelde jätta, kui UK klient nõuab Eesti ettevõttelt Cyber Essentialsi. Taani usaldusmärgist D-mærket ei saa Eesti ettevõte üldse taotleda. Vastus on sealgi meetmed, mitte märgis.

Et surve on päris, näitab Briti valitsuse enda 2025/2026 küberuuring: tarnijate riske kontrollib ligi pool suurettevõtetest (48%), aga vaid 12% mikroettevõtetest. Küsimustik tuleb seega praktiliselt alati suurelt kliendilt. Sama uuring tsiteerib väikeettevõtjat, kes uurib sertifikaati "puhtalt sellepärast, et kliendid küsivad". Just sellepärast tasub vastus ette valmistada üks kord, mitte iga kliendi jaoks uuesti.

### Mis on tõesti kasulik ja mis on paberitöö

Küsimustik mõõdab olemasolu. Rünnak mõõdab sügavust. Nende kahe vahe ongi koht, kus väikeettevõte saab tegelikult võita:

| PABERIL | PRAKTIKAS |
|---|---|
| "Meil on varunduspoliitika" | taaste on testitud ja testil on kuupäev |
| "Kasutame MFA-d" | MFA on õngitsuskindel, mitte SMS |
| "Meil on intsidendiplaan" | plaan on läbi mängitud ja kontaktid kehtivad |
| "Paikame regulaarselt" | paikamise kiirus on mõõdetud päevades |
| "EDR on olemas" | see katab kõiki seadmeid ja keegi vaatab teateid |

Marsh McLennani kübersiskide analüüs (august 2025) näitab, et vahe on mõõdetav: õngitsuskindel mitmeastmeline autentimine seostub ligikaudu 9% madalama turvarikkumise tõenäosusega **võrreldes õngitsuskindluseta mitmeastmelise autentimisega**, ja regulaarsete läbimängude tegemine ligikaudu 13% madalama tõsise intsidendi tõenäosusega. Iseloomulik on ka see, et MFA on sama analüüsi kindlustusandjate soovituste tabelis langenud 2023. aasta esikolmikust 2025. aastaks kuuendaks. Mitte sellepärast, et see enam ei loeks, vaid sellepärast, et see on kõigil olemas ega erista enam kedagi. Hindamine on liikunud olemasolult tõendile. Meie ootus on, et sama nihe jõuab ka kliendi küsimustikku.

Ja kuna hirmuturundus on selles valdkonnas norm, siis üks number vastukaaluks. RIA küberturvalisuse aastaraamat 2026 loendas 2025. aastal 756 teenusetõkestusrünnakut — rekord, üle kolmandiku rohkem kui aasta varem. Aga mõju rünnatava teenusele oli **vähem kui sajal** neist. Varem õnnestus ligi iga viies. Baaskaitse töötab; see on mõõdetud, mitte lubatud.

### Kust alustada, kui küsimustikku veel ei ole

Kolm sammu, mis on kasulikud sõltumata sellest, kes ja millal küsib:

1. **Tehke esmased turvameetmed läbi kui kontrollnimekiri.** Üheksa valdkonda, mille saab ükshaaval läbi käia. Kirjutage iga punkti juurde kas "tehtud", "samaväärne meede: …" või "ei kohaldu, sest …". See kolmas variant on määruses lubatud — aga ainult kirjapanduna.
2. **Pange kokku üleandmiskaust.** Ülaltoodud tabeli kaheksa artefakti. Osa neist on teil sisuliselt olemas, lihtsalt kirja panemata; osa tuleb esmalt kokku koguda.
3. **Testige üks taaste ära ja pange kuupäev kirja.** See on nimekirja kõige raskemini paberil võltsitav punkt. Seetõttu jääb see tõsiseltvõetavale küsijale kohe silma.

## Kokkuvõte

Küberturvalisuse seadus enamikule Eesti väikeettevõtetest otse ei kohaldu ja seda ei tasu lasta endale müüa. Küll aga jõuab nõue kohale lepingu kaudu, sest teie klient vastutab seaduse ees ka teie süsteemide eest. Selle vastu ei aita sertifikaat, mida te ei vaja, vaid kaust, mille saab üle anda.

Kui teie ees on praegu küsimustik ja te ei tea, mis sellest teile kohaldub, saatke meile sõnum.

---

Originaal veebis: `https://mentisec.ee/analyysid/turvalisus-ariettevottes/`