Andmekogude juurdepääsuhaldus

Kas andmekogude juurdepääsuhaldus tagab, et andmetele pääsevad juurde ainult volitatud isikud?

Riigikontrolli aruanne Riigikogule
Tallinn, 1. veebruar 2023

Andmekogude juurdepääsuhaldus

Kas andmekogude juurdepääsuhaldus tagab, et andmetele pääsevad juurde ainult volitatud isikud?

Kokkuvõte auditeerimise tulemustest

Auditeeritud andmekogud:

- sotsiaalkaitse infosüsteem (SKAIS),
- sotsiaalteenuste ja -toetuste andmeregister (STAR),
- karistusregister,
- e-toimiku väärteomenetluse liides ja
- automaatse biomeetrilise isikutuvastuse süsteemi andmekogu.

Riigikontrolli audit näitas, et ehkki juurdepääsuhaldus tagab, et auditeeritud andmekogudes pääsevad andmetele juurde vaid volitatud isikud, on kahe andmekogu puhul neil isikutel liiga laiad juurdepääsuõigused. Senisest enam tuleb asutustes tegeleda logiandmete analüüsimise ja andmepäringute põhjendatuse kontrolliga, et ära hoida intsidente või vähendada juba toimunud intsidentide mõju.

Auditi peamised tähelepanekud

Riigi andmekogudele kohustuslik infoturbe rakendamise audit oli läbi viidud viiest auditeeritud andmekogust neljas. Neis auditites ei olnud juurdepääsuhalduse mooduli turvameetmeid üle kontrollitud, kuna selleks ei kohustanud audiitoreid kolmeastmelise etalonturbe süsteemi ISKE auditeerimise juhend. Juurdepääsuõiguste auditeerimine tuleks tundlike andmete korral edaspidi kohustuslikuks muuta, kuna see aitaks maandada andmete turvalisusega seonduvaid riske.

Andmekogudes SKAIS1 ja STAR on kasutajate juurdepääs liiga ulatuslik. Näiteks on STARis omavalitsuse ametnikul võimalik pääseda juurde teiste omavalitsuste elanikega seotud menetlustele ja neis sisalduvatele andmetele. Kuivõrd STARis ei ole rakendatud logide analüüsimise ja päringute põhjendatuse kontrolliks vajalikke meetmeid, suureneb andmete väärkasutamise risk.

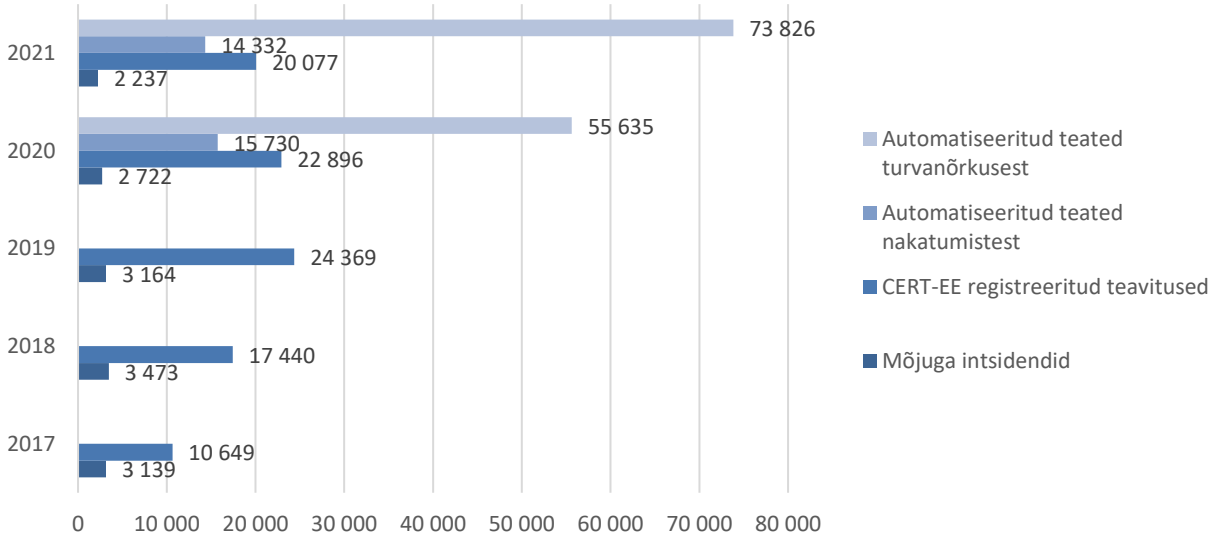
Auditeeritud andmekogudes koguti ja säilitati küll logiandmeid ehk infot andmekogus toimunud sündmuste kohta, ent neid logisid ei analüüsitud süsteemselt ega regulaarselt ning sellekohast kohustust ei olnud kehtestatud ka asutuste või andmekogude tegevust reguleerivates dokumentides. Logiandmeid on vaja analüüsida, et jooksvalt või tagantjärele avastada andmekogudes esinevad rikked või toime pandud intsidendid ning välja selgitada nende tekkimise põhjused.

Auditeeritud andmekogudes ei viidud läbi andmepäringute põhjendatuse regulaarset ega süstemaatilist seiret või kontrolli. Seesuguste kontrollimiste tegemine oli täpsemalt reguleerimata ka asutuste või andmekogude tegevust reguleerivates dokumentides. Kontrolle tehti pigem ebaregulaarselt ning vaid avastatud intsidentide, andmesubjektide päringute/kaebuste või muude väliste sündmuste järel.

Riigi Infosüsteemi Ameti intsidentide käsitlemise osakond registreeris 2021. aastal Eestis *ca* 73 800 automatiseeritud teadet turvanõrkuste kohta ja *ca* 2200 mõjuga intsidenti (vt joonis 1). Enamik neist intsidentidest rajanes juurdepääsu ülevõtmisel või oli suunatud juurdepääsuõiguste ärakasutamisele, et üle võtta võõraid kasutajakontosid ja seeläbi ohustada andmete õigsust või lekitada andmeid.

Riigi andmekogud, mis sisaldavad suurel hulgal isikuandmeid, võivad samuti sattuda küberrünnakute sihtmärgiks.

Joonis 1. Intsidendid ja teavitused aastatel 2017–2021



Allikas: Riigi Infosüsteemi Amet

Auditi peamised soovitused

Riigikontrolli soovitused justiitsministrile, Politsei- ja Piirivalveameti peadirektorile, Sotsiaalkindlustusameti peadirektorile, Tervise ja Heaolu Infosüsteemide Keskuse direktorile, Registrite ja Infosüsteemide Keskuse direktorile ning Siseministeeriumi infotehnoloogia- ja arenduskeskuse peadirektorile:

- Täiendada valitsemisalade või asutuste infoturbe kordasid nii, et reguleeritud oleks ka päringute põhjendatuse kontroll.
- Täiendada valitsemisalade või asutuste infoturbe kordasid nii, et reguleeritud oleks ka logide jooksva analüüsimise kohustus, samuti võtta kasutusele turvateabe ja sündmuste analüüsimise vahend SIEM.

Justiitsministeeriumi kantsler, Politsei- ja Piirivalveameti peadirektor, Sotsiaalkindlustusameti peadirektor, Tervise ja Heaolu Infosüsteemide Keskuse direktor, Registrite ja Infosüsteemide Keskuse direktor ning Siseministeeriumi infotehnoloogia- ja arenduskeskuse peadirektor nõustuvad Riigikontrolli soovitustega ja asuvad neid käesoleval aastal ellu viima.

Riigikontrolli soovitus ettevõtlus- ja infotehnoloogiaministrile:

- Muuta infoturberaamistiku (ISKE ja hiljem E-ITS) rakendamise auditeerimise reegleid ja juhendeid nii, et vähemalt keskmise tervikluse ja konfidentsiaalsuse turvaklassi korral auditeeritakse ka juurdepääsuõigusi.

Ettevõtlus- ja tehnoloogiaminister vastas, et 16.12.2022 kehtestatud E-ITSil põhineva auditi tegemise juhendi kohaselt kontrollib audiitor, kuidas organisatsioon on talle kohaldatud põhimeetmeid rakendanud. Kui neid meetmeid on mingil põhjusel osaliselt rakendatud, siis ka seda

aspekti kontrollitakse. E-ITSis on olemas ligipääsuhaldusega seonduvad meetmed nagu kasutajakontode halduse eeskiri, õiguste andmine, muutmine ja tühistamine ning kasutajate õiguste dokumenteerimine.

Riigikontrolli soovitus Sotsiaalkindlustusameti peadirektorile ning Tervise ja Heaolu Infosüsteemide Keskuse direktorile:

- Tagada, et STARi andmekogu kasutajad kohalikes omavalitsustes saaksid juurdepääsu vaid samas omavalitsuses elukoha aadressi registreerinud inimeste ja nendega seotud menetluste andmetele. Kui aga vajatakse juurdepääsu teiste omavalitsuste elanikega seotud menetlustele, siis määrata kindlaks täiendava juurdepääsu valideerimise kontrolliprotseduur.

Sotsiaalkindlustusameti peadirektor vastas, et ameti seisukohalt ei ole tegemist liiasusega, kuna nimetatud laiem lähenemise vajadus on seotud kohalike omavalitsuste töö spetsiifikaga.

Riigikontrolli kommentaar: Kui SKA hinnangul ei ole võimalik korraldada juurdepääsutaotluse menetlust piisavalt kiiresti ja selliselt, nagu abivajaduse hindamise protsess seda nõuab, siis tuleb andmete väärkasutuse ärahoidmiseks ja avastamiseks seda enam rakendada muid meetmeid (vt punktid 64 ja 86).

Sisukord

Andmekogude juurdepääsuhalduse korraldus

1. Juurdepääsuhaldus kui üks olulisemaid infoturbe valdkondi andmekogude pidamisel peab tagama, et informatsioonile ja IT-ressurssidele pääsevad juurde ainult selleks volitatud kasutajad, lähtudes nende tööülesannetest ja teadmisvajadusest. Turvaline juurdepääsuhaldus võimaldab verifitseerida kasutajad ja väljastada juurdepääsuõigused ainult sellises ulatuses, mis on kasutajate tööks vajalik.

2. Andmekogude juurdepääsuhalduse määratlus käesoleva aruande kontekstis hõlmab riigiasutuste identiteedi- ja õiguste halduse seda osa, mis annab organisatsiooniliste ja infotehniliste vahendite abil kasutajatele juurdepääsu andmekogude andmetele (sh isikuandmetele). Organisatsiooniliselt tähendab see asutustesisest ja -vahelist töökorraldust, mis tagab turvalise ja selgelt määratud andmete kasutuse kõigile osapooltele regulatsioonides sätestatud mahus.

3. Andmekogude kasutamisel peab olema üheselt selge, kes, milleks, millal ja millises ulatuses tohivad isikuandmeid töödelda. Kõik osapooled peavad kaitsma neile usaldatud isikuandmeid. Neile küsimustele vastamiseks on Riigikontroll käesolevas auditis kriteeriumidena kasutanud kolmeastmelise etalonturbe süsteemi (ISKE) põhimõtteid.

4. Auditis vaadati järgmisi andmekogusid, mille konfidentsiaalsus-nõuded ISKE järgi on keskmised või kõrged (turvaosaklass S2 või S3):

- sotsiaalkaitse infosüsteem (SKAIS) – vastutav töötleja Sotsiaalkindlustusamet (SKA), volitatud töötleja Tervise ja Heaolu Infosüsteemide Keskus (TEHIK) ning Maksu- ja Tolliamet;
- sotsiaalteenuste ja -toetuste andmeregister (STAR) – vastutav töötleja Sotsiaalkindlustusamet, volitatud töötleja TEHIK, kohaliku omavalitsuse üksus ning sotsiaalteenuse osutaja;
- karistusregister (KARR) – vastutav töötleja Justiitsministeerium ja volitatud töötleja Registrite ja Infosüsteemide Keskus (RIK);
- e-toimiku väärteomenetluse liides (VMP) – vastutav töötleja Justiitsministeerium, volitatud töötlejad on kohtud, prokuratuur, politseiasutused, uurimisasutused, kohtuvälised menetlejad, julgeolekuasutused, kohtutäiturid, maksukohustuslaste registri volitatud töötlejad, vanglad, arestimajad ja kriminaalhooldajad. E-toimiku väärteomenetluse liidest arendab, haldab ja majutab Siseministeeriumi infotehnoloogia- ja arenduskeskus.
- automaatse biomeetrilise isikutuvastuse süsteemi andmekogu (ABIS)[1] – vastutavad töötlejad on Politsei- ja Piirivalveamet, Välisministeerium, Eesti Kohtuekspertiisi Instituut ning volitatud töötlejad on Kaitsepolitseiamet, Kaitsevägi, Välisluureamet. Andmekogu volitatud töötleja andmekogu arendamisel, hooldamisel ja majutamisel on Siseministeeriumi infotehnoloogia- ja arenduskeskus (SMIT).

Identiteedihaldus – protsesse ja poliitikaid järgides mingi konteksti (süsteemi, ettevõtte, võrgu, riigi) piires vajalike identiteetide atribuutide (sh elutsükli, väärtuste, võimalike metaandmete) haldamine.

