

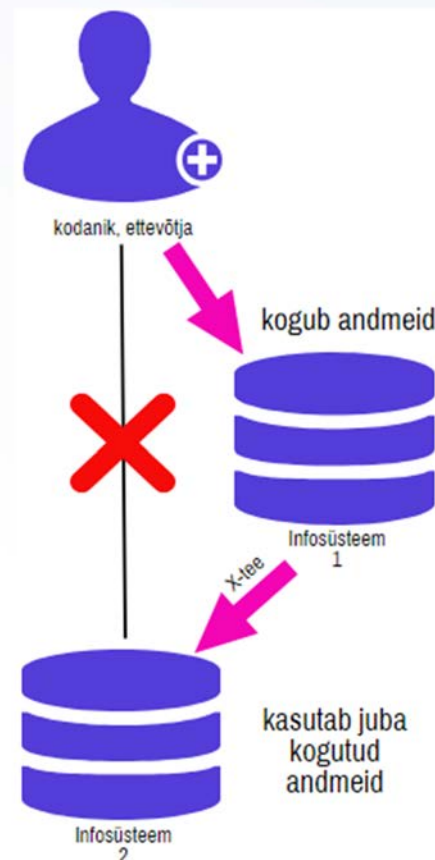
IT-turvameetmete süsteemi rakendamine kohalikes omavalitsustes

Meeli Saksing, audiitor-projektijuht

Riigikogu riigieelarve kontrolli erikomisjon
6. juuni 2018

Teema olulisus ja auditi eesmärk

- Omavalitsuste ja riigi andmekogud vahetavad üksteisega X-tee kaudu andmeid, mis tähendab, et omavalitsustes tähelepanuta jäetud nõrkused kanduvad edasi ja võivad teha kahju laiemalt.
 - Seetõttu on andmete turvalisus eriti oluline.
- Auditi eesmärk oli hinnata KOVide tegevust infoturbemeetmete rakendamisel ning riigi tegevust KOVide infoturbe olukorra parendamisel.



Põhiküsimus ja kriteeriumid

Kas omavalitsuste kätte usaldatud andmete turvalisus on nõuetele kohaselt tagatud?

- Omavalitsus on planeerinud infoturbetegevusi ja loonud dokumentatsiooni selle kohta, kuidas tagatakse X-tee kaudu andmetevahetuse turvalisus.
- Omavalitsus rakendab turvameetmeid X-tee kaudu toimuva andmevahetuse turvalisuse tagamiseks.
- Andmete turvalise vahetamise üle tehakse järelevalvet.

Peamised järeldused

Auditeeritud omavalitsuste kätte usaldatud andmete turvalisus ei ole nõuetekohaselt tagatud.

- IT-turve on paljude omavalitsuste jaoks küsimus, millega seotud riske endiselt ei teadvustata, mistõttu ei täideta valdavalt ka riigi seatud nõudeid, ehkki need on praeguseks kehtinud pea 10 aastat.
- Riigi järelevalve on vähene ega sunni omavalitsusi pingutama.
- Loodetud arengut ei ole kaasa toonud ka riigi teavitustegevus ega rahaline toetus.

Tähelepanekud: omavalitsuste tegevus andmete turvalisuse tagamisel

Omavalitsused ei teadvusta andmete töötlemisel oma vastutuse ulatust ega kaasnevaid nõudeid

- Ei ole seatud andmeturbe eesmäärke:
 - Turbevajadus on välja selgitamata ja kinnitamata.
Ühetaoliste andmekogude turvaklassi määramine on dubleeriv tegevus.
 - Nn karbitoote turbevõimekus on tegelikust vajadusest madalam ja lisameetmeid omavalitsused ei rakenda.
 - Levinud on väärarusaam, et andmete turvalisuse eest vastutab karbitoote pakkuja, kelle juures andmeid hoitakse.
- Ei ole võetud vastutust andmekogude
 - riigi infosüsteemi halduse infosüsteemi RIHA registreerimise,
 - andmevahetuskihiga X-tee liidestamise ega
 - turvameetmete süsteemi ISKE rakendamise eest.

