Serveri- ja kontoriruumide turvalisus

Kas riigi IT-taristuga seotud ruumide füüsiline turvalisus on tagatud?

Riigikontrolli aruanne Riigikogule
Tallinn, 30. oktoober 2023

Serveri- ja kontoriruumide turvalisus

Kas riigi IT-taristuga seotud ruumide füüsiline turvalisus on tagatud?

Mida me auditi tulemusel leidsime ja järeldasime?

Riigi IT-maja – ministeeriumi hallatav asutus, mis tegeleb valitsemisala IKT haldamisega ning infosüsteemide arendamise ja ülalpidamisega.

Auditeeritud kümne riigiasutuse ja ühe avalik-õigusliku juriidilise isiku serveriruumides ja serveriruumide tööks vajalikes tehnilistes ruumides on vajalikud turvameetmed üldjuhul rakendatud. IT-majade kontoriruumides rakendatakse esmaseid vajalikke turvameetmeid füüsilise turvalisuse tagamiseks ja volitamata ligipääsu riski ruumidesse on vähendatud aktsepteeritavale tasemele.

Positiivsele üldhinnangule vaatamata leidis Riigikontroll mõningaid puudusi serveri- ja kontoriruumide füüsilise turvalisuse tagamisel.

Auditi käigus leidis Riigikontroll mitmeid probleeme serveriruumides vajalike tingimuste tagamisel, s.t jahutus- ja ventilatsiooniseadmete, aga samuti tule-, suitsu- ja veelekkeandurite töö tagamisel. Mõnes auditis vaadeldud serveriruumis oli ebatõhusalt korraldatud serveriruumi jahutus. Lisaks olid kahe auditeeritud asutuse vanemates serveriruumides puhvertoite seadmed ja jahutusseadmed serveriruumides sees, see aga suurendab seadmete ülekuumenemise või põlengu tekkimise riski. Osas serveriruumides ei olnud kasutusel täppiskliimaseadmeid. Samuti hoiustati mitme auditeeritud asutuse serveriruumides ja serveriruumi abiruumis tuleohtlikke materjale, näiteks pappkaste.

Riigikontroll tegi tähelepanekuid serveriruumide ja kontoriruumide valvestamise ning valvesüsteemide kaitsmise kohta. Ühes auditi valimis olnud asutuses ei valvestatud serveriruumi. Teise auditeeritud asutuse videovalvesüsteem ei olnud piisavalt kaitstud, videovalve kesksеadmetele pääses ligi liiga suur hulk kasutajaid. Mitmel asutusel ei olnud kordades kindlaks määratud, kui kaua minimaalselt tuleb säilitada videovalve salvestisi ning ühel asutusel juurdepääsu ja valvestamise logisid. Ühe auditeeritud asutuse büroohoones valvestati töövälisel ajal vaid sissepääsukorruse kontoriruumid.

Serveriruumide hoonete välise turvaperimeetri kaitsel esines probleeme serveriruumide tööks vajalike rajatiste kaitsmisel. Näiteks ei olnud ühe auditeeritud asutuse hoone väline perimeeter kaetud vajalike anduritega. Samuti esines puudusi ühe teenindava alajaama kaitsmisel.

Juurdepääsuhalduse korraldamisel leidsime mõningaid probleeme nii organisatsiooniliste kui ka tehniliste meetmete rakendamisel. Näiteks pääses ühe auditeeritud asutuse serveriruumi ühefaktorilise autentimisega, s.t ainult uksekaarti kasutades. Teisel asutusel oli aga juurdepääsusüsteemi kesksеadmele võimalik ligi pääseda administraatori õigustes valvelauaarvutist.

Auditi tulemusena tegi Riigikontroll iga auditeeritud asutuse turvalisuse kohta detailsemad tähelepanekud ja andis soovitusi, kuidas olukorda parandada.

Auditeeritute vastused: Auditeeritud asutused nõustusid enamiku Riigikontrolli tähelepanekute ja soovitustega ning esitasid oma plaanid puuduste likvideerimiseks ja vajalike turvameetmete rakendamiseks. Üksikute tähelepanekute osas otsustasid auditeeritud asutused riske aktsepteerida ja/või rakendada riski vähendamiseks muid lisaturvameetmeid.