Õiguste haldus – kasutajate pääsuõigusi reguleerivate poliitikate ja protsesside määratlemine ja elluviimine.

Andmekogu – riigi, kohaliku omavalitsuse või muu avalik-õigusliku isiku või avalikke ülesandeid täitva eraõigusliku isiku infosüsteemis töödeldavate korrastatud andmete kogum, mis asutatakse ja mida kasutatakse seaduses, selle alusel antud õigusaktis või rahvusvahelises lepingus sätestatud ülesannete täitmiseks.

Avaliku teabe seadus, § 43[1] lg 1, vt https://www.riigiteataja.ee/akt/122032011010?leiaKehtiv

Isikuandmete töötlemine – isikuandmete või nende kogumitega tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum, näiteks kogumine, dokumenteerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, kustutamine või hävitamine.

Allikas: Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725 artikli 3 lõige 3

Turvaosaklass S2 – salajane info, mille kasutamine on lubatud ainult teatud kindlatele kasutajagruppidele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral.

Turvaosaklass S3 – ülisalajane info, mille kasutamine on lubatud ainult teatud kindlatele kasutajatele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral.

Allikas: Vabariigi Valitsuse 20.12.2007. a määrus nr 252 „Infosüsteemide turvameetmete süsteem“, vt https://www.riigiteataja.ee/akt/13125331?leiaKehtiv

[1] ABIS oli auditi ajal arendamisel andmekogu ja selles süsteemis ei oldud mitmeid planeeritavaid funktsionaalsusi kasutusele võetud.

Andmekogu vastutav töötleja – riigi- või kohaliku omavalitsuse asutus, muu avalik-õiguslik juriidiline isik või avalikke ülesandeid täitev eraõiguslik isik, kes korraldab andmekogu kasutusele võtmist, teenuste ja andmete haldamist. Andmekogu vastutav töötleja vastutab andmekogu haldamise seaduslikkuse ja andmekogu arendamise eest.

Avaliku teabe seadus, § 43[4]

Andmekogu volitatud töötleja – teine riigi- või kohaliku omavalitsuse asutus, avalik-õiguslikule juriidiline isik või hanke- või halduslepingu alusel eraõiguslik isik vastutava töötleja poolt ettenähtud ulatuses.

Avaliku teabe seadus, § 43[4]

Infoturbe kordade all on aruandes mõistetud infoturbe poliitikaid, protseduure ja juhendeid, mis kirjeldavad asutustes ja valitsemisalades kindlaks määratud infoturbemeetmeid.

5. Auditi ajal oli andmekogude pidamisel kohustuslik rakendada infoturbe raamistikku ISKE. Juurdepääsu halduse osas sisaldab see organisatsioonilisi ja IT-tehnilisi meetmeid nii andmekogu vastutavale kui ka volitatud töötlejale. Organisatsioonilised meetmed peavad sisalduma nii asutuse kui ka andmekogu tasemel IT või infoturbe juhtimise ja haldamise kordades või õigusaktides.

6. ISKE järgi peab juurdepääsu haldusega olema tagatud, et kasutajatel oleks juurdepääs üksnes nendele andmetele ja IT-ressurssidele, mida nad vajavad oma tööülesannete täitmiseks, ja ainult selles ulatuses, milleks neid on volitatud.[2]

7. Muu hulgas peab olema reguleeritud

- protseduuride ülesehitus ja rakendamine, et juhtida ja kontrollida juurdepääsu teabele ning ligipääsu IT-ressurssidele, eelkõige identiteetide ja volituste käsitlemist ning nende haldamist;
- kasutajate registreerimine, õiguste andmine ja äravõtmine;
- kasutajatunnuste ja nende juurde kuuluvate volituste haldus;
- kasutajatunnuste kontrollimine.

Andmepäringute põhjendatuse kontrolli ja logide regulaarset analüüsi ei ole juurdepääsukordades reguleeritud

8. Tagamaks, et andmetele saavad juurdepääsu ainult selleks volitatud isikud, peavad andmekogusid pidavas asutuses (või üle valitsemisala) olema kehtestatud juurdepääsuhalduse korrad. Juurdepääsuhalduse kordadega kehtestatakse näiteks järgmised asjaolud:

- määratud ja kirjeldatud on kasutajarollid, nende tööeesmärgid, kohustused ja vastutajaid;
- olemas on kasutajanimede loomise ja kasutajarühmade (rollide) moodustamise kord;
- õiguste andmise, muutmise, tühistamise ja kontrolli protsessi kirjeldus;
- paroolide kasutamise kord;
- autentimisviisid;
- privilegeeritud kasutajaõiguste haldamine ja kasutamine.[3]

9. Juurdepääsuhalduse korraldust reguleerivad dokumendid peab olema kinnitanud juhtkond ja neid peab olema regulaarselt uuendatud. Juurdepääsuhalduse kordasid tuleb tutvustada regulaarselt kõigile asutuse või valitsemisala töötajatele.

[2] ISKE B 1.18 „Identiteedi- ja volituste haldus“.

[3] ISKE M 2.585 „Identiteedi ja volituste halduse kontseptsioon“, M 2.11 „Paroolide kasutamise reeglid“, M 2.586 „Volituste andmine, muutmine ja äravõtmine“, M 2.220 „Pääsu reguleerimise suunised“.

10. Kõik olulisemad infoturbe põhimõtted peavad olema kirjalikult reglementeeritud, et sisekontrollisüsteem oleks toimiv ja võimaldaks aegsasti avastada kõrvalekaldeid ja rikkumisi kehtestatud nõuetest.

11. Nii Justiitsministeerium, Siseministeerium kui ka Sotsiaalministeerium on kogu valitsemisalas kehtestanud juurdepääsuhalduse korrad.

Valdav osa juurdepääsuhalduse korraldusest on reguleeritud

12. Audit näitas, et auditeeritud andmekogude haldajate valitsemisalades kehtestatud juurdepääshalduse korrad sisaldasid üldjuhul (vt aruande punktid 14–17) juurdepääsude haldamiseks vajalikke juhiseid (sh kirjeldatud kasutajarollid, õiguste juhtimise protsess, paroolide kasutamise kord ja privilegeeritud kasutajaõiguste haldus). Need juhised peaksid võimaldama juurdepääse turvaliselt hallata ning nende väljatöötamisel oli lähtutud ISKEst.

13. Auditeeritud andmekogude haldajate valitsemisalades on juurdepääsuhalduse kordades enamasti (vt punktid 14–17) ära määratud kasutajarollid ja nendega seotud kasutajaõigused. Nendes valitsemisalades peavad töötajad juurdepääsuhaldust puudutavate asjaoludega ja kordade tutvuma ning nendega tutvumist kinnitama oma allkirjaga.

Täpsemalt on reguleerimata andmepäringute põhjendatuse kontroll ja logide analüüs

14. Riigikontroll leidis, et kõigis vaadeldud andmekogude haldajate valitsemisalade kordades ja andmekogude regulatsioonides ei olnud reguleeritud andmepäringute põhjendatuse kontrolli põhimõtteid ning selliseid kontrolle tegelikkuses ka ei tehtud (vt punktid 79–84).

15. Sotsiaalkindlustusameti infoturbe kordades on kirjas küll säte, et infoturbe spetsialist kontrollib logide alusel vähemalt kord kvartalis isikuandmeid sisaldavate infosüsteemide sihipärast kasutamist. Samal ajal näitas audit, et vastava kontrolli tegemiseks ei ole välja töötatud juhiseid ega protseduure ning praktikas seda kontrolli ka ei tehtud. Lisaks ei olnud Sotsiaalkindlustusametis auditi tegemise ajal täidetud infoturbespetsialisti ametikoht.

Logi – kronoloogiline sündmuste andmik, mis talletatakse andmefailina järgnevaks läbivaatuseks ja analüüsiks. Juurdepääsuhalduse seisukohast on olulisemad logi liigid näiteks pääsulogi (andmed juurdepääsu saamise või pääsukatse kohta) ja tehingulogi (andmed andmebaasihalduse süsteemi sooritatud toimingute kohta).

Allikas: Andmekaitse ja infoturbe leksikon (AKIT)

16. Teise asjaoluna selgus, et auditeeritud andmekogude haldajate valitsemisalade infoturbe kordades ei ole kehtestatud logide regulaarse analüüsimise kohustust infoturbeintsidentide (sealhulgas juurdepääsuintsidentide) avastamiseks võimalikult varajases staadiumis. Üldine praktika on pigem see, et logisid analüüsitakse juhtumite järel või pärast seda, kui andmesubjekt on esitanud päringu (vt punktid 57–63).

Riigikontrolli järeldused ja soovitused

17. Riigikontrolli hinnangul on positiivne, et auditeeritud andmekogude haldajad on infoturbe kordades ja muudes dokumentides kehtestanud suurema osa juurdepääsu halduseks vajalikest infoturbe meetmetest. Samas vajavad nimetatud korrad parandamist ja täiendamist andmepäringute põhjendatuse kontrolli ning logide jooksva analüüsimise ja seire osas. See võimaldab riigi jaoks olulisi andmeid paremini kaitsta volitamata töötlemise eest ja avastada infoturbeintsidente palju varem.

18. **Riigikontrolli soovitus TEHIKu direktorile, RIKi direktorile ja SMITi peadirektorile:** täiendada valitsemisalade infoturbe dokumentatsiooni või andmekogusid reguleerivaid kordasid nõudega analüüsida süstemaatiliselt ja regulaarselt logisid ning kontrollida päringute põhjendatust.

TEHIKu direktori vastus: TEHIK võtab soovituse teadmiseks ning teeb andmekogude vastutava töötlejaga koostööd tehniliste lahenduste täpsustamisel ning vaatab üle ja vajadusel täiendab infoturbe dokumentatsiooni. Dokumentatsiooni uuendamine on kavandatud lõpetada 2023. aasta kolmandas kvartalis.

RIKi direktori vastus: Justiitsministeeriumil on plaanis 2023. a üle vaadata logipoliitika, mille raames vaadatakse üle ka käesolevas auditis kajastatud murekohad, sh räägime kindlasti läbi SIEMi kasutusele võtmise ning vahekontrollide teostamise vajaduse ja tellimise protsessi.

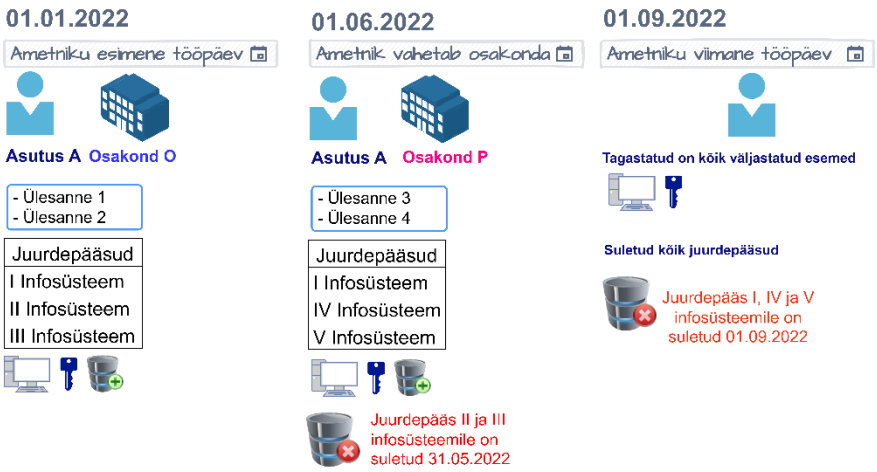
SMITi peadirektori vastus: Tegeleme hetkel SIEMi juurutamisega ja selle raames kordade uuendamisega. Siseministeeriumi valitsemisala infosüsteemide turvatestimise, turvanõrkuste haldamise ning nende logimise nõuete korras on logianalüüs ja pidev seire kaetud (punkt 5.1.9). SMIT ei saa auditeeritud andmekogudes teadmisvajaduse ehk päringute põhjendatuse kontrolli teha. SMIT ei ole andmete omanik ja ei kontrolli vastavat äriprotsessi. Andmete omanik saab põhjendada, kas saame või mitte ja tellida selle funktsionaalsuse (näiteks PPA).

Riigikontrolli kommentaar: Nõustume asjaoluga, et andmete omanik saab päringute põhjendatuse kontrolli teha ja SMIT saab eelkõige luua vastava funktsionaalsuse.

Õiguste andmine

19. Juurdepääsude andmisel andmekogu andmetele peab iga kasutaja puhul lähtuma ametikoha tööülesannetest ja vajadusest andmeid töödelda. Inimese asumisel ametikohale, tööülesannete täitmisel, tööülesannete muutumisel ja ametikohalt lahkumisel peab asutus tagama, et andmeid töödeldakse turvaliselt ja andmetele ei pääseks juurde volitamata kasutajad (vt joonis 2).