Tähelepanekud: omavalitsuste tegevus andmete turvalisuse tagamisel

Infoturbe planeerimise seis omavalitsustes on kehv

- Infovarade inventuurid ei ole ajakohased.
- Andmekogude loetelu koostamisega saadakse hakkama.
- Turvaklasside (K..., T..., S...) ja turvaastmete (L, M, H) määramine on osutunud suureks probleemiks.
- Puudub rakendamisele kuuluvate tüüpmodulite ja nendest valitud turvameetmete loetelu.
- MKM ei ole tellinud ISKE-auditeid.
- Puudub kindlus, et ISKE rakendamise metoodika väljatöötamisel on nn karbitoodete eripära arvestatud.

Tähelepanekud: omavalitsuste tegevus andmete turvalisuse tagamisel

Infoturbe rakendamise seis omavalitsustes on kehv

- IT-kasutajatele on antud kergekäeliselt piiranguteta õigusi.
- Tihti puudub ka ülevaade, kes ja kuhu üldse ligi pääseb.
- Paroolihaldus on puudulik (määramata parooli miinimumpikkus, aegumistähtaeg, kasutajate paroolid salastamata).
- Asutusesiseseks kasutamiseks tunnistatud e-kirjad ja kõvakettad ei ole krüpteeritud.
- Turvapaikade paigaldamine oli jäetud paljuski kasutajate meelevalda.
- Ei ole teada, kuidas ja kus andmeid ja nende varukoopiaid hoitakse.
- Mittesoovitud tarkvara ei ole töökohaarvutites kontrollitud.
 - Selle paigaldamist ei takistata; keskhaldust ei ole sisse seatud.

Tähelepanekud: omavalitsuste tegevus andmete turvalisuse tagamisel

Omavalitsuste infoturbekultuur on madal nii teenistujate kui ka juhtkonna tasandil

- Infoturbepoliitikast päriselus ei lähtuta ning selle rakendamine on eelarveraha jagamisel teisejärguline.
- Juhtkonna huvi infoturbe meetmete rakendamise vastu on vähene.
 - Üheski KOVis ei ole juhtkonda seadusest tulenevate infoturbenõuetega kurssi viidud; majasiseseid koolitusi ei tehta, RIA koolitustel ei osaleta.
 - Vähene on arusaam turbetegevuse olulisusest ja vajalikkusest.
- IT-turbe eest vastutajad on puudu, nende asendajaid ei ole määratud või asendaja on määratud, kuid isikul puudub väljaõpe.
 - Peamiselt suudetakse pakkuda IT tehnilist tuge, aga spetsialiseerumist (sh infoturbele) on vähe.
- IT-kasutajatele ei ole kehtestatud suuniseid olulisemate turbeaspektidega ümberkäimiseks või on need kehtestatud, aga neid pole tutvustatud.

Tähelepanekud: riigi tegevus andmete turvalisuse tagamisel

Omavalitsuste ja riigi andmekogude vahel on andmete vahetust vähe

- RIHAs registreeritud andmekogud ei läbi alati kooskõlastusprotsessi.
- Avalikule sektorile teenust pakkuvale tarkvaraarendajale ei laiene RIHAs registreerimise (sh kooskõlastuse) kohustus.
- Andmekogud ei ole X-teega liidestatud või X-teega liidestus ei ole tehniliselt võimalik.

X-teel andmeteenuse osutajad ei esita konkreetseid turbenõudeid ega kontrolli oma andmete kasutajaid

- Andmeteenuse osutajatele ei ole selge, miks peab läbi viima kontrolli andmeteenuse kasutaja üle, kui viimane täidab ISKE nõudeid.
- ISKE-auditi tulemustele ei saa alati tugineda – KOVides ei ole MKM neid tellinud; erasektoris puudub kohustus ISKEt rakendada; saab tugineda ainult kattuvate turvameetmete puhul.
- Pole selge, mis tingimustel võib andmeteenuse osutaja keelduda X-tee vahendusel andmete edastamisest.