Sisukord

Valdkonna ülevaade 4

Hoonete turvalisus 5

Asukohast tulenevate riskide hindamine 5
Välise turvaperimeetri kaitse 6

Serveriruumide turvalisus 6

Serveriruumi ebasobivast mikrokliimast tulenevad riskid 6
Juurdepääsude haldamine 8
Serveriruumide valve 9
Puhver- ja varutoite probleemid 10

Kontoriruumide turvalisus 11

Kontoriruumide turvalisuse korraldus 11
Kontoriruumide valve 11

Riigikontrolli soovitused ja auditeeritute vastused 13

Auditi iseloomustus 14

Auditi eesmärk 14
Hinnangu andmise kriteeriumid 14

Riigikontrolli varasemaid auditeid infoturbe valdkonnas 16

Valdkonna ülevaade

1. Riigi igapäevaseks toimimiseks, sh avalike e-teenuste pakkumiseks, asutustevahelise asjaajamise tagamiseks ning elanike, ettevõtjate, aga ka teiste riikidega suhtluseks ja andmevahetuseks on vaja, et infosüsteeme käitavad serverid ja nendega seotud muud infovarad oleksid füüsiliselt kaitstud. See omakorda tähendab, et ruumides ja hoonetes, kus eelnimetatud varasid hoitakse, peab olema tagatud füüsiline turvalisus.

2. Sellisteks ruumideks on eelkõige riigiasutuste serveriruumid ja nende toimimiseks vajalikud tehnilised ruumid, näiteks elektrivarustuse, jahutuse, tulekustutuse või sideruumid. Kõik nimetatud ruumid vajavad nende omanikelt/haldajatelt erilist kaitset ning kindlaks määratud turvalisusnõuetega arvestamist.

ISKE – infosüsteemide kolmeastmeline etalonturbe süsteem, mille rakendamine on riigi andmekogudele kohustuslik kuni 31.12.2023. Selleks kuupäevaks peavad kõik ISKE rakendajad üle minema uuele Eesti infoturbestandardile E-ITS.

Andmekeskus – organisatsiooni füüsiline või virtuaalne infotehnoloogiataristu arvutite, serverite, salvestite ja sidesüsteemide koondmajutuseks koos töötluse, andmete, side ja toite varunduse süsteemidega, jahutus- ja kliima-seadmetega ning turvasüsteemidega.

Allikas: Eesti infoturbestandard E-ITS

3. Serveriruumide ja serveriruumide tööks vajalike tehniliste ruumidega seotud olulisemad ohud on (ISKE ja E-ITSi ohtude kataloogi põhjal)

- andmekeskuse kavandamise vead;
- lubamatu sissepääs;
- puudulik seire;
- andmekeskuse ebasobiv mikrokliima;
- tuli;
- vesi;
- puuduv või puudulik sissemurdmiskaitse;
- elektrikatkestus.

4. Tõsise intsidendi korral mõnes serveriruumis, kus hoitakse riigiasutuste infosüsteeme, on teenuste katkestuste korral sellest mõjutatud enamik Eesti elanikest ja ettevõtetest. Suuremates serveri-ruumides asuva vara hävimisel ulatuvad kahjud miljonitesse, keskmise suurusega serveriruumides sadadesse tuhandetesse eurodesse.

5. Kui volitamata juurdepääsu korral serveriruumidele lekivad isikuandmed, siis kahjustatakse selle tulemusena inimeste privaatsust ja kannatab e-teenuste usaldusväärsus. Samuti võib see kaasa tuua suuri trahve. Lisaks on väga tõenäoline, et laiaulatusliku andmelekkega või mõne serveriruumi hävimisega kaasneb oluline mainekahju.

6. Nõuded serveri- ja kontoriruumide turvalisuse tagamiseks on kuni 31.12.2023 kehtestatud infosüsteemide kolmeastmeline etalonturbe süsteemiga (ISKE). Edaspidi on nõuded kehtestatud Eesti uue infoturbestandardiga (E-ITS). Kui ISKE puhul toimub infovarade kaitse korraldamine andmekogupõhiselt, siis E-ITSi rakendamisel lähtutakse kaitset vajavatest äriprotsessidest. Auditis lähtus Riigikontroll mõlemast nimetatud infoturbe raamistikust.

Hoonete turvalisus

Turvaperimeeter – turvapoliitika kehtivuse ala piir, mille puutumatuse tagamiseks rakendatakse turvameetmeid. Perimeeter on piirjoon, mis eraldab mingi ala selle ala ümbrusest otseses või kaudses tähenduses.

Loe lähemalt

auditeeritud asutuste kohta lk 14–15.

7. Serveri- ja kontoriruumide turvalisuse tagamine saab alguse hoone välisest turvaperimeetrist. Andmekeskuse või serveriruumi hoone asukohast tulenevad ohud võivad oluliselt mõjutada IT-süsteemide käideldavust ja töökindlust. Samuti võivad serveriruumide tööd mõjutada katkestused või häired energiavarustuses ja andmesideühenduses.

8. Audit tõi välja, et enim infoturbepuudusi esineb vanemates hoonetes asuvates serveriruumides või kontoriruumidega samas majas asuvates serveriruumides. Valimisse võetud asutustest enamik hoidis oma andmeid ja infosüsteeme peamiselt andmekeskustes renditud serveriruumides. Vaid neljal auditeeritud asutusel üheteistkümnest olid endal serveriruumid, mis asusid nende endi hoonetes.

Asukohast tulenevate riskide hindamine

9. Andmekeskuse kavandamisel või serveriruumiks sobivate ruumide valimisel tuleb arvesse võtta seal asuvate IT-varade kaitsetarvet ja hinnata, milliseid turvameetmeid on vaja rakendada nende kaitseks. Sellest lähtudes peavad asutused rakendama andmekeskuse või serveriruumi tarbeks tehnilised ja korralduslikud kaitsemeetmed.

Kahes asutuses ei olnud hinnatud mõningaid füüsilise turvalisuse olulisi riske

10. Audit näitas, et enamasti olid auditeeritud asutused hinnanud, millised riskid võivad enim ohustada hooneid, milles serveriruumid asuvad. Ent alati ei olnud asutused ise neid riske analüüsinud.

11. Näiteks oli kahe auditeeritud asutuse puhul hoone omanik selle valmides hinnanud küll kõige otsesemaid hoonet ähvardavaid riske, kuid ei olnud arvesse võtnud mitmeid muid olulisi riske, mis võivad ohustada serveri-, kontori- ja sideruumide füüsilist turvalisust. Seejuures olid hindamata side- ja tehnovõrkude häirete, varavastaste kuritegude (vargus, vandalism), füüsilise ründe või lubamatu sisenemise riskid. Kui mõned riskid jäävad hindamata, võivad rakendamata olla ka nende maandamiseks vajalikud turvameetmed ning infovarad võivad olla ohustatud. Nimetatud kahes asutuses hindamata riskide realiseerumist ja rakendamata meetmeid auditi käigus ei tuvastanud.

12. Probleemiks võib osutuda ka see, et kõik andmed ja infosüsteemid asuvad ühes hoones ning füüsilise intsidendi korral ei ole võimalik neile andmetele ligi pääseda või nendel põhinevaid teenuseid tarbida varuandmekeskust või -serveriruumi kasutades.

Nelja asutuse teenuseid ei dubleerita

13. Auditis tuli välja, et avariiolukorras ei ole nelja asutuse puhul infosüsteemid ega teenused dubleeritud teises asukohas olevas andmekeskuses. Seesugune olukord on enamasti põhjustatud otsustest, mida asutused peavad tegema piiratud eelarveraha jaotamisel infoturbele. Kui teises asukohas olevas varuandmekeskuses ei ole võimalik teenuseid ja andmeid dubleerida, peab aktsepteerima ainsas andmekeskuses juhtuda võivaid intsidente.

14. Võimaluse puudumine põhitegevuse seisukohalt oluliste infosüsteemide või teenuste taastamiseks või kasutamiseks teises asukohas võib intsidentide korral ainsas andmekeskuses põhjustada pakutavate teenuste pikaajalisi katkestusi.

Välise turvaperimeetri kaitse

15. Hoone kaitsmise kõrval tuleb kaitsta ka hoone välises turvaperimeetris asuvaid serveriruumide tööks vajalikke rajatisi.

Mõnedel juhtudel ei olnud serveriruume teenindav taristu kaitstud

16. Audit näitas, et enamasti asusid serveriruumide tööks vajalikud rajatised ja seadmed nendega samas hoones või hoone juurde kuuluval kaitstaval alal ning olid väliste ohtude vastu kaitstud. Siiski asus ühes asutuses serveriruumi teenindav alajaam territooriumilt väljas eraldi kaitsmata alal. Samuti ei olnud mõnes asutuses hoonest väljas paiknevad seadmed (elektrigeneraatorid) kaitstud piisavate turvameetmetega. Väliste seadmete kaitsmiseks tuleks füüsiliselt piirata nendele ligipääsu ja ühtlasi katta vajalikud alad andurite ja videovalvekaameratega.

17. Rünnak alajaamale, puhvertoiteallikale või varutoitegeneraatorile, mis varustab serveriruume vajaliku elektrienergiaga, võib tekitada elektriühenduse katkemise ning seeläbi ka teenuste katkestuse.

18. Samuti tuleb kaitsta hoone puhul, kus asuvad serveri- ja kontoriruumid, välist turvaperimeetrit. See võib sisaldada näiteks turvaliste välispiirete ehitust, hoone ümbritsemist aiaga, meetmete rakendamist piiratud territooriumile kellegi kogemata sattumise ärahoidmiseks või hoonesse sissetungi raskendamiseks jne.

Ühe asutuse väline turvaperimeeter ei olnud täielikult kaitstud

19. Ühe auditeeritud asutuse hoone väline turvaperimeeter ei olnud kogu ulatuses kaetud vajalike anduritega. Nende andurite eesmärk on tuvastada sissetungikatsed. Kuna osa perimeetrist oli anduritega katmata, suurendab see territooriumile märkamatu sisenemise riski. Teiste auditeeritud asutuste puhul ei olnud seesugused turvameetmed ei vajalikud ega nõutavad.

20. **Riigikontroll saatis 13.09.2023 auditeeritud asutustele märgukirjad, mis sisaldasid detailseid soovitusi** serveriruume puudutavate riskihinnangute koostamiseks, põhitegevuse seisukohalt kriitiliste infosüsteemide ja teenuste dubleerimiseks teises asukohas olevates andmekeskustes ning serveriruumide tööks vajalike rajatiste ja seadmete kaitsmiseks täiendavate meetmete kasutusele võtmiseks.

Serveriruumide turvalisus

21. Audit näitas, et vaadeldud serveriruumides ja serveriruumide tööks vajalikes tehnilistes ruumides on enamasti rakendatud vajalikud turvameetmed, kuid mõningates ruumides ja hoonetes esineb puudusi.

22. Ka ei olnud auditile eelnenud ajal toimunud valimisse võetud serveriruumides kriitilisi küberintsidente. Serveriruumides esines väiksema mõjuga intsidente, näiteks puhvertoiteseadmete (UPS) ülekuumenemist ja rikkeid, häireid jahutusseadmete töös või volitamata sisenemist tehnilistesse ruumidesse, kuid need ei mõjutanud pikemaajaliselt asutuste tööd ega teenuste osutamist.

Serveriruumi ebasobivast mikrokliimast tulenevad riskid

23. Serveriruumide efektiivse töö tagamise üks olulisemaid eeldusi on tagada neis ruumides vajalik mikrokliima, s.t hoida temperatuur, õhuniiskus ja õhus sisalduvate peenosakeste hulk vajalikus vahemikus.

See seab mitmed nõuded näiteks kütte-, jahutus- ja ventilatsiooni-seadmete, aga samuti tule-, suitsu- ja veelekkeandurite haldamisele ja juhtimisele. Ekstreemsete tingimuste korral võivad tekkida tulekahjud ja veeõnnetused, mis võivad pöördumatult kahjustada serveriruumides olevaid seadmeid.

24. Audit näitas, et enamasti oli serveriruumides vajalik mikrokliima tagatud ning serveriruumide tööks vajalike tehniliste süsteemide, näiteks tulekustutussüsteemide, jahutusseadmete, puhvertoiteallikate hooldused üldjuhul läbi viidud vastavalt hooldusgraafikutele.

Osas serveriruumides ei olnud tõhusat jahutust

25. Samas leidis Riigikontroll, et mõnes auditis vaadeldud serveriruumis oli ebatõhusalt korraldatud jahutuse lahendus, s.t seadmekappidel puudusid uksed ja seinad (olid vaid raamid), seadmekappide vahel puudusid nn sooja- ja külmavahed, ei toimunud külma õhu suunamist seadmekappidesse ja sooja õhu väljatõmmet. Ebatõhusa jahutus-lahendusega kaasnevad märkimisväärselt suuremad jahutuskulud. Samuti on võimalik, et mõnes ruumiosas tekib ohtlik temperatuuri tõus, mis võib ohustada seadmeid.

M-turbeaste — ISKEs on kirjeldatud kolm turbeastet: madal (L), keskmine (M) ja kõrge (H). Turbetase määratakse andmete turvaklasside (turvaosaklasside) järgi. Turvaklasside määramisel lähtutakse teabe konfidentsiaalsusest, teabe terviklusest ja käideldavusest.

Täppiskliimaseadmed – seadmed, mis võimaldavad täpsemalt seadistada õhutemperatuuri ja niiskusparameetreid.

26. Osas M-turbeastmega serveriruumides ei olnud kasutusel täppiskliimaseadmed. Kui täppiskliimaseadmeid ei kasutata, siis ei taga kliimaseadmed kindlat õhuniiskuse taset ja rakendada tuleb alternatiivseid niiskusnäitajate tagamise meetmeid.

27. Tuli ja suits võivad serveriruumides põhjustada suurt kahju (seadmete ülekuumenemine, hävinemine). Kõige sagedasemaks tulekahju põhjuseks on elektriseadmete rikked (nt avarii toitegeneraatoris, puhvertoiteallikas, kliimaseadmes).

Kahe asutuse serveriruumis ja abiruumis hoiti tuleohtlikke materjale

28. Üheksas auditeeritud asutuses üheteistkümnest olid serveriruumide tuleohutuse tagamisel olulisemad riskid maandatud. Samas hoiustati auditi ajal kahe auditeeritud asutuse serveriruumis ja serveriruumi kõrval olevas gaaskustutuse ruumis tuleohtlikke materjale (pappkastid ja paberkotid). Põlevmaterjalide hoiustamine serveri- ja tehnilise taristu ruumides võib tekitada soodsa keskkonna tuleõnnetuste tekkimiseks.

29. Kahe auditeeritud asutuse vanemates serveriruumides olid puhver-toiteseadmed ja jahutusseadmed serveriruumides sees. Täiendavate seadmete paigutamine serveriruumi tõstab seadmete ülekuumenemise või põlengu tekkimise riski.

Ühes serveriruumis puudus automaatne tulekustutussüsteem

30. Ühes serveriruumis, kus majutatakse mitmeid olulisi valdkondlikke andmekogusid, puudus automaatne tulekustutussüsteem (gaaskustutus). Kõigis olulisemates serveriruumides tuleks kasutada automaatset tulekustutussüsteemi, mis võimaldab tulekahju võimalikult varajases staadiumis kustutada. Automaatse tulekustutussüsteemi puudumisel tuleb tuli kustutada käsikustutiga või oodata päästjate saabumist, kuid selle aja jooksul võivad serveriruumis olevad seadmed tules hävineda.

31. Serveriruumis valitseva mikrokliima seiramine on vajalik seal paiknevate seadmete tõrgeteta töö tagamiseks. Kui selle tarbeks ei ole ruumi paigutatud andureid või kaameraid ning protseduure nende jälgimiseks, võidakse seadmete rivist väljalangemist märgata liiga hilja ja tõrkele ei suudeta reageerida õigel ajal. Seesugused tõrked mõjutavad aga otseselt andmete vahetust ja teenuste osutamist.

Ühes serveriruumis esines probleeme anduritega

32. Ruumi paigutatud andurid peavad olemas töökorras ja nende katteulatus peab olema piisav. Üheksas vaadeldud asutuses Riigikontroll serveriruumide anduritega seotud märkimisväärseid probleeme ei leidnud. Ühe auditeeritud asutuse serveriruumis ei olnud töökorras kaks automaatse tulekahjusignalisatsioonisüsteemi (ATS) andurit. Samuti puudus kindlus, et serveriruumi paigutatud liikumisandurid suudavad tuvastada sisenemise välisseinas olevate kinniehitatud aknaavade kaudu. Lisaks ei olnud teise auditeeritud asutuse serveriruumi paigaldatud veelekkeandurit.

33. Kliima- ja liikumisandurite puudumine või mittetoimimine võib suurendada riski, et tule- või veeõnnetus või sissetung avastatakse liiga hilja. See omakorda tähendab, et selliste intsidentide põhjustatud tagajärjed, näiteks teenuste tõrked, seadmete kahjustused, on oluliselt raskemad.

34. Samuti aitab veeõnnetusi varakult avastada ja tagajärgi leevendada põrandate tõstmine serveriruumides. See on meede, mida on rakendatud enamikus tänapäevastes serveriruumides. Audit näitas, et ühe auditeeritud asutuse serveriruumi põrandat ei olnud tõstetud.

Juurdepääsude haldamine

35. Infoturbe seisukohalt on vaja piirata isikute ringi, kellel on õigus pääseda serveriruumi. Samuti on vaja kehtestada meetmed, et volitamata isikutel ei oleks võimalik nendest reeglitest üle astuda. Puuduliku pääsukontrolli korral saavad volitamata isikud serveriruumidesse siseneda ning hooletusest või tahtlikult kahju tekitada. Tahtlik kahju tekitatakse eelkõige seadmete varguse, nende rikkumise või süsteemidesse sissemurdmisega.

Ühe asutuse serveriruumidesse pääsemiseks piisab vaid uksekaardist

36. Audit näitas, et ühe asutuse serveriruumidesse pääses ühefaktorilise autentimisega, s.t ainult uksekaarti kasutades. Serveriruumidesse volitamata isikute ligipääsemise riski vähendamiseks tuleb kasutada kahefaktorilist autentimist, näiteks uksekaarti ja koodi.

37. Tehniliste vahendite olemasolu korral on nõrgematel kaardistandarditel töötavate uksekaartide kopeerimine võimalik loetud minutite või isegi sekundite jooksul. Riigikontroll leidis, et mõni asutus kasutab serveri- ja kontoriruumides ligipääsukaarte, mis ei ole piisavalt tugeva turvastandardiga. Samas puudub ka uues infoturberaamistikus E-ITS nõue selle kohta, millist kaardistandardit peaks kasutama.

38. Mitmed juurdepääsuhaldusega seotud probleemid ilmnesid auditi käigus vaid üksikutes asutuses:

- Ühe auditeeritud asutuse juurdepääsusüsteemi keskseadme halduskontod olid liiga laialdaste õigustega ning ligipääsetavad ka valvelaua arvutist.
- Teise auditeeritud asutuse serveriruumide seadmete lepingulised hooldajad saavad serveriruumidesse siseneda ka ilma asutusepoolse saatjata.
- Kolmanda asutuse serveriruumi hoonesse suunduval teel on üks kilomeeter enne hoonet lukustatav tõkkepuu, mida saab avada

vaid asutus. See võib aga takistada näiteks operatiivsõidukite või muude osapoolte juurdepääsu hoonele.

Serveriruumide valve

39. Serveriruumi valvesüsteemi loomisel peab lähtuma hoone turvanõuetest, arvesse tuleb võtta ka hooneosade erinevat kaitsetarvet. Pääsu reguleerimise süsteemi kõrval on tavaliselt vaja kasutusele võtta ka sissemurdmisevastane valvesüsteem ning tundlikes asukohtades täiendada seda videovalvesüsteemiga. Audit näitas, et mõningatel juhtudel olid juurdepääsu- ja videovalvesüsteemi keskseadmete füüsilise kaitse meetmed puudulikud.

Ühe asutuse serveriruumid ei olnud valvestatud

40. Auditi valimis olnud neljal asutusel asusid serveriruumid enda hoonetes. Neist asutustest üks ei valvestanud oma serveriruume. Riigikontroll leiab, et kõik serveriruumid peaksid olema vähemalt väljaspool tööaega valvestatud, tundlikke andmeid ja andmekogusid sisaldavad serveriruumid aga ööpäev läbi. Valvestamata jätmine loob võimaluse serveriruumi või seal olevate seadmete kahjustamiseks, nendega manipuleerimiseks, samuti nende varguseks või tundlike andmete kopeerimiseks.

41. Kui kaitsemeetmena kasutatakse videovalvesüsteemi, siis peab see toimuma vastavuses üldise turbekontseptsiooniga. Videovalvesüsteemi keskseadmed peavad asuma turvalises keskkonnas ja olema kaitstud volitamata juurdepääsu eest, s.t kättesaadavad ainult neile isikutele, kellele need seadmed ja juurdepääsud on tööülesannete täitmiseks vajalikud. Samuti peab videovalvesüsteem olema regulaarselt hooldatud ja videosalvestised piisavalt kaua säilinud, et intsidendi korral selle tekkimise põhjuseid või tagajärgi välja selgitada ja analüüsida.

Leiti mõningaid puudusi videovalvesüsteemide haldamisel ja kasutamisel

42. Auditi käigus leidis Riigikontroll mõningaid puudusi videovalvesüsteemide haldamisel ja kasutamisel:

- Ühe auditeeritu videovalvesüsteem ei olnud piisavalt kaitstud. Hoones, kus serveriruum asus, pääses videovalve keskseadmetele ligi suurem hulk inimesi. Sellega kaasneb kõrgem andmetega manipuleerimise risk, mis võib kaasa tuua süsteemi desaktiveerimise või salvestiste kustutamise.
- Ühes asutuses asusid videosalvestised ja nende talletamise seadmed serveriruumides koos teiste seadmetega. See tähendab, et ligipääsu neile ei olnud eraldi piiratud, sh ei olnud seadmed eraldi asuvas ega lukustatud hoiupaigas.
- Kahel asutusel üheteistkümnest puudus videovalvesüsteemi hooldusleping. Sellises olukorras võivad videovalvesüsteemi või selle komponentide tõrgete korral olla serveriruumid pikalt ilma valveta.
- Kolmel asutusel üheteistkümnest ei olnud kirjalikus vormis kindlaks määratud, kui kaua minimaalselt säilitatakse videovalve salvestisi. Ühe auditeeritu puhul oli küll määratud maksimaalne säilitamise aeg, kuid miinimumnõuded puudusid. Samas tuleb märkida, et ka uues infoturberaamistikus E-ITS ei ole üheselt

kindlaks määratud, kes ja kui kaua peab säilitama turvavideote salvestusi ning valvestamis- ja juurdepääsulogisid.

43. Sarnaselt videovalve salvestiste turvalisusega tuleb hoolt kanda ka kõigi valvesüsteemi komponentide logifailide eest (nt füüsilise juurdepääsusüsteemi logid, valvestamise logid). Ka logisid tuleb säilitada turvaliselt ja piisavalt kaua, et tagada tõhus turvaintsidentide avastamine ja analüüsimine.

44. Auditi käigus veendus Riigikontroll videosalvestiste ja logide kontrolliga, et auditeeritud asutused säilitavad neid enamasti vähemalt ühe kuu ulatuses ning see kohustus oli kindlaks määratud ka sisekordades. Samas selgus, et ühes auditeeritud asutuses ei olnud juurdepääsu- ja valvestamislogile sätestatud aega, kui kaua minimaalselt oleks vaja seda säilitada.

Puhver- ja varutoite probleemid

45. Andmekeskuse tööks olulised elektri- ja IT-seadmed, välja arvatud suure energiatarbega seadmed (nt kliimaseadmed), peavad olema katkematu toite tagamiseks ühendatud puhvertoiteallikaga (UPS). Puhvertoiteallikaid hooldatakse ja nende töövõimelisust kontrollitakse perioodiliselt, tootja ettenähtud sagedusega. Voolukatkestuse korral kasutatakse andmekeskuse toite tagamiseks lisaks UPSidele avariitoitegeneraatoreid.

Ühes asutuses oli UPS nõutud sagedusega hooldamata

46. Kõigis auditeeritud asutuste serveriruumides oli puhver- ja varutoide üldjuhul tagatud. Ühes auditeeritud asutuses oli puhvertoiteallika viimane hooldus tehtud 22.03.2022 ehk enam kui aasta tagasi. Selles asutuses oleks UPSi pidanud hooldama aga vähemalt üks kord aastas. Regulaarse hoolduseta ei pruugi puhvertoiteseadmed olla vajadusel töökorras ega teenindada serveriruumi, kuni avariitoitegeneraator käivitub. See võib põhjustada katkestusi serverite töös ja nende kaudu pakutavates teenustes.

47. Kahes auditeeritud asutuses ei asunud avariitoitegeneraator hoone juures, kuid vajadusel oli need võimalik sinna transportida. Neist ühe asutuse avariitoitegeneraatori hooldamiseks ei olnud sõlmitud hoolduslepingut, samuti ei olnud selge generaatori kasutamise kord. Kui generaatorit ei suudeta tööle panna enne UPSi akude tühjenemist – kas siis seepärast, et see ei jõua piisavalt kiirelt serveriruumini, või seepärast, et selle kasutamise korraldus ei ole selge –, võib serveriruum jääda elektrienergiata ning sealtkaudu osutatavad teenused katkeda.

48. **Riigikontroll saatis 13.09.2023 auditeeritud asutustele märgukirjad, mis sisaldasid detailseid soovitusi** automaatse gaaskustutussüsteemi kasutuselevõtuks, UPSide ja kliimaseadmete kasutamiseks serveriruumides, tuleohtlike materjalide hoiustamise vältimise kohta serveriruumides, andurite kasutamiseks serveriruumides, serveriruumide kaitsmiseks veelekete eest, serveriruumidesse turvalisema sissepääsu tagamiseks, videovalve- ja juurdepääsulogide haldamise süsteemi muutmiseks turvalisemaks ning avariigeneraatori valmisoleku tagamiseks.

Kontoriruumide turvalisus

49. Asutustel, millel on oma serveriruum, on samas hoones enamasti ka muu otstarbega ruume, näiteks sideruume, tehnilisi ruume, laoruume ja peaaegu alati ka kontoriruume. Sellistes asutustes on kontoriruumides infoturbe tagamine olulisem juba seetõttu, et kontoriruumid on sel juhul serveriruumide turvaperimeetri üheks osaks.

50. Aga ka ilma serveriruumideta on kontoriruumides infoturbe tagamine oluline, kuna enamasti on seal olemas kaugjuurdepääs andmekogudele ja andmetele. Seetõttu varitsevad ka kontoriruume mitmesugused ohud, näiteks volitamata isikute juurdepääs kontoris olevatele IT-varadele või tundlikele andmetele võib päädida nende varguse, nendega manipuleerimise või nende hävitamisega.

Esmane turvalisus on kontoriruumides tagatud

51. Auditi käigus veendus Riigikontroll, et IT-majade kontoriruumides olid üldiselt esmased vajalikud turvameetmed füüsilise turvalisuse tagamiseks rakendatud ja seetõttu on volitamata isikute ligipääsu riskitase kontoriruumidesse madal.

Kontoriruumide turvalisuse korraldus

52. Esmase turvalisuse tagamisel kontoriruumides on oluline, et nende ruumide turbe- ja pääsukontrollisüsteemid vastavad ruumis käideldava teabe kaitsetarbele. Samuti on oluline, et kontoriruumide infoturbemeetmed oleksid ametlikult kirjaliku reeglistikuna vormistatud, et vajalikud infoturbeprotseduurid ja nende rakendamise kohustuslikkus oleks kõigile asutuse töötajatele selgelt ja arusaadavalt teada antud.

Kahes asutuses esines puudusi turvalisusreeglite ja -kordade kehtestamisel

53. Auditi käigus selgus, et seitsmel asutusel üheksast olid kontoriruumide kaitsemeetmed asutuste sisekordades reguleeritud. Kahe auditeeritud asutuse töösisekorra reeglid ei kohustanud töötajaid sulgema kontoriruumide aknaid ja uksi tööpäeva lõpus oma kabinetist või kontorist lahkudes.

54. Nimetatud kahest asutusest ühe kontorihoones on tavaks, et külalised iseseisvalt kontoriruumides liikuda ei saa ning neil peab olema saatjaks asutuse töötaja. See reeglistik aga ei olnud kirjalikult kehtestatud.

55. Juhul kui bürooruume või selle aknaid ei lukustata või kui IT-seadmeid piisavalt ei turvata, võib volitamata sisenejal olla väga lihtne kiiresti ja märkamatult kaasa võtta andmekandja või nutiseade. Vargusest tekkiv kaudne kahju on oluliselt suurem kui andmekandja või seadme asendamise kulu, sest ligi võidakse pääseda konfidentsiaalsetele andmetele ning neid kustutada, oma huvides ära kasutada või avalikustada.

Kontoriruumide valve

56. Nagu kõigi muude infoturbemeetmete puhul, tuleb kontoriruumide valvesüsteemi ülesehitamisel lähtuda ruumide kaitsetarbest, näiteks vajaduse korral kombineerida mehitatud valve ja tehnilise valve vahendeid (andurid, kaamerad jne). Samuti tuleb kindlaks määrata ka protseduurid selleks, et juba toimunud intsidentide korral oleks säilinud piisavas mahus infot tehniliste valveseadmete kohta (nt logid, videosalvestised).

Ühe asutuse hoonet ei valvestatud töövälisel ajal kogu ulatuses

57. Auditi käigus ei leidnud Riigikontroll probleeme enamiku auditi valimis olnud asutuste valvesüsteemides. Ühe auditeeritud asutuse büroohoones ei valvestata töövälisel ajal kogu hoonet. Riigikontrolli hinnangul tagaks aga parema kaitse kontoriruumide valvesse panemine täies ulatuses.

58. Kahe auditeeritud asutuse puhul leidis Riigikontroll probleeme juurdepääsu- ja valvestamislogide ning videosalvestiste säilitamisel:

- Ühe asutuse kontorihoone juurdepääsu- ja valvestamislogide ning videosalvestiste säilitamise tähtajad ei olnud infoturbe dokumentatsioonis kindlaks määratud.
- Teise asutuse sisemine kord nägi ette, et infosüsteemis säilitatakse valvekaamerate videosalvestisi 3 kuud. Kontrollides tegelikku säilitamise aega, leidis Riigikontroll, et videosalvestisi oli säilitatud vaid 10 päeva ulatuses.

59. Kontorihoone osaline tehnilise valveta jätmine suurendab lubamatu sissetungi, seega andmete ja IT-vahendite varguse või nendega manipuleerimise riski. Sissepääsu- ja valvestamislogi puudumisel aga ei saada ülevaadet, kes ja millal on viibinud kontoriruumides ning millal on sisse lülitatud tehniline valve. Kui logisid ja videosalvestisi ei säilitata piisavalt kaua, raskendab see füüsilise juurdepääsu intsidentide lahendamist.

60. **Riigikontