KPMG uuring: Eesti ettevõtete juhid peavad infoturvet ja küberturvalisust oluliseks

2 aastat tagasi Autor: AM

2022. aasta esimeses kvartalis viis KPMG Baltics koostöös Äripäevaga läbi sõltumatu infoturbe ja küberturvalisuse uuringu Eesti juhtivate ettevõtete seas. Uuringu peamine eesmärk oli teada saada, kuidas ettevõtted suhtuvad infoturbe ja küberturvalisuse tagamisse ning mismoodi on ettevõtted infoturvet ja küberturvalisust üles ehitanud. Uuringu ajendiks on kaasaja poliitilise, tervishoiualase ning majandusliku olukorra ebastabiilsus maailmas, mis on vaieldamatult mõjutanud ka infotehnoloogia ning kitsamalt ka küberturvalisuse valdkonda.

Uuringu abil soovime juhtida tähelepanu infoturbe valdkonna olulisusele ning spetsiifilistele kitsaskohtadele, mille abil saavad paljud ettevõtted teadvustada võimalikke ohte ja valmistada end paremini ette ohtudele reageerimiseks.

Uuring teostati kahes etapis – 1. etapis küsitleti ettevõtete juhte 300 suurima Eesti tööandja hulgast. Uuringu 2. etapp keskendus eraldiseisvalt tervishoiusektorile, mille raames küsitleti tervishoiuasutuste ja -organisatsioonide juhte. Tervishoiusektorit käsitleti uuringus eraldiseisvalt seetõttu, et sektoris on kehtestatud kõrgemad nõuded andmete kaitsele delikaatsete isikuandmete töötlemise tõttu.

Uuringu tulemused kinnitavad, et valdav osa Eesti ettevõtete juhte peavad infoturvet ja küberturvalisust oluliseks ning ettevõtete juhid on seisukohal, et küberintsidentide realiseerumise oht on täna pigem tõenäoline. Täiendavalt näitavad andmed, et suurt osa ettevõtteid on küberintsidendid ka vahetult mõjutanud.

Ettevõtete juhid kinnitavad, et viimase aasta jooksul on sagenenud infoturbe intsidentide arvukus arvestatavas mahus. Samas on vaid alla poole vastanutest hinnanud enda võimekust infoturbe ja küberturvalisuse tagamisel piisavaks.

Antud fakte iseloomustab uuringu statistika küsitletud 300 suurima Eesti tööandja hulgas: 90% vastanutest tunneb muret võimalike intsidentide pärast, mis võivad juhtuda tulevikus, 54% vastanutest on kannatanud küberintsidentide tõttu ajalist kahju ning 41% vastanutest on kannatanud küberintsidentide tõttu rahalist kahju.

Tervishoiu ettevõtete ning organisatsioonide puhul on aga statistika selgelt erinev: võimalike intsidentide pärast tunneb muret 85% küsitletud tervishoiu ettevõtetest, aga kõigest 10% vastanutest on kannatanud küberintsidentide tõttu ajalist kahju ning ükski Eesti tervishoiu ettevõte pole kannatanud küberintsidentide tõttu rahalist kahju. Tervishoiu ettevõtete statistikaerinevus võib omada tõenäoliselt kolme võimalikku põhjust:

1. võimalikud kurjategijad ei tunne eetilistel põhjustel huvi tervishoiu ettevõtete ründamise vastu;
2. tervishoiu ettevõtete kaitsemeetmed on tõhusamad, kui teiste ettevõtete omad;
3. tegelikult on rünnakud juba toimunud, kuid tervishoiu ettevõtted pole neid lihtsalt suutnud tuvastada.

Märgiline on asjaolu, et enam kui pooled kõikidest vastanutest nentisid, et nende ettevõttes vastutab infoturbe eest teenuspartner. See võib

tõesti nii olla, kuid ei saa mainimata jätta, et KPMG kogemuse kohaselt arvatakse sageli ekslikult, et IT-teenuseid tagavale teenuspartnerile peaks automaatselt kohalduma ka ettevõtte küberturvalisuse tagamise kohustus. See tähendab praktikas seda, et ostes sisse IT-süsteemide haldamise teenust, eeldab ettevõtte juhtkond, et sellega kaasneb ka IT-süsteemide turvalisuse tagamine (nt seadmete ja rakenduste turvaline konfigureerimine, vaikeparoolide muutmine, perioodiline paroolide muutmine, võrkude turvaline segmenteerimine, seadmete ja rakenduste järjepidev turvapaikade paigaldamine, kahjurpääsupunktide (ingl k *Rogue Access Point*) avastamine, turvanõrkuste skaneerimine jpm) ning seega kanduks justkui vastutus infoturbe tagamisel ettevõttelt teenuspartnerile. Praktikas teeb IT-teenuste partner vaid neid tegevusi, mis on ette nähtud lepingus – reeglina haldamise teenuste osutamise puhul puudub vastavas lepingus turvalisuse tagamise kohustus. Tihti avastavad ettevõtted alles küberintsidendi toimumise hetkel, et tegelikult ei vasta nende poolt sisse ostetud teenus turvalisuse seiskohast nende ootustele. Lisaks on oluline ettevõtete juhtidel mõista, et lõplik vastutus infosüsteemide turvalisuse üle jääb alatiseks nende kanda, isegi, kui IT-teenuspartneriga sõlmitud lepingus on kõikvõimalikud turvalisuse kohustused sätestatud.

Täiendavalt näitavad uuringu tulemused, et sõltumatu osapoole poolt teostatavaid infoturbe kontrolle teostatakse Eesti ettevõtete seas pigem vähe (nt läbistustestimine või IT-turvaaudit). Kahetsusväärne on see, et eriti vähe teostatakse selliseid kontrolle tervishoiu ettevõtete seas, kus kõrgemate nõuete kehtivuse tõttu võiks eeldada, et kontrolle tehakse pigem rohkem. Võimalik, et sõltumatute kontrollide puudumise tõttu jäävad paljud küberintsidendid avastamata ning ettevõtte juhtkond jääb ekslikult arvamusele, et neil ei olegi selliseid intsidente toimunud (kui tegelikkuses võivad küberkurjategijad omada ligipääsu ettevõtete infosüsteemidele ning tegeleda juba käesoleval hetkel isikuandmeid või ärisaladust puudutavate elektrooniliste dokumentide müümisega nn „mustal turul“).

Tänapäeval on infoturve ning küberturvalisus olulisemad kui kunagi varem. KPMG soovitab tegeleda küberturvalisusega proaktiivselt ja kvaliteetselt, kaardistada hetkeolukord (ideaalselt koostöös sõltumatu osapoolega) ning olla valmis halvimateks stsenaariumiteks (nt kogu organisatsiooni IT-infrastruktuuri hõlmav lunavara rünnak, mis võib halvata kogu ettevõtte äritegevuse). Teostatud uuring näitab, et ettevõtete küberturvalisuse olukord on kaugel ideaalsest ning eelkõige tuleks saada lahti mõtteviisist, et „meie vastu ei tunne küberkurjategijad huvi, mistõttu on rünnak ebatõenäoline“ ning pöörata tähelepanu olukorra parandamisele juba täna, sest homme võib olla juba hilja.

KPMG Baltics OÜ ning Äripäeva poolt läbiviidud sõltumatu uuringuga saab lähemalt tutvuda lisatud raportis:

- Uudised
- Turvalisus