Tähelepanekud: riigi tegevus andmete turvalisuse tagamisel

Seni on riiklikku järelevalvet turvameetmete süsteemi rakendamise üle omavalitsustes tehtud vähe

- 7-aastase perioodi jooksul on omavalitsusi kontrollitud 72 korral.
- Mitte ühtegi ettekirjutust ei ole tehtud, kuigi kontrollkäikudel on tuvastatud rikkumisi, sh
 - andmekogude RIHAs registreerimata jätmine,
 - andmete topelt kogumine elanikelt ja ettevõtjatelt,
 - andmete vahetamiseks selleks ettenähtud X-tee mittekasutamine,
 - turvameetmete süsteemi kehv rakendamine.

Teavitustegevus ei ole toonud loodetud tulemusi

- Koolitused on olnud omavalitsustele kättesaadavad, aga
 - juhtkonna osalus on olnud vähene.

Tähelepanekud: riigi tegevus andmete turvalisuse tagamisel

Infoturbe valdkonna toetamise tegelik mõju omavalitsustes ei ole teada

- Eesmärk: omavalitsused oskavad hankida turvanõuetele vastavaid seadmeid ja lahendusi ise.
- Euroopa Liidu toetusraha kasutamise tulemuslikkust infoturbetaseme olukorra parandamisel ei ole hinnatud.
- ISKE rakendamine ei saa sõltuda Euroopa Liidu toetusraha olemasolust.
 - Omavalitsused ei uuenda järjepidevalt oma IKT-töövahendeid, vaid planeerivad suuremad investeeringud, kui saavad välisrahastuse.
- Eraldiseisvaid üksikuid arendusi ja seadmete ostu ei tohiks toetada, kui riik on juba välja arendanud nõuetele vastava taristu (nt riigipilv) ja ühislahendused.

Riigikontroll soovitused omavalitsustele

- Määrata infoturbe juhi ülesannete täitja või tellida infoturbe juhtimine teenusena sisse.
- Seada andmekogude pidamiseks kasutatavatele standardsetele tarkvaralahendustele nõuded sisestatavate andmete turbevajadusest lähtudes.
- Veenduda, et lahendus oleks vajaduse korral liidestatav X-teega.
- Leppida lepingus teenuse osutajaga kokku turvameetmete auditeerimise korraldus.

Riigikontroll soovitused ettevõtlus- ja infotehnoloogiaministrile

- Mõelda läbi omavalitsustele omasest andmekogude pidamise praktikast lähtudes nii RIHA, X-tee kui ka turvameetmete süsteemi õigusnõuete täitmise suunised.
- Analüüsida põhjuseid, miks turvameetmete süsteemi rakendamine omavalitsustes on pikalt viibinud, ning sellest tulenevalt töötada välja tegevused, kuidas muuta ISKE rakendamine omavalitsustes paindlikumaks.
- Muuta ISKE-auditi tellimise korda nii, et neid hakataks järjepidevalt tellima.
- Võtta arvesse infoturbe toetamiseks mõeldud meetmete puhul, et need peaks motiveerima omavalitsusi kasutusele võtma lahendusi, mille riik või mõni teine omavalitsus on juba maksumaksja raha eest loonud.

Riigikontroll soovitus Riigi Infosüsteemi Ametile ja Andmekaitse Inspektsioonile

- Tõhustada omavalitsustes kontrolli
 - ISKE rakendamise,
 - X-teega liitumise,
 - RIHAs registreerimise üle.

Riigikontrolli soovitus Riigi Infosüsteemi Ametile

- Propageerida IT-spetsialistidele mõeldud koolituste kõrval rohkem omavalitsuste juhtkonnale suunatud koolitusi ja teha laiemat teavitustööd.

Tänan tähelepanu eest!