Joonis 2. Näide õiguste elukaarest



Allikas: Riigikontroll

Privilegeeritud kasutajate loomist tuleks paremini kontrollida

20. Juurdepääsuhalduses õiguste jagamiseks vajaliku süsteemi ja keskkonna loomiseks peab töökorralduses tagama mitmed põhieeldused:

- kasutajanimed peavad olema identiteedipõhised ja kasutajarühmad tuleb määrata rollipõhiselt;
- kasutajakonto, pääsuõigused ja profiilid peaksid olema loodud ja antud vajadusepõhiselt ning olema dokumenteeritud;
- õiguste komplektid tuleks luua sõltuvalt põhitegevusest ja tööülesannetest tekkinud vajadustest.[4]

21. Audit näitas, et vaadeldud andmekogudes ja nende haldajatel olid enamasti kindlaks määratud kasutajarollid ja nendega seotud kasutajaõigused, samuti olid kasutajanimed identiteedipõhised ja kasutajarühmad olid määratud rollipõhiselt.

22. Õiguste andmine uutele töötajatele või uuele ametikohale asunud töötajatele peab toimuma kontrollitult, nii et selle ametikoha eest vastutav pool (näiteks uue töötaja otsene juht) on teadlik töötajale vajalikust juurdepääsuõiguste komplektist ja kooskõlastab töötajale vaja olevad juurdepääsutaotlused. Andmekogu peakasutaja või tema volitatud osapool omakorda kinnitab vastavad taotlused.

23. Audit näitas, et juurdepääsuõiguste andmise protsess oli kordades reguleeritud ja enamasti ka ellu rakendatud kõigi auditeeritud andmekogude haldajate puhul. Üldjuhul tegelesidki vahetud ja valdkondade juhid töötajatele andmekogudes õiguste taotlemisega või taotluste kooskõlastamisega. Andmekogu peakasutajad või nende volitatud isikud kinnitasid need taotlused, peale seda avati vajalikud juurdepääsud.

Uute privilegeeritud kasutajate loomist SKA jooksvalt ei jälgi

24. Paaris andmekogus (VMP ja STAR) ei väljasta andmekogu pidaja juurdepääsuõigust ainult konkreetsetele kasutajatele. Seal antakse ka privilegeeritud kasutajaõigusi teise asutuse esindajale (STAR peamiselt omavalitsuste asutuste ning VMP pigem riigiasutuste esindajatele), kes saavad oma asutuse piires jagada kasutajaõigusi teistele töötajatele.

Privilegeeritud õigustega kasutaja – suuremate õigustega kasutaja, näiteks haldaja, hooldaja või seiraja. Sellise õigusega on tavaliselt usaldatud isik, sest kasutusvõimalused ja volitused on laiemad kui tavalisel kasutajal ning info kasutamise võimalused laiemad ja kriitilisemad. Teatud juhtudel võib selline kasutaja saada võimaluse muuta oma tegevuse märkamatuks, sh moonutades süsteemis olevat logi, nt kustutades seda.

Allikas: Riigikontroll ja AKIT

25. STARis võivad eelnimetatud privilegeeritud kasutajad luua omakorda teisi privilegeeritud õigustega kasutajaid. Auditi käigus selgus, et selliste uute privilegeeritud kasutajate loomist SKA jooksvalt ei jälgi. Kui andmekogul on privilegeeritud kasutajaid, kelle tegevust vastutav töötleja ei kontrolli, suureneb risk, et laiemaid kasutajaõigusi kasutatakse kurjasti ära.

Kontrollisüsteem õiguste muutmiseks ja äravõtmiseks on olemas

26. Kontrolliõiguste turvaliseks muutmiseks ja õigeaegseks sulgemiseks peab asutusest lahkuv töötaja tööandjale tagastama tööks kasutatava tööarvuti ja muu arvutustehnika ning tööandja sulgema töötaja juurdepääsud andmekogudesse ja IT-ressurssidele.

27. Kasutajaõiguste turvaliseks haldamiseks tuleks teha järgmist:

- peatada või õigel ajal sulgeda mittevajalikud kontod ja õigused,
- võimaldada ajutistele ja erakorralistele kontodele ainult ajaliselt piiratud juurdepääs,

[4] ISKE M 2.585 „Identiteedi ja volituste halduse kontseptsioon“.

- kontrollida regulaarselt juurdepääsuõigusi.

28. Audit näitas, et kirjeldatud sisekontrollisüsteem oli enamasti auditeeritud andmekogudes olemas. Kordades oli kirjas inventuuri läbiviimise kohustus ning selle teostamise kord. Ajutiste ja erakorraliste kontode puhul ei olnud juurdepääs andmekogule ajaliselt määratud, kuid selliste kontode sulgemine toimus tavaprotseduuri järgides. Siiski tagaks ajalise piirangu seadmine ajutistele ja erakorralistele kontodele paremini selle, et juurdepääsuõigused võetaks nimetatud kasutajatelt õigel ajal ära. Kasutajaõiguste inventuure tehti kõigis vaadeldud andmekogudes.

29. Auditi käigus viis Riigikontroll auditeeritavates andmekogudes läbi pääsulogide analüüsi, et veenduda, kas ajavahemikul 01.04.2021–31.03.2022 olid nimetatud andmekogudesse sisenenud ainult selleks volitatud isikud. Selleks võrreldi logiandmeid riigi personaliarvestuse (SAP tarkvara) andmetega ja kohalike omavalitsuste edastatud andmekogude kasutajate andmetega. Riigiasutuste ja omavalitsuste kohta koostati valimid (vt „Auditi iseloomustus“).

Logianalüüs tõi välja mõned vead juurdepääsude halduses

30. Analüüs näitas, et auditeeritud andmekogudes ei esinenud suuremaid eksimusi. Enamasti olid need põhjustatud kasutajaõiguste liiga hilisest äravõtmisest lahkuvatelt töötajatelt (nt lapsehoolduspuhkusele minejad).

Riigikontrolli järeldused ja soovitused

31. Riigikontroll leiab, et õiguste andmise protsess oli auditeeritud andmekogudes olulises osas kordades paika pandud ja ellu rakendatud. Samas oleks STARis ja VMPs vaja suuremat kontrolli selle üle, kuidas andmekogude volitatud kasutajad jagavad privilegeeritud kasutajaõigusi. Samuti näitas Riigikontrolli läbiviidud logifailide analüüs, et SKAISi ja STARi puhul ei taga sisekontrollisüsteem täpset õiguste andmise ja äravõtmise korraldust.

32. Riigikontrolli soovitused SKA peadirektorile ja TEHIKu direktorile:

- Muuta juurdepääsuõiguste andmine ja äravõtmine SKAISi ja STARi andmekogudes tõhusamaks ja täpsemaks, et kasutajatel oleks neile juurdepääs ainult selleks volitatud ajal.
- Seada edaspidi ajutistele ja erakorralistele kontodele ajalise piiranguga kasutajaõigused, nii et need antakse ja võetakse ära kindlatel kuupäevadel.
- Muuta õiguste andmise protsessi nii, et vastutav töötleja kas annaks ainult ise privilegeeritud kasutajaõigusi volitatud kasutajatele või omaks nende õiguste andmise üle suuremat kontrolli.

SKA peadirektori vastus: Soovituses välja toodud funktsionaalsuste puudujäägid esinevad meie infosüsteemide vanades rakendustes, mida edasi ei arendata. Arendame nõuetekohased funktsionaalsused oma uues infosüsteemis.

Privilegeeritud kasutajaõiguste andmise kitsendamiseks STARis nii, et privilegeeritud kasutajaid saaks luua ja nendele õiguseid anda ainult SKA töötajad, on arenduste prioriteetsete tööde järjekorras. 2023. aasta lõpuks saame anda täpsema info arendusprotsessi seisu kohta.

Ajutiste ja erakorraliste kontode õigeaegseks andmiseks ja sulgemiseks arenduste valmimisteni jälgib STARi kasutatugi õigustatuse perioodi ja vastavalt tööprotsessile avab ja sulgeb kontod õigeaegselt käsitsi.

Juurdepääsu tagamine

33. Juurdepääsu administratiivset andmist, muutmist ja äravõtmist peab organisatsiooniliste protsesside kõrval toetama ka andmekogu, selle käitamiseks kasutatava infosüsteemi ülesehitus ja juurdepääsuhalduse korraldamist võimaldavad süsteemid. On märgatavalt efektiivsem, kui õigustega seotud muudatused toimuvad asutuse põhitegevuses tehtavatest otsustest ja toimuvatest protsessidest lähtudes.

Andmekogudes STAR ja SKAIS1 on kasutajatel liiga ulatuslikud juurdepääsud

34. Efektiivse juurdepääsuhalduse andmekogudes tagab olukord, kus asutuste kordades kehtestatud reeglid on rakendatud andmekogu käitavas infosüsteemis. See tähendab, et juurdepääs infosüsteemis on võimalik vaid nendele andmetele, mis on kasutajarollis ette nähtud. Kui erinevate kasutajaprofiilide hulk ei ole andmekogus piisav, siis peaks olema võimalik andmekogus detailseid õigusi eraldi jagada, et tööks mittevajalikud andmed ei oleks kasutajatele kättesaadavad.

Juurdepääsuõigusi pole SKAIS1-s võimalik piirata

SKAIS ehk sotsiaalkaitse süsteem koosneb sisuliselt kahest infosüsteemist:

SKAIS1 – Sotsiaalkindlustusameti vanal platvormil olev infosüsteem, mis toetab ameti avalike teenuste tööprotsesse, sh riikliku pensionikindlustuse registri tööd.

SKAIS2 – uuemal platvormil olev infosüsteem, mida on arendatud eesmärgiga asendada SKAIS1, kuid seni pole suudetud seda teha, arendustegevused jätkuvad.

Allikas: Riigikontroll

35. Audit näitas, et sotsiaalkaitse infosüsteemi vanemas versioonis ehk SKAIS1-s ei ole võimalik juurdepääsuõigusi anda nii, et kasutajatel oleks juurdepääs ainult tööülesannete täitmisega seotud andmetele ja välistatud oleks juurdepääs andmetele, mida tööks vaja ei ole. SKAIS1-s on kõigil kasutajatel valdkonniti ühesugused kasutajaõigused.

36. Kui andmekogus ei ole täpselt kindlaks määratud, kellele ja mis ametikohal antakse mingid kasutajaõigused ja juurdepääs andmetele, siis ohustab see paratamatult andmesubjektide privaatsust. Juurdepääsuõiguse andmisel tuleb lähtuda asutuse põhitegevusest, töötaja tööülesannetest ja teadmisvajadusest.

37. Nii nagu andmekogudes eksisteerivad erinevate kasutajarollide puhul keelud või piirangud mingit liiki andmeid töödelda, võivad olemas olla ka vajadused piirata juurdepääsu andmetele haldusüksuse piires. See omakorda tähendab, et näiteks teatud asutuses või piirkondlikus üksuses töötaval andmekogu kasutajal tuleb lubada juurdepääsu vaid selle asutuse või piirkonna andmetele.

38. Andmekogu käitavas infosüsteemis on erinevate kasutajate töö iseloomust, s.t nende teadmisvajadusest lähtuvalt võimalik piirata juurdepääsu erinevatele andmeväljadele. Samuti peab olema võimalik juurdepääsu piirata näiteks valdade/linnade kaupa, kus andmesubjektid elavad. Auditis vaadeldud andmekogude puhul on selline vajadus olemas näiteks kohalikel omavalitsustel (KOV), kui nad kasutavad STARis olevaid andmeid.

STARi kasutajatele KOVides ei rakendata valla-/linna-põhiseid juurdepääsu-piiranguid

39. KOVid otsustavad ja korraldavad kohaliku elu küsimusi eelkõige oma valla/linna piirides, seepärast aitaks KOVi-põhised piirangud vähendada andmete väärkasutuse riske. Kui aga näiteks KOVi töös tekib vajadus töödelda teiste valdade/linnade elanike isikuandmeid, siis peab SKA selleks välja töötama eraldi protseduurid, mis tagaksid seesuguse

teadmisvajaduse eelneva hindamise. Praegu sellised protseduurid STARi puhul puuduvad, kasutaja saab oma otsustusest lähtudes avada menetluse iga andmekogus oleva isiku suhtes.

40. Riigikontrolli hinnangul on SKAIS1 ja STARi kasutajatel liiga ulatuslik juurdepääs. Näiteks on STARis KOVi ametnikul võimalik vaadata ka teiste KOVide elanikega seotud menetlusi ja neis sisalduvaid andmeid, kui ta on ise loonud menetluse nende elanike suhtes. Selline vaatamine ei ole võimalik juhtudel, kui menetleja on märkinud menetluse kinniseks.

41. Andmekogu STAR on kasutusel olnud alates aprillist 2010 ja sellest ajast saadik ei ole andmeid andmekogust välja viidud, näiteks arhiveeritud. Selle tulemusel on menetluste hulk, millele kasutajatel on juurdepääs, suhteliselt suur. See lisab suure hulga isikutega seotud andmete kaitsmise vajadusele veel suurema kaalu.

42. Piirangute kehtestamine andmekogude juurdepääsuõigustes andmesubjektide kaupa on niisama oluline kui andmeväljade kaupa. Seesuguste piirangute puudumisel võivad andmetele juurdepääsu saada kasutajad, kelle tööülesanded seda ei nõua.

Privilegeeritud kasutajate tegevusi logitakse

43. Teatud ülesannete täitmiseks andmekogude arendamisel ja haldamisel on vajalikud ka kasutajarollid, mille puhul antakse tavapärasest suuremad õigused. Ka nende õiguste üle peab andmekogu vastutaval töötlejal olema tõhus kontroll, sest sellises rollis on kasutajatel tavapärasest ulatuslikumad õigused ja andmete töötlemisel suurema kahju tekitamise risk.

44. Privilegeeritud kasutajate õiguste haldamisel on oluline, et administraatori kontode loomise, muutmise ja kustutamisega seotud tegevusi logitakse ning privilegeeritud õigustega kasutajate tegevusi analüüsitakse.

Privilegeeritud kasutajate logisid kogutakse ja säilitatakse

45. Audit näitas, et privilegeeritud kasutajate haldamiseks ja nende töö korraldamiseks vajalikud reeglid on paika pandud detailsemate töökorraldust reguleerivate dokumentidega, näiteks infoturbekordade, ametijuhendite, andmemajutuslepingutega. Kõikides auditis vaadeldud andmekogudes logitakse privilegeeritud kasutajate juurdepääsuhaldusega seotud tegevusi ning nende kasutajate tegevusi analüüsitakse intsidentide järel vajaduse korral.

Riigikontrolli järeldused ja soovitused

46. Riigikontrolli hinnangul on juurdepääsu tagamisel üldiselt olemas vajalik sisekontrollisüsteem, vaid STARi ja SKAIS1 puhul on andmekogude kasutajatel liiga ulatuslik juurdepääs või puudub vastutava töötleja kontroll nende üle. See suurendab riske olukorras, kus jooksvat logide analüüsi ei tehta (vt p-d 57–63) ja päringute põhjendatust süstemaatiliselt ei kontrollita (vt p-d 80–84). Privilegeeritud kasutajate tegevusi auditeeritud andmekogudes logitakse.

47. Riigikontrolli soovitus SKA peadirektorile ja TEHIKu direktorile: tagada, et STARi andmekogu kasutajad kohalikes omavalitsustes saaksid juurdepääsu vaid samas omavalitsuses elukoha aadressi registreerinud inimeste ja nendega seotud menetluste andmetele. Kui aga vajatakse juurdepääsu teiste valdade/linnade elanikega seotud

menetlustele, siis määrata kindlaks kontrolliprotseduur täiendava juurdepääsu valideerimiseks.

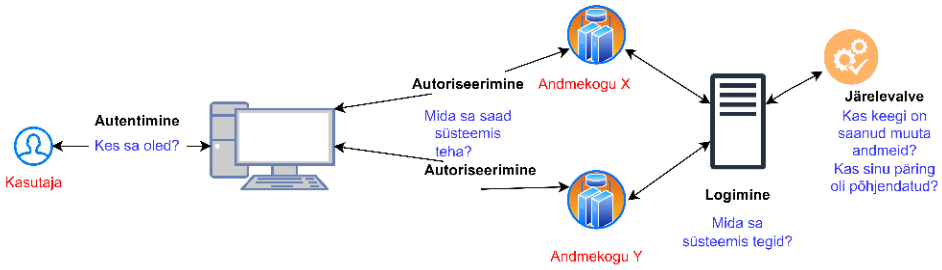
SKA peadirektori vastus: SKA on seisukohal, et tegemist ei ole liiasusega, kuna nimetatud laiem lähenemise vajadus on seotud KOVide töö spetsiifikaga. Abivajaduse hindamine on aegkriitiline protsess ja abivajaduse hindamiseks ja sobiva sekkumisviisi leidmiseks vajab KOV tervikpilti, mis võib olla KOVide-ülene, kuna inimene võib olla registreeritud teise KOVi elanikuks, mitte KOVi, kus ta reaalselt elab. Samuti on lastekaitse juhtumite lahendamisel oluline mitme KOVi samaaegne koostöö, kuna lapsevanemad võivad olla erinevate KOVide elanikud. Probleemi lahendamiseks ei saa oodata teise KOVi või SKA nõusolekut, kuna sekkumise kiirusest võib sõltuda ka abivajaja elu ja tervis.

Riigikontrolli kommentaar: Kui SKA hinnangul ei ole võimalik korraldada juurdepääsutaotluse menetlust piisavalt kiiresti ja selliselt, nagu abivajaduse hindamise protsess seda nõuab, siis tuleb andmete väärkasutuse ärahoidmiseks ja avastamiseks seda enam rakendada muid meetmeid (vt punktid 64 ja 86).

Õiguste jõustamine

48. Kui andmekogude juurdepääsuõigused on tehnoloogiliselt kindlaks määratud, kasutajatele üle antud ning riist- ja tarkvaraliselt kättesaadavaks tehtud, siis tuleb ka kogu andmekogu kasutamise ajal need õigused jõustada, s.t tagada sisekontrollimeetmed, mis kindlaks määratud piirangud ka tõhusalt ellu rakendaks (vt joonis 3).

Joonis 3. Olulisemad juurdepääsuõiguste jõustamise vahendid.



Allikas: The Institute of Internal Auditors ja Riigikontroll

Autentimine – identiteediväite kontroll: üks kasutaja, süsteem, muu olem kontrollib teise olemi väidetava identiteedi tõesust, aluseks on tavaliselt mingi spetsiifiline

- esitatud teave, näiteks parool;
- ese, näiteks kiipkaart vm turvatõend;
- eristav püsitunnus (biomeetrik);
- eristav asukoht (aadress).

Allikas: AKIT

Kaheastmeline või kahefaktoriline autentimine ehk kaksikautentimine – kahe sõltumatu identsustõendiga autentimine, multiautentimise lihtsaim vorm.

Allikas: AKIT

49. Esmasteks õiguste jõustamise vahenditeks andmekogu kasutama asudes on kasutajate identiteedi kindlakstegemine (autentimine) ja juurdepääsu andmine pääsuõiguste alusel (autoriseerimine). Juba andmekogude kasutamise hetkel saab juurdepääsuõiguste jõustamise vahendiks logi, kuhu talletatakse kõik andmekogus tehtud toimingud kas jooksvaks automaatseks analüüsiks (vt punktid 75–78) või hilisemaks läbivaatuseks ja kontrolliks.

Autentimiseks kasutatakse üldjuhul keskseid teenuseid

50. Autentimine ja autoriseerimine peab andmekogudes toimuma turvaliselt. Eelistatult võiks selleks kasutada kaheastmelise autentimise vahendeid, näiteks ID-kaart, mobiil-ID või Smart-ID. Samuti on oluline võimaluse korral kasutada autentimiseks erinevaid viise, et ühe autentimisvahendi rikke korral ei seiskuks töö andmekoguga.

SKAIS1 ei kasuta turvalise autentimise vahendeid

TARA – Riigi Infosüsteemi Ameti (RIA) arendatud ja hallatav platvorm, mis on liidestatud kolmanda isiku pakutavate autentimismeetoditega ning teeb autentimiseks vajalikke andmepäringuid. TARA kasutab omavahel kombineerides või eraldi erinevaid autentimismeetodeid, sh ID-kaart, mobiil-ID, Smart-ID ja Euroopa Liidu eID.

Allikas: RIA

Terviklus – lubamatute muudatuste puudumine, hõlmab ka autentsust ja salgamatust, üks teabe turvalisuse kolmest põhikomponendist levinuimas turvamudelis.

Allikas: Eesti infoturbestandard ehk E-ITS

Logifailide säilitamine on reguleeritud

Logide regulaarset analüüsi ei tehta

51. Auditis vaadeldud andmekogudest olid SKAIS1-s kasutusel kasutajanimed ja paroolid. SKAIS2, STAR ja VMP puhul toimub autentimine ja autoriseerimine, kasutades riigi autentimisteenust TARA. ABISesse ja KARRi logitakse sisse asutuse sisevõrgust või teise asutuse sisevõrgust x-tee teenuste kaudu.

52. Kui tundlikke andmeid sisaldavasse andmekogusse saab sisse logida, kasutades üheastmelist autentimisviisi, näiteks kasutajanime ja parooli, siis see suurendab riski, et nendele andmetele võidakse saada volitamata juurdepääs. SKAIS1 kasutamise puhul on seega nimetatud riski realiseerumise tõenäosus suurem.

Logide tervikluse tagamiseks tuleks rakendada täiendavaid meetmeid

53. Käesolevas aruandes (vt p 15) on juba kirjeldatud kasutajalogide olulisust juurdepääsuhalduse kindlustamisel ja andmekogudesse volitamata juurdepääsu takistamisel. Et logifailides oleks kättesaadav kogu info andmekogus toimunud tegevuste kohta, peab olema tagatud logide terviklus, s.t välistatud võimalus logifaile muuta või kustutada logide säilitamistähtaja jooksul. Logifailide kustutamise või muutmisega võidakse varjata andmekogudele volitamata juurdepääsu ärakasutamist, sh näiteks andmete töötlemist (k.a vaatamist, muutmist, kustutamist).

54. Audit näitas, et logiandmete salvestamise ja hoiustamise reeglid on vaadeldud andmekogude tegevust reguleerivates dokumentides enamasti kirjeldatud. Nende andmekogude puhul on kasutusel logiserver, kuhu kõik logifailid salvestatakse ning kus need on vajaduse korral kättesaadavad analüüsimiseks.

55. Riigikontrolli hinnangul tuleks auditeeritud andmekogude juures hinnata logide volitamata muutmisega seonduvaid riske ja sellest tulenevalt rakendada logide tervikluse tagamiseks ajatembeldamise ja/või krüptoaheldamise lahendusi.

56. Nii nagu peavad olema kaitstud tundlikud andmed andmekogudes, peab olema kaitstud ka info nende andmetega toimunud tegevuste ehk logide kohta. Kui siin eksisteerib võimalus logide tervikluse ohustamiseks volitamata muutmise ja kustutamise kaudu, on olemas ka võimalus ilma jälgi jätmata ohustada andmete enda terviklust.

Logisid ei analüüsita regulaarselt

57. Juurdepääsuõiguste jõustamisel on oluline ka logifailide korrektne haldamine ja analüüsimine. Kui logifailide terviklus on tagatud, siis logifailide säilitamine, kättesaadavaks tegemine ja nende analüüsimine aitavad andmete kasutamist jooksvalt kontrollida, aga ka uurida oluliste turvaintsidentide põhjuseid.

58. Selleks peab andmekogu vastutaval töötlejal olema välja töötatud logimist (sh logihaldust ja seiret) reguleeriv juhendmaterjal. Samuti peab olema kindlaks määratud, milliseid komponente (nt teenused, rakendused) tuleb logida ning kes vastutavad logide halduse erinevate tegevuste eest.

59. Auditis vaadeldud andmekogude haldajatel olid logimise reeglid enamasti olemas, ehkki mitte küll alati eraldi dokumentidena, vaid pigem

andmekogude põhimääruste, seaduste või muude regulatsioonide ühe osana. Samuti näitas audit, et juurdepääsudega seotud tegevusi küll logitakse, kuid logide analüüsimise korraldust ei ole kordades sätestatud.

60. Andmete väärkasutuse avastamiseks peaks andmekogu logifaile regulaarselt analüüsima. See on samuti vajalik intsidentide korral nende põhjuste väljaselgitamiseks.

61. Auditi käigus selgus, et intsidentide korral analüüsitakse kõikides auditeeritud andmekogudes logifaile, et kindlaks teha intsidentide toimumise üksikasjad ning seejärel eemaldada nõrkused sisekontrolli-süsteemides (näiteks rakendades täiendavaid infoturbemeetmeid). Ent regulaarset ja süstemaatilist logifailide analüüsimist, mis võimaldaks jooksvalt või operatiivselt avastada andmete mittelubatud töötlemist, auditis vaadeldud andmekogudes ei toimu. See ei ole infoturbekordades ka enamasti kohustuseks tehtud.

62. Ilma logifailide regulaarse kontrollita ei ole võimalik operatiivselt avastada nõrkusi andmekogude juurdepääsu kaitsemeetmetes. Selle tulemusena kas ei avastata infoturbeintsidente üldse või avastatakse need siis, kui andmekogudele on tekitatud juba suuremat kahju. Samuti võidakse avastada liiga hilja muud tehnilised ja organisatsioonilised puudujäägid, mis võivad tekitada probleeme asutuste ja infosüsteemide töös.

Riigikontrolli järeldused ja soovitused

63. Riigikontroll leiab, et auditeeritud andmekogudes kasutatavad autentimislahendused on turvalised, välja arvatud SKAIS1-s kasutatav üheastmeline autentimine. Logide tervikluse tagamiseks aga peaks auditeeritud andmekogude haldamisel kasutusele võtma täiendavaid meetmeid (nt ajatembeldamist ja/ või krüptoaheldamist), et kõrgema taseme terviklus- ja konfidentsiaalsusnõuetega andmeid paremini kaitsta. Andmekogudes tekkivaid logisid ei analüüsita regulaarselt ja süstemaatiliselt, vaid seda tehakse ainult avastatud infoturbeintsidentide uurimisel.

64. Riigikontrolli soovitused TEHIKu direktorile, RIKi direktorile ja SMITi peadirektorile:

- Täiendada infoturbe dokumentatsiooni ja praktikaid logide süstemaatilise ja regulaarse analüüsimise sisseviimisega IT-sisekontrollimeetmete hulka. Selleks on soovitatav kasutusele võtta turvateabe ja sündmuste analüüsimise vahend SIEM (vt ka punkt 76).
- Hinnata logide volitamata muutmisega seonduvaid riske ja sellest tulenevalt rakendada logide tervikluse tagamiseks ajatembeldamise ja/või krüptoaheldamise lahendusi.

TEHIKu direktori vastus:

- TEHIK võtab soovituse teadmiseks ning teeb andmekogude vastutava töötlejaga koostööd tehniliste lahenduste täpsustamisel ning vaatab üle ja vajadusel täiendab infoturbe dokumentatsiooni. Dokumentatsiooni uuendamine on kavandatud lõpetada 2023. aasta kolmandas kvartalis.

- SIEM on TEHIKus kasutusel ning SKAISi ja STARi andmete töötlemiseks kasutatakse tööjaamadel ja võrguühendustel automatiseeritud järelevalvet, et tuvastada tavapärasest erinevaid protsesse, kasutajaid, võrguühendusi või sisselogimisi, ning korraldatud on igapäevane tulemuste analüüs potentsiaalsete turvarikkumiste tuvastamiseks. Rakendatud on kõrvalekaldeid automaatselt tuvastavad tööriistad.

RIKi direktori vastus:

- Justiitsministeeriumil on plaanis 2023. a üle vaadata logipoliitika, mille raames vaadatakse üle ka käesolevas auditis kajastatud murekohad, sh räägime kindlasti läbi SIEMi kasutusele võtmise ning vahekontrollide teostamise vajaduse ja tellimise protsessi.

- Plaanime teostada EITSe rakendamise raames riskianalüüsid 2023.–2024. a. Nende riskianalüüside raames vaadatakse üle süsteemi logide ajatembeldamise ja/või krüptoaheldamise vajadus.

SMITi peadirektori vastus: Tegeleme hetkel SIEMi juurutamisega ja selle raames kordade uuendamisega ning automaatse logide analüüsiga. Tegeleme hetkel ka TrueTrail-i juurutamisega. SMITis on käimas vSOC-projekt, mille raames võetakse kasutusele SIEM. Logide protsessiga on tagatud logide terviklus.

65. **Riigikontrolli soovitus SKA peadirektorile ja TEHIK-u direktorile:** muuta SKAIS1 andmekogus autentimine turvalisemaks, s.t kasutada kaheastmelist lahendust.

SKA peadirektori vastus: Nimetatud puudujääk esineb meie infosüsteemi vanades rakendustes, mida edasi ei arendata. Meie uues infosüsteemis on nõuetekohane kaheastmeline autentimise lahendus rakendatud, praegu veel vanades rakendustes kasutatavad funktsionaalsused viiakse uude infosüsteemi üle. Tegeleme teenuste üleviimisega aktiivselt, aga tähtaega ei saa hetkel prognoosida, kuna see sõltub, kui palju tuleb kõrgema prioriteediga poliitilisi arendussoove.

Seniks on SKAIS1 turvalisus tagatud alljärgnevate meetmetega:

- SKAIS1 saab kasutada ainult kasutaja, kellele on loodud meie domeenis kasutajakonto ja kes omab TEHIKu väljastatud ja TEHIKu kontrolli all olevat arvutit;

- pensionide ja hüvitistega seotud rakendus ei ole veebipõhine, vaid kasutaja arvutisse on installeeritud SKAIS1 (n-ö paks klient);

- TEHIK teeb konkreetse arvuti registrites kliendipõhiselt muudatusi, ilma milleta ei ole kasutajal võimalik SKAIS1-te sisse logida;

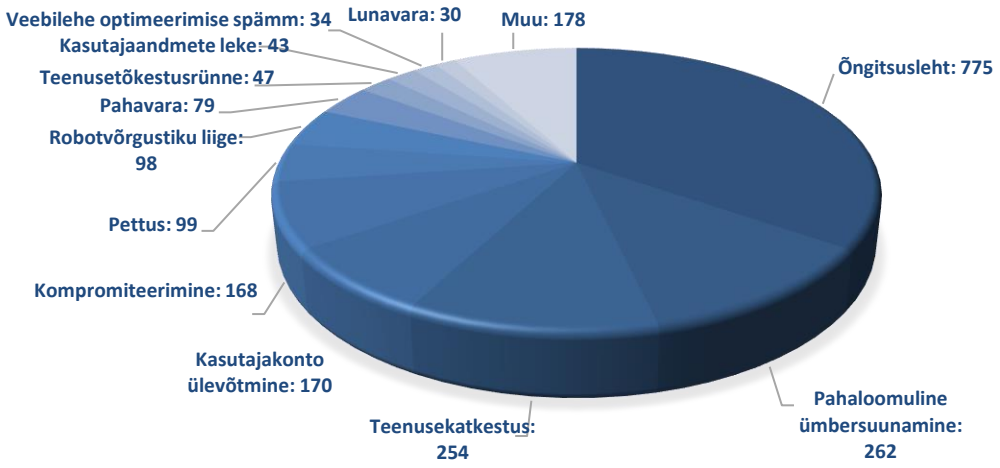
- rakendatud on minimaalselt 12 tähemärgise salasõna kohustus autentimisel;

- välisvõrgust saab kasutaja SKAIS1 sisse logida ainult TEHIKu väljastatud arvutiga üksnes üle VPN,i mis on kaheastmelise autentimisega.

Juurdepääsuhalduse sisekontrollisüsteem ja järelkontroll

66. Kaitseks kübermaailmas valitsevate ohtude vastu peab iga andmekogu vastutav töötleja looma piisava infoturbe- ja sisekontrollisüsteemi. 2021. aastal laekus Riigi Infosüsteemi Ameti intsidentide käsitlemise osakonda (CERT-EE) 20 077 registreeritud teavitust küberjuhtumitest.[5] Automatiseeritud teateid turvanõrkustest laekus aga koguni 73 826 ja automatiseeritud teateid nakatumistest 14 332. Mõjuga intsidente registreeriti kokku 2237, nende täpsem jaotus on toodud joonisel 4.

Joonis 4. Mõjuga intsidentide arv 2021. aastal



Allikas: Küberturvalisuse aastaraamat 2022

67. Suurem osa infoturbeintsidentidest toetub juurdepääsu ülevõtmisele või on suunatud juurdepääsuõiguste ärakasutamisele. Näiteks üritatakse õngitsuskirjade ja -lehtede levitamise kaudu üle võtta võõraid kasutajakontosid ja seeläbi ohustada andmete õigsust või teha need kättesaadavaks isikutele, kellel andmete töötlemise õigus puudub.

68. Tõhus sisekontrollisüsteem ja järelkontroll juurdepääsude haldamisel aitab vältida olulise mõjuga küberintsidentide toimumist andmekogudes. Samuti aitavad järelkontrolli protseduurid avastada intsidente, mille ilmsikstulek teiste allikate kaudu ei oleks võimalik.

Infoturberaamistiku ISKE rakendamist ei ole vaadeldud andmekogudest auditeeritud ABISe puhul

69. Riigis on andmekogude pidamisel tõhusa sisekontrollisüsteemi loomise esmane vahend ISKE. Selle rakendamine on kohustuslik kõigi riigi ja omavalitsuse andmekogude pidamisel.[6] Samuti on kohustuslik turvameetmete süsteemi rakendamise regulaarne sõltumatu audit.[7]

70. Käesolevas auditis vaadeldud andmekogud sisaldavad enamasti tundlikke andmeid, millele on kehtestatud kõrgemad tervikluse ja konfidentsiaalsuse nõuded, ning seetõttu klassifitseeruvad need kas kõrgema või keskmise turbeastmega andmekogudeks. Kõrge

Teadmiseks, et

senine infoturbesüsteem ISKE kehtib kuni 31.12.2023. Selleks ajaks peavad kõik ISKE rakendajad minema üle uuele infoturbestandardile ehk E-ITSile.

Allikas: https://www.ria.ee/et/kuberturvalisus/eesti-infoturbestandard.html

[5] Küberturvalisuse aastaraamat 2022. Riigi Infosüsteemi Amet.

[6] Avaliku teabe seadus, § 43^9 lg 1 ja 3.

[7] Vabariigi Valitsuse 20.12.2007. a määrus nr 252 „Infosüsteemide turvameetmete süsteem“, § 9^1

turbeastmega andmekogudes tuleb ISKE auditeid läbi viia iga kahe aasta järel, keskmise turbeastmega andmekogudes iga kolme aasta järel.[8]

71. Auditi käigus selgus, et SKAISis on ISKE rakendamise audit läbi viidud aastatel 2016 ja 2019, STARis 2018 ja 2021, VMPs 2020 ja KARRis aastal 2020. Andmekogus ABIS ei olnud ISKE auditeid tehtud.

72. Toimunud ISKE rakendamise auditite aruandeid kontrollides selgus, et auditeeritud andmekogudes ei ole vaadatud juurdepääsude haldusega seotud moodulisse[9] kuuluvaid meetmeid. ISKE auditi juhendi kohaselt tuleb igas auditis üle kontrollida vaid moodulisse B 1.0 „Infoturbe haldus“ kuuluvate infoturbe meetmete rakendamine.[10]

73. Teistest moodulite gruppidest tuleb auditeerimiseks valida juhusliku valimi meetodit kasutades kaks moodulit, ning arvestades tellija esindaja arvamust, viis kõige kaalukamat moodulit. Samuti võib audiitor hinnata vajaduse korral täiendavalt muude turvameetmete rakendamist või teha seda ISKE auditi tellija soovil. Sellise reeglistiku raames ei sattunud ja ei valitud käesolevas auditis olevate andmekogude ISKE rakendamise auditite valimisse kunagi identiteedi- ega volituste halduse moodulit.

74. Olukorras, kus infoturbe raamistiku rakendamist juurdepääsude haldamisel ei ole üle vaadanud sõltumatu väline hindaja, võib juhtuda, et vajalikke infoturbe meetmeid ei ole kas rakendatud või sisaldavad need nõrkusi, mida saab andmete tervikluse kahjustamiseks ära kasutada.

Turvateabe ja -sündmuste jooksvat automaatkontrolli ei tehta

75. Andmekogudes, mis sisaldavad suurel hulgal tundlikke andmeid (sh isikuandmeid) ja mille kasutus on väga intensiivne, on juurdepääsuhalduse seisukohast väga oluline, et nende kaitseks oleks rakendatud ennetavaid meetmeid. Näiteks võiks asutuste sisekontrollisüsteem tuvastada suuremahulisi andmete päringuid või allalaadimisi juba toimumise hetkel.

SIEM ehk– turvateabe ja -sündmuste haldus (*Security Information and Event Management*) – tarkvara ja teenuste valdkond, mis ühendab turvateabe haldust ja turvasündmuste haldust ehk võimaldab koguda logi ja andmeid ning aitab tuvastada kõrvalekaldeid.
Allikas: AKIT ja Riigikontroll

Jooksvat logide analüüsi ei tehta

76. Kui andmetöötlemise kohta tekib logifaile suures mahus, siis on selliseid kontrolle käsitsi läbi viia peaaegu võimatu, seega peab nende kontrollide tegemiseks kasutama infotehnoloogilisi lahendusi. Enamasti kasutatakse sellistel puhkudel turvateabe ja sündmuste analüüsimise vahendit ehk SIEM-lahendust.

77. Auditi käigus selgus, et auditeeritud andmekogudes jooksvat logide analüüsi andmete väärkasutuse leidmiseks ei tehta. Turvateabe ja -sündmuste halduse lahendused ei olnud RIKis (KARR) ja SMITis (VMP ja ABIS) kasutusel. TEHIK (SKAIS ja STAR) on kasutusele võtnud SIEMi tarkvara, ent ei olnud seda kasutanud vaadeldud andmekogude logi analüüsimisel. Seega ei ole 2022. aastal auditeeritud andmekogusid pidavates asutustes SIEM-süsteeme käivitatud nii, et oleks võimalik logisid automaatselt ja jooksvalt analüüsida.

78. Logide automaatse ja jooksva analüüsi puudumine suurendab riski, et andmekogude vastutavad kasutajad ei avasta volitamata tegevusi andme-

[8] Sealsamas § 9[1] lg 1.
[9] ISKE B 1.18 „Identiteedi- ja volituste haldus“.
[10] ISKE auditi juhend (versioon 1.4), p 6.

kogude kasutamisel või avastavad need juba siis, kui nende tegevuste tõttu on tekkinud kahju. Regulaarne logide analüüs looks võimalused varajasemas staadiumis andmete väärkasutus avastada ja lõpetada.

Regulaarselt ja süstemaatiliselt teadmisvajadust ei kontrollita

79. Isegi kui andmekogu vastutav töötleja annab volituse andmeid töödelda, peab volitatud kasutajal olema selleks ka n-ö teadmisvajadus. Käesolevas aruandes on teadmisvajaduse all mõeldud andmekogu volitatud kasutaja või tema esindaja õigust isikuandmeid töödelda, lähtudes isikuandmete kaitse üldmäärusest.[11]

80. Selline õigus tekib muu hulgas siis, kui isikuandmeid on vaja töödelda

- vastutava töötleja juriidilise kohustuse täitmiseks;
- andmesubjekti või mõne muu füüsilise isiku eluliste huvide kaitsmiseks;
- avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks;
- vastutava töötleja või kolmanda isiku õigustatud huvi korral, välja arvatud juhul, kui sellise huvi kaaluvad üles andmesubjekti huvid või põhiõigused ja -vabadused, mille nimel tuleb kaitsta isikuandmeid, eriti juhul kui andmesubjekt on laps.

Andmepäringute põhjendatust regulaarselt ja süstemaatiliselt ei kontrollita

81. Auditi käigus selgus, et auditeeritud andmekogudes viiakse teadmisvajaduse (andmepäringute põhjendatuse) kontrolli läbi ebaregulaarselt, see tähendab vaid avastatud intsidentide, andmesubjektide päringute, kaebuste või muude väliste motivaatorite sunnil. Süstemaatilist ja regulaarset seiret ega kontrollimisi ei tehta.

Andmejälgija – lahendus, mis jälgib andmekogu sisest ja sellest väljuvat liiklust, eraldab sealt vajalikud logikirjed ning salvestab need andmesalvestisse. Andmesalvestil on liides, mille kaudu kuvatakse vajalik informatsioon inimesele riigiportaalis eesti.ee.

Allikas: RIA

82. Andmesubjektidel, s.t inimestel, kelle andmed on andmekogudes, on õigus osaliselt siiski saada infot iseenda andmete töötlemise kohta. Nimelt on Riigi Infosüsteemi Amet loonud andmejälgija lahenduse, mis võimaldab pakkuda inimestele selget ülevaadet tema andmetega sooritatud toimingutest.

83. Seesugune võimalus jälgida andmesubjektidel nendega seotud päringuid on realiseeritud pooltes vaadeldud andmekogudest. Andmejälgijaga on liidestatud STAR ja SKAIS. KARRi on see funktsionaalsus sisse ehitatud e-toimikusse ja võimalik on saada infot enda kohta päringu teinud isikute kohta.

84. Olukord, kus andmete töötlemise kohta info saamine ei ole paljudes andmekogudes hõlbus ning andmekogude vastutavad töötlejad ei kontrolli teadmisvajaduse olemasolu süstemaatiliselt ega regulaarselt, ei ole andmekaitse seisukohast läbipaistev. Sellises olukorras võivad paljud seadusliku aluseta andmetöötlusepisoodid jääda avastamata ja isikute eraelu puutumatus satub ohtu.

[11] Isikuandmete kaitse põhimääruse 2. peatükk „Põhimõtted“, artikkel 6 „Isikuandmete töötlemise seaduslikkus“, p 1

Riigikontrolli järeldused ja soovitused

85. Audit näitas, et kohustuslik infotarbe raamistik ISKE oli auditeeritud andmekogudes küll rakendatud, kuid ühe andmekogu puhul ei ole selle rakendamist kunagi auditeeritud. Riigikontrolli hinnangul on see tundlike andmete tõttu oluliseks riskiks andmete turvalisusele. Samuti ei tee ühegi auditeeritud andmekogu vastutav töötleja turvateabe ja -sündmuste jooksvat automaatkontrolli. Andmepäringute põhjendatust kontrollitakse vaid pisteliselt ja intsidendipõhiselt. Regulaarne ja süstemaatiline teadmisvajaduse kontroll puudub.

86. Riigikontrolli soovitused justiitsministrile, Politsei- ja Piirivalveameti peadirektorile, SKA peadirektorile, TEHIKu direktorile, RIKi direktorile ja SMITi peadirektorile:

- Täiendada valitsemisalade või asutuste infoturbe kordasid nii, et reguleeritud oleks ka päringute põhjendatuse (teadmisvajaduse) kontroll, sh selle toimumise kord, sagedus ja ulatus, ning hakata vastavaid kontrolle läbi viima.

- Täiendada valitsemisalade või asutuste infoturbe kordasid nii, et reguleeritud oleks ka logide jooksva analüüsimise kohustus, sh analüüsi läbiviimise kord, selleks kasutatavad vahendid, selle eest vastutajad, ning hakata vastavalt sellele logisid analüüsima.

Justiitsministeeriumi kantsleri vastus: Justiitsministeerium alustas 2022. aastal Justiitsministeeriumile ja haldusalale kehtiva Justiits-ministeeriumi infotehnoloogia valdkonna planeerimise, juhtimise ja haldamise korra ning Justiitsministeeriumi infovaradega teostatud toimingute logimise korralduse uuendamisega. Plaanime selle protsessi viia lõpule 2023. a jooksul. Võtame Teie esitatud soovitusi muudatuste tegemisel kindlasti arvesse ja analüüsime, kuidas neid rakendada.

Politsei- ja Piirivalveameti peadirektori vastus: Andmete väärkasutuse avastamiseks on andmekogude logisid analüüsitud süsteemselt ja regulaarselt järelevalve käigus. Seatud on prioriteedid ning menetletud intsidendid näitavad, et järelevalve toimib. SMIT on kasutusele võtmas sündmuste analüüsimise vahendit SIEM. Intsidentide korral nende põhjuste väljaselgitamiseks kaasatakse infoturbest andmekaitsespetsialist. Vajadusel täpsustame ning täiendame E-ITSi raames koostatavat vajalikku dokumentatsiooni.

Täiendavalt lisame: PPAs on kinnitatud 25.08.2021 peadirektori käskkirjaga nr 1.1-1/83 „Politsei- ja Piirivalveameti infoturbepoliitika ning IKT varade turbe ja halduse kord“, mille lisa 1 on „Infosüsteemi pidamise kord“. Nimetatud lisas kirjeldatakse eraldi punktina juurde-pääsupiirang andmetele ning infosüsteemide juurdepääsuõigused ehk millised on piirangud ja kellele need kehtivad. Lisaks lähtume info-süsteemide turvameetmete süsteemi määrusest, milles konfidentsiaalsuse alusel määratakse turvaosaklass(id). IKT-korra lisa 2 on juurdepääsu-õiguste andmise ja sulgemise kord. Kirjeldatud on kogu protsess alates taotlemisest kuni sulgemiseni. IKT korraga on kohustuslik tutvuda kõikidel uutel töötajatel. Andmekogude juurdepääsu haldamiseks on olemas eraldi infosüsteem.

SKA peadirektori vastus: Täiendame SKA infoturbe põhimõtteid ja loome vajaliku protsessi päringute põhjendatuse kontrolli teostamiseks hiljemalt 2023. aasta II kvartali lõpuks.

RIK direktori vastus: RIK saab teadmisvajadust kontrollida enda asutuse töötajate toimingute keskselt, kuid RIKil puudub õigus teostada järelevalvet teiste asutuste üle. Võtame kindlasti auditis kajastatud murekohad arvesse ja analüüsime 2023. a jooksul, kuidas päringute põhjendatuse kontrolli RIKi töötajate osas tõhustada ja milliseid kordasid, juhendeid looma/täiendama peab.

SMITi peadirektori vastus: ABISe päringuid üle X-tee saavad teha vastavad andmekogud, kes on ABISega liidestunud ning kellel on selleks kindel vajadus. ABISega liidestujad on ABIS põhimäärusega määratletud. Vaata lisaks vastust punktile nr 18.

87. **Riigikontrolli soovitus Politsei- ja Piirivalveameti peadirektorile:** viia ABISes läbi ISKE (või E-ITS) rakendamise audit.

Politsei- ja Piirivalveameti peadirektori vastus: ABIS on arendusjärgus ning ei olnud 2022. a kevadel läbi viidud ISKE-auditi fookuses. PPA on üle minemas uuele E-ITSi standardile ning SMIT ISO standardile. Edaspidi on ABIS osa SMITi ISO auditist.

SMITi peadirektori kommentaar: SMITis on ISO27001 juurutamisel. Lisainfo: E-ITSi auditeerimise juhendis (https://eits.ria.ee/et/versioon/2021/juhendid/auditeerimisjuhend/) on punktis 4.3 välja toodud, et E-ITSi auditi kohustus ei rakendu organisatsioonidele, kelle vastavust standardile ISO/IEC 27001 on nõutud kaitseala osas kinnitatud ISO/IEC 27006 kohaselt akrediteeritud sertifitseerija väljastatud ning ajaliselt kehtiva sertifikaadiga.

SIEM ja TrueTrail on juurutamisel. Loodetavasti on 2023. a jaanuari lõpuks vastav ISO27001 sertifikaat olemas.

88. **Riigikontrolli soovitus ettevõtlus- ja infotehnoloogiaministrile:** muuta infoturberaamistiku (ISKE ja hiljem E-ITS) rakendamise auditeerimise reegleid ja juhendeid nii, et vähemalt keskmise tervikluse ja konfidentsiaalsuse turvaosaklassi korral auditeeritakse ka juurdepääsuõigusi.

Ettevõtlus- ja infotehnoloogiaministri vastus: E-ITSis on olemas protsessimoodulite all moodul „ORP. Organisatsioon ja personal“, mille alammooduliks on „ORP.4: Identiteedi- ja õiguste haldus“. Tolle alam-mooduli meetmetena on põhimeetmete hulgas mh meetmed „ORP.4.M1. Kasutajakontode halduse eeskiri“, „ORP.4.M2. Õiguste andmine, muutmine ja tühistamine“ ja „ORP.4.M3. Kasutajate õiguste dokumenteerimine“, mis on seotud mh ka andmekogudele juurdepääsuõiguste andmise ja kontrolliga organisatsioonis endas. Viidatud meetmed on põhimeetmed ehk need meetmed on igal juhul kohustuslikud ära rakendada n-ö baasnõuetena.

Vastavalt 16.12.2022 kehtestatud E-ITSi auditeerimisjuhendile kontrollib audiitor, kuidas organisatsioon on talle kohaldatavaid põhimeetmeid rakendanud, sh kui neid on mingil põhjusel osaliselt rakendatud, siis ka seda aspekti kontrollitakse.

/allkirjastatud digitaalselt/

Ines Metsalu-Nurminen
auditiosakonna peakontrolör

Riigikontrolli soovitused ja auditeeritute vastused

Riigikontroll andis auditi põhjal SKA peadirektorile, RIKi direktorile, TEHIKu direktorile, SMITi peadirektorile, Politsei- ja Piirivalveameti peadirektorile, justiitsministrile ning ettevõtlus- ja infotehnoloogiaministrile mitmeid soovitusi. SKA peadirektor ja RIKi direktor saatsid oma vastuse Riigikontrolli soovitustele 23.12.2022, TEHIKu direktor ja SMITi peadirektor 27.12.2022, Politsei- ja Piirivalveameti peadirektor 28.12.2022, Justiitsministeeriumi kantsler 05.01.2023 ning ettevõtlus- ja infotehnoloogiaminister 23.01.2023.

Üldised kommentaarid auditiaruande kohta

SKA peadirektori vastus: Täname auditi „Andmekogude juurdepääsuhaldus“ kontrolliaruande eelnõus kirjeldatud tähelepanekute ja soovituste eest. Sotsiaalkindlustusametit puudutavate soovituste ja tähelepanekute kohta esitame alljärgnevad seisukohad.

RIKi direktori vastus: Esmalt peame vajalikuks kajastada tähelepanekut, mis RIKile silma jäi auditi tulemuste analüüsis. Nimelt avaliku teabe seaduse § 434 alusel on andmekogu vastutav töötleja (haldaja) riigi- või kohaliku omavalitsuse asutus, muu avalik-õiguslik juriidiline isik või avalikke ülesandeid täitev eraõiguslik isik, kes korraldab andmekogu kasutusele võtmist, teenuste ja andmete haldamist. Andmekogu vastutav töötleja vastutab andmekogu haldamise seaduslikkuse ja andmekogu arendamise eest. Avaliku teabe seaduse § 434 lg 3 kohaselt on volitatud töötleja kohustatud täitma vastutava töötleja (haldaja) juhiseid andmete töötlemisel ja andmekogu majutamisel ning tagama andmekogu turvalisuse. Samas on haldajana auditis silmas peetud osas kohtades volitatud töötlejaid (vt näiteks auditi punktis 77 sedastatut: Turvateabe ja sündmuste halduse lahendused ei olnud RIKis (KARRi haldaja) ja SMITis (VMP ja ABISe haldaja) kasutusel. Palume seega haldaja mõiste sisustamist auditi tulemustes täpsustada.

Riigikontrolli kommentaar: Riigikontroll korrigeeris aruandes andmekogu vastutava töötleja ehk haldaja mõiste kasutamist.

TEHIKu direktori vastus: Täname kontrollaruandes väljatoodud tähelepanekute ja soovituste eest. TEHIK esitab täiendavalt Sotsiaalkindlustusameti (SKA) esitatud seisukohtadele oma seisukohad. TEHIK on andmekogude SKAIS1 ja STAR volitatud töötleja ning saab antud andmekogude infoturbe, sh logimiste analüüsimisega seonduvatel teemadel olla tehniliseks nõuandjaks.

Punkti 73 osas saame anda teada, et SKAISi ISKE-audit on töös ning järeldused esitatakse 2023 jaanuaris. ISKE-audit sisaldab identiteedi- ja volituste halduse mooduli B 1.15 auditeerimist.

Üldise kommentaarina soovime välja tuua, et TEHIKus on kinnitatud direktori käskkirjaga „Infosüsteemide logimiskontseptsioon“, mis annab suunised logi halduseks TEHIKu hallatavates infosüsteemides eesmärgiga võimaldada tagantjärele kindlaks teha, millal, kes ja milliseid andmeid kasutas. Lähtudes kontrollaruandes toodud ettepanekutest, vaatame üle „Infosüsteemide logimiskontseptsioonis“ toodud nõuded.

Politsei- ja Piirivalveameti peadirektori vastus: Täname auditi „Andmekogude juurdepääsuhaldus“ aruandes toodud tähelepanekute, seisukohtade ning Politsei- ja Piirivalveametile antud soovituste eest. Arvestame auditis kajastatuga oma edaspidises töös.

Justiitsministeeriumi kantsleri vastus: Üldise märkusena soovime juhtida tähelepanu seoses eelnõu punktis 4 alapunktis 4 tooduga, et e-toimiku väärteomenetluse liidest (VMP) arendab, hooldab ja majutab Siseministeeriumi infotehnoloogia- ja arenduskeskus.

Riigikontrolli soovitused	Auditeeritute vastused
Andmekogude juurdepääsuhalduse korraldus **18. Riigikontrolli soovitus TEHIKu direktorile, RIKi direktorile ja SMITi peadirektorile:** täiendada valitsemisalade infoturbe dokumentatsiooni või andmekogusid reguleerivaid kordasid nõudega analüüsida süstemaatiliselt ja regulaarselt logisid ning kontrollida päringute põhjendatust. **p-d 8–17**	**TEHIKu direktori vastus:** TEHIK võtab soovituse teadmiseks ning teeb andmekogude vastutava töötlejaga koostööd tehniliste lahenduste täpsustamisel ning vaatab üle ja vajadusel täiendab infoturbe dokumentatsiooni. Dokumentatsiooni uuendamine on kavandatud lõpetada 2023. aasta kolmandas kvartalis. **RIKi direktori vastus:** Justiitsministeeriumil on plaanis 2023. a üle vaadata logipoliitika, mille raames vaadatakse üle ka käesolevas auditis kajastatud murekohad, sh räägime kindlasti läbi SIEMi kasutusele võtmise ning vahekontrollide teostamise vajaduse ja tellimise protsessi. **SMITi peadirektori vastus:** Tegeleme hetkel SIEMi juurutamisega ja selle raames kordade uuendamisega. Siseministeeriumi valitsemisala infosüsteemide turvatestimise, turvanõrkuste haldamise ning nende logimise nõuete korras on logianalüüs ja pidev seire kaetud (punkt 5.1.9). SMIT ei saa auditeeritud andmekogudes teadmisvajaduse ehk päringute põhjendatuse kontrolli teha. SMIT ei ole andmete omanik ja ei kontrolli vastavat äriprotsessi. Andmete omanik saab põhjendada, kas saame või mitte ja tellida selle funktsionaalsuse (näiteks PPA). **Riigikontrolli kommentaar:** Nõustume asjaoluga, et andmete omanik saab päringute põhjendatuse kontrolli teha ja SMIT saab eelkõige luua vastava funktsionaalsuse.

Riigikontrolli soovitused	Auditeeritute vastused
Õiguste andmine **32. Riigikontrolli soovitused SKA peadirektorile ja TEHIKu direktorile:** ▪ Muuta juurdepääsuõiguste andmine ja äravõtmine SKAISi ja STARi andmekogudes tõhusamaks ja täpsemaks, et kasutajatel oleks neile juurdepääs ainult selleks volitatud ajal. ▪ Seada edaspidi ajutistele ja erakorralistele kontodele ajalise piiranguga kasutajaõigused, nii et need antakse ja võetakse ära kindlatel kuupäevadel. ▪ Muuta õiguste andmise protsessi nii, et vastutav töötleja kas annaks ainult ise privilegeeritud kasutajaõigusi volitatud kasutajatele või omaks nende õiguste andmise üle suuremat kontrolli. **p-d 20–31**	**SKA peadirektori vastus:** Soovituses välja toodud funktsionaalsuste puudujäägid esinevad meie infosüsteemide vanades rakendustes, mida edasi ei arendata. Arendame nõuetekohased funktsionaalsused oma uues infosüsteemis. Privilegeeritud kasutajaõiguste andmise kitsendamiseks STARis nii, et privilegeeritud kasutajaid saaks luua ja nendele õiguseid anda ainult SKA töötajad, on arenduste prioriteetsete tööde järjekorras. 2023. aasta lõpuks saame anda täpsema info arendusprotsessi seisu kohta. Ajutiste ja erakorraliste kontode õigeaegseks andmiseks ja sulgemiseks arenduste valmimisteni jälgib STARi kasutatugi õigustatuse perioodi ja vastavalt tööprotsessile avab ja sulgeb kontod õigeaegselt käsitsi.
Juurdepääsu tagamine **47. Riigikontrolli soovitus SKA peadirektorile ja TEHIKu direktorile:** tagada, et STARi andmekogu kasutajad kohalikes omavalitsustes saaksid juurdepääsu vaid samas omavalitsuses elukoha aadressi registreerinud inimeste ja nendega seotud menetluste andmetele. Kui aga vajatakse juurdepääsu teiste valdade/linnade elanikega seotud menetlustele, siis määrata kindlaks kontrolliprotseduur täiendava juurdepääsu valideerimiseks. **p-d 34–46**	**SKA peadirektori vastus:** SKA on seisukohal, et tegemist ei ole liiasusega, kuna nimetatud laiem lähenemise vajadus on seotud KOVide töö spetsiifikaga. Abivajaduse hindamine on aegkriitiline protsess ja abivajaduse hindamiseks ja sobiva sekkumisviisi leidmiseks vajab KOV tervikpilti, mis võib olla KOVide-ülene, kuna inimene võib olla registreeritud teise KOVi elanikuks, mitte KOVi, kus ta reaalselt elab. Samuti on lastekaitse juhtumite lahendamisel oluline mitme KOVi samaaegne koostöö, kuna lapsevanemad võivad olla erinevate KOVide elanikud. Probleemi lahendamiseks ei saa oodata teise KOVi või SKA nõusolekut, kuna sekkumise kiirusest võib sõltuda ka abivajaja elu ja tervis. **Riigikontrolli kommentaar:** Kui SKA hinnangul ei ole võimalik korraldada juurdepääsutaotluse menetlust piisavalt kiiresti ja selliselt nagu abivajaduse hindamise protsess seda nõuab, siis ei saa sellist kontrolliprotseduuri rakendada. Teisalt tuleb sel juhul andmete väärkasutuse ärahoidmiseks ja avastamiseks seda enam rakendada muid meetmeid (vt punktid 64 ja 86).
Logide terviklus ja analüüsimine **64. Riigikontrolli soovitused TEHIKu direktorile, RIKi direktorile ja SMITi peadirektorile:** ▪ Täiendada infoturbe dokumentatsiooni ja praktikaid logide süstemaatilise ja regulaarse analüüsimise sisseviimisega IT-sisekontrollimeetmete hulka. Selleks on soovitatav kasutusele võtta turvateabe ja sündmuste analüüsimise vahend SIEM. ▪ Hinnata logide volitamata muutmisega seonduvaid riske ja sellest tulenevalt rakendada logide tervikluse tagamiseks ajatembeldamise ja/või krüptoaheldamise lahendusi. **p-d 53–63**	**TEHIKu direktori vastus:** ▪ TEHIK võtab soovituse teadmiseks ning teeb andmekogude vastutava töötlejaga koostööd tehniliste lahenduste täpsustamisel ning vaatab üle ja vajadusel täiendab infoturbe dokumentatsiooni. Dokumentatsiooni uuendamine on kavandatud lõpetada 2023. aasta kolmandas kvartalis. ▪ SIEM on TEHIKus kasutusel ning SKAISi ja STARi andmete töötlemiseks kasutatakse tööjaamadel ja võrguühendustel automatiseeritud järelevalvet, et tuvastada tavapärasest erinevaid protsesse, kasutajaid, võrguühendusi või sisselogimisi, ning korraldatud on igapäevane tulemuste analüüs potentsiaalsete turvarikkumiste tuvastamiseks. Rakendatud on kõrvalekaldeid automaatselt tuvastavad tööriistad. **RIK direktori vastus:** ▪ Justiitsministeeriumil on plaanis 2023. a üle vaadata logipoliitika, mille raames vaadatakse üle ka käesolevas auditis kajastatud murekohad, sh räägime kindlasti läbi SIEMi kasutusele võtmise ning vahekontrollide teostamise vajaduse ja tellimise protsessi. ▪ Plaanime teostada EITSe rakendamise raames riskianalüüsid 2023.–2024. a. Nende riskianalüüside raames vaadatakse üle süsteemi logide ajatembeldamise ja/või krüptoaheldamise vajadus. **SMITi peadirektori vastus:** Tegeleme hetkel SIEMi juurutamisega ja selle raames kordade uuendamisega ning automaatse logide analüüsiga. Tegeleme hetkel ka TrueTrail-i juurutamisega. SMITis on käimas vSOC-projekt, mille raames võetakse kasutusele SIEM. Logide protsessiga on tagatud logide terviklus.

Autentimine ja autoriseerimine **65. Riigikontrolli soovitus SKA peadirektorile ja TEHIK-u direktorile:** muuta SKAIS1 andmekogus autentimine turvalisemaks, s.t kasutada kaheastmelist lahendust. **p-d 50–52**	**SKA peadirektori vastus:** Nimetatud puudujääk esineb meie infosüsteemi vanades rakendustes, mida edasi ei arendata. Meie uues infosüsteemis on nõuetekohane kaheastmeline autentimise lahendus rakendatud, praegu veel vanades rakendustes kasutatavad funktsionaalsused viiakse uude infosüsteemi üle. Tegeleme teenuste üleviimisega aktiivselt, aga tähtaega ei saa hetkel prognoosida, kuna see sõltub, kui palju tuleb kõrgema prioriteediga poliitilisi arendussoove. Seniks on SKAIS1 turvalisus tagatud alljärgnevate meetmetega: ▪ SKAIS1 saab kasutada ainult kasutaja, kellele on loodud meie domeenis kasutajakonto ja kes omab TEHIKu väljastatud ja TEHIKu kontrolli all olevat arvutit; ▪ pensionide ja hüvitistega seotud rakendus ei ole veebipõhine, vaid kasutaja arvutisse on installeeritud SKAIS1 (n-ö paks klient); ▪ TEHIK teeb konkreetse arvuti registrites kliendipõhiselt muudatusi, ilma milleta ei ole kasutajal võimalik SKAIS1-te sisse logida; ▪ rakendatud on minimaalselt 12 tähemärgise salasõna kohustus autentimisel; ▪ välisvõrgust saab kasutaja SKAIS1 sisse logida ainult TEHIKu väljastatud arvutiga üksnes üle VPNi, mis on kaheastmelise autentimisega.
Turvateabe ja -sündmuste ning teadmisvajaduse kontroll **86. Riigikontrolli soovitused justiitsministrile, Politsei- ja Piirivalveameti peadirektorile, SKA peadirektorile, TEHIKu direktorile, RIKi direktorile ja SMITi peadirektorile:** ▪ Täiendada valitsemisalade või asutuste infoturbe kordasid nii, et reguleeritud oleks ka päringute põhjendatuse (teadmisvajaduse) kontroll, sh selle toimumise kord, sagedus ja ulatus, ning hakata vastavaid kontrolle läbi viima. ▪ Täiendada valitsemisalade või asutuste infoturbe kordasid nii, et reguleeritud oleks ka logide jooksva analüüsimise kohustus, sh analüüsi läbiviimise kord, selleks kasutatavad vahendid, selle eest vastutajad, ning hakata vastavalt sellele logisid analüüsima. **p-d 75–85**	**Justiitsministeeriumi kantsleri vastus:** Justiitsministeerium alustas 2022. aastal Justiitsministeeriumile ja haldusalale kehtiva Justiitsministeeriumi infotehnoloogia valdkonna planeerimise, juhtimise ja haldamise korra ning Justiitsministeeriumi infovaradega teostatud toimingute logimise korralduse uuendamisega. Plaanime selle protsessi viia lõpule 2023. a jooksul. Võtame Teie esitatud soovitusi muudatuste tegemisel kindlasti arvesse ja analüüsime, kuidas neid rakendada. **Politsei- ja Piirivalveameti peadirektori vastus:** Andmete väärkasutuse avastamiseks on andmekogude logisid analüüsitud süsteemselt ja regulaarselt järelevalve käigus. Seatud on prioriteedid ning menetletud intsidendid näitavad, et järelevalve toimib. SMIT on kasutusele võtmas sündmuste analüüsimise vahendit SIEM. Intsidentide korral nende põhjuste väljaselgitamiseks kaasatakse infoturbest andmekaitsespetsialist. Vajadusel täpsustame ning täiendame E-ITSi raames koostatavat vajalikku dokumentatsiooni. Täiendavalt lisame, et PPAs on kinnitatud 25.08.2021 peadirektori käskkirjaga nr 1.1-1/83 „Politsei- ja Piirivalveameti infoturbepoliitika ning IKT varade turbe ja halduse kord“, mille lisa 1 on „Infosüsteemi pidamise kord“. Nimetatud lisas kirjeldatakse eraldi punktina juurdepääsupiirang andmetele ning infosüsteemide juurdepääsuõigused ehk millised on piirangud ja kellele need kehtivad. Lisaks lähtume infosüsteemide turvameetmete süsteemi määrusest, milles konfidentsiaalsuse alusel määratakse turvaosaklass(id). IKT-korra lisa 2 on juurdepääsuõiguste andmise ja sulgemise kord. Kirjeldatud on kogu protsess alates taotlemisest kuni sulgemiseni. IKT-korraga on kohustuslik tutvuda kõikidel uutel töötajatel. Andmekogude juurdepääsu haldamiseks on olemas eraldi infosüsteem. **SKA peadirektori vastus:** Täiendame SKA infoturbe põhimõtteid ja loome vajaliku protsessi päringute põhjendatuse kontrolli teostamiseks hiljemalt 2023. aasta II kvartali lõpuks. **RIK direktori vastus:** RIK saab teadmisvajadust kontrollida enda asutuse töötajate toimingute keskselt, kuid RIKil puudub õigus teostada järelevalvet teiste asutuste üle. Võtame kindlasti auditis kajastatud murekohad arvesse ja analüüsime 2023. a jooksul, kuidas päringute põhjendatuse kontrolli RIKi töötajate osas tõhustada ja milliseid kordasid, juhendeid looma/täiendama peab. **SMITi peadirektori vastus:** ABISe päringuid üle X-tee saavad teha vastavad andmekogud, kes on ABISega liidestunud ning kellel on selleks kindel vajadus. ABISega liidestujad on ABISe põhimäärusega määratletud. Vaata lisaks vastust punktile nr 18.

Infoturberaamistiku rakendamise audit **87. Riigikontrolli soovitus Politsei- ja Piirivalveameti peadirektorile:** viia ABISes läbi ISKE (või E-ITS) rakendamise audit. **p-d 69–74**	**Politsei- ja Piirivalveameti peadirektori vastus:** ABIS on arendusjärgus ning ei olnud 2022. a kevadel läbi viidud ISKE-auditi fookuses. PPA on üle minemas uuele E-ITSi standardile ning SMIT ISO standardile. Edaspidi on ABIS osa SMITi ISO auditist. **SMITi peadirektori kommentaar:** SMITis on ISO27001 juurutamisel. Lisainfo: E-ITS auditeerimise juhendis (https://eits.ria.ee/et/versioon/2021/juhendid/auditeerimisjuhend/) on punktis 4.3. välja toodud, et E-ITSi auditi kohustus ei rakendu organisatsioonidele, kelle vastavust standardile ISO/IEC 27001 on nõutud kaitseala osas kinnitatud ISO/IEC 27006 kohaselt akrediteeritud sertifitseerija väljastatud ning ajaliselt kehtiva sertifikaadiga. SIEM ja TrueTrail on juurutamisel. Loodetavasti on 2023. a jaanuari lõpuks vastav ISO27001 sertifikaat olemas.
Infoturberaamistiku rakendamise auditi juhend **88. Riigikontrolli soovitus ettevõtlus- ja infotehnoloogiaministrile:** muuta infoturberaamistiku (ISKE ja hiljem E-ITS) rakendamise auditeerimise reegleid ja juhendeid nii, et vähemalt keskmise tervikluse ja konfidentsiaalsuse turvaosaklassi korral auditeeritakse ka juurdepääsuõigusi. **p-d 69–74**	**Ettevõtlus- ja infotehnoloogiaministri vastus:** Alates 01.01.2023. a ei ole edaspidi kolmeastmeline etalonturbe süsteem ehk ISKE kehtiv, kuna selle aluseks olev volitusnorm avaliku teabe seaduses kaotati küberturvalisuse seaduse ja teiste seaduste muutmise seadusega 531 SE ära. Seetõttu ei ole võimalik edaspidi teha täiendusi või muudatusi ISKE dokumentatsioonis, sh auditeerimisjuhendis. ISKE on nüüdseks asendatud Eesti infoturbestandardiga ehk E-ITSiga. E-ITS on mõeldud rakendamiseks küberturvalisuse seaduse tähenduses olevate teenuse osutajate võrgu- ja infosüsteemidele, sh ka avaliku teabe seaduse tähenduses andmekogudele. E-ITS on seotud küberturvalisuse seaduse alusel antud Vabariigi Valitsuse 09.12.2022. a määrusega nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ ning ettevõtlus- ja infotehnoloogia-ministri 16.12.2022. a määrusega nr 101 „Eesti infoturbestandard“. E-ITS on leitav ka E-ITSi portaalist. E-ITSis on olemas protsessimoodulite all moodul „ORP. Organisatsioon ja personal“, mille alammooduliks on „ORP.4: Identiteedi- ja õiguste haldus“. Tolle alammooduli meetmetena on põhimeetmete hulgas mh meetmed „ORP.4.M1. Kasutajakontode halduse eeskiri“, „ORP.4.M2. Õiguste andmine, muutmine ja tühistamine“ ja „ORP.4.M3. Kasutajate õiguste dokumenteerimine“, mis on seotud mh ka andmekogudele juurdepääsuõiguste andmise ja kontrolliga organisatsioonis endas. Viidatud meetmed on põhimeetmed ehk need meetmed on igal juhul kohustuslikud ära rakendada n-ö baasnõuetena. Välise kontrolliva osapoole ehk audiitori tegevust reguleerib E-ITSi auditeerimis-juhend, mis annab juhiseid E-ITSi-põhise sõltumatu auditi läbiviimiseks. E-ITSi auditi eesmärk on hinnata, kas auditeeritava organisatsiooni infoturbe halduse süsteem ning selle raames rakendatud meetmed on piisavad organisatsiooni äriprotsesside kaitseks ja organisatsiooni eesmärkide täitmiseks (auditeerimis-juhendi p 3.1). Auditeerimisjuhendi peatükk 5 sisustab E-ITSi auditi eeldused ja selle alapunktis 5.6 on märgitud järgmist: *E-ITS rakendamise käigus on organisatsioon koostanud infoturbe meetmete rakendusplaani. Infoturbe meetmete rakendusplaan sisaldab:* *5.6.1. rakendamisele kuuluvaid E-ITS turvameetmeid koos meetme koodi, nimetuse ja meetme teostatuse määraga;* *5.6.2. rakendamisele kuuluvaid etalonturbe väliseid turvameetmeid koos meetme teostatuse määraga (vajadusel);* *5.6.3. meetme rakendamise eest vastutajaid;* *5.6.4. meetme rakendamisega seotud tähtaegu;* *5.6.5. meetme osalise rakendamise puhul täpsustavaid selgitusi, mis osas on meede täitmata;* *5.6.6. meetme mitterakendamise puhul juhtkonna aktsepteeringut meetmete mitterakendamisest tulenevatele jääkriskidele.* E-ITSi põhiauditi olemust sisustab auditeerimisjuhendi peatükk 10, mille punktid 10.2 ja 10.2.1. on järgmised: *10.2. Audiitor valib kontrollitavaid sihtobjekte ja infoturbe meetmeid järgnevalt:* *10.2.1. põhimeetmete rakendamist kontrollib audiitor täies ulatuses …* Seega kontrollib audiitor, kuidas organisatsioon on talle kohaldatavaid põhimeetmeid rakendanud, sh kui neid on mingil põhjusel osaliselt rakendatud, siis ka seda aspekti kontrollitakse. Sellega on Riigikontrolli esitatud soovitus E-ITSi dokumentatsiooni osas juba täidetud. Kui Riigikontrollile tundub, et E-ITSi dokumentatsioonis on vaja teha täiendusi, siis palume need edastada Riigi Infosüsteemi Ameti e-maili aadressile standard@ria.ee. Neid muudatusi viiakse dokumentidesse üks kord aastas, iga aasta sügisel.

Auditi iseloomustus

Auditi eesmärk

Auditi eesmärk oli hinnata, kas juurdepääsuhaldus on korraldatud kehtestatud nõuete ja parima praktika alusel; kas auditeeritavates andmekogudes rakendatakse meetmeid, mis tagavad volitatud isikutele juurdepääsu andmekogule ja välistavad volitamata isikute juurdepääsu; ning kas rakendatavad meetmed toimivad.

Hinnangu andmise kriteeriumid

Auditi peamised kriteeriumid olid järgmised:

- Asutustes on kehtestatud juurdepääsukorrad ja need vastavad infoturbe raamistikule ISKE.
- Juurdepääsude avamine, kasutamine, muutmine, sulgemine ja kontroll toimub turvaliselt (riigis kehtiva raamistiku alusel) ning määratud korra kohaselt.
- Andmekogu kasutamise ja administreerimisega, sh juurdepääsuhaldusega seonduvaid tegevusi logitakse piisavalt, logide terviklus on tagatud ja logisid analüüsitakse.
- Andmepäringute sisulise põhjendatuse kontrolle tehakse ning kontrolli võimalust pakutakse ka andmesubjektidele endile.

Auditi ulatus ja käsitlusviis

Ekspertvalimi tulemusena auditeeriti järgmisi andmekogusid:

- sotsiaalkaitse infosüsteem (SKAIS),
- sotsiaalteenuste ja -toetuste andmeregister (STAR),
- karistusregister (KARR),
- e-toimiku väärteomenetluse liides (VMP),
- automaatse biomeetrilise isikutuvastuse süsteemi andmekogu (ABIS).

Põhiline kriteerium, mille alusel valiti auditeerimiseks andmekogud, oli nende ISKE konfidentsiaalsuse turvaosaklass S2 või S3 (S2 – salajane info: info kasutamine lubatud ainult teatud kindlatele kasutajagruppidele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral; S3 – ülisalajane info: info kasutamine lubatud ainult teatud kindlatele kasutajatele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral).

Auditeeritud asutused olid Sotsiaalkindlustusamet, Tervise ja Heaolu Infosüsteemide Keskus, Sotsiaalministeerium, Justiitsministeerium, Registrite ja Infosüsteemide Keskus, Politsei- ja Piirivalveamet, Siseministeeriumi infotehnoloogia- ja arenduskeskus, Siseministeerium, Türi Vallavalitsus, Haabersti Linnaosa Valitsus, Viljandi Linnavalitsus, Tõrva Vallavalitsus, Kuusalu Vallavalitsus, Räpina Vallavalitsus, Kiili Vallavalitsus, Kihnu Vallavalitsus, Antsla Vallavalitsus, Lääne-Harju Vallavalitsus, Tartu Linnavalitsus, Keskkonnaamet, Päästeamet, Maksu- ja Tolliamet, Tarbijakaitse ja Tehnilise Järelevalve Amet, Rahapesu Andmebüroo, Tallinna Haridusamet, Eesti Kohtuekspertiisi Instituut. Kohalike omavalitsuste valimise eelduseks oli, et KOV kasutab erinevaid auditeeritud andmekogusid, ülejäänud asutused valiti juhuvalimiga.

Auditi käigus ei tehtud andmekogude läbistustestimisi ja seetõttu ei anta hinnangut selle kohta, kas küberrünnaku tulemusel on võimalik saavutada auditeeritud andmekogudesse volitamata juurdepääs.

Auditeeritud periood: 1. aprill 2021 – 31. märts 2022.

Auditi lõpetamise aeg: auditi toimingud lõpetati septembris 2022.

Auditi meeskond: auditijuht Toomas Viira, vanemaudiitor Alo Lääne ja audiitor Jevgeni Lazartšuk**.**

Kontaktandmed

Auditi kohta saab lisainfot Riigikontrolli kommunikatsiooniüksusest
tel +372 640 0704 või +372 640 0777, e-post riigikontroll@riigikontroll.ee

Auditiaruande elektrooniline koopia (pdf) on saadaval koduleheküljel www.riigikontroll.ee.

Auditiaruande kokkuvõte on saadaval ka inglise keeles.

Auditiaruande number Riigikontrolli asjaajamissüsteemis on 80087.

Riigikontrolli postiaadress on:

Kiriku 2/4
15013 TALLINN
Tel +372 640 0700
riigikontroll@riigikontroll.ee

Riigikontrolli varasemaid auditeid juurdepääsuhaldusega seotud valdkonnas

14.05.2018 – **Eesti riigi kriitiliste andmekogude turvalisuse ja säilitamise tagamine**

Kõik aruanded on kättesaadavad Riigikontrolli koduleheküljelt www.riigikontroll.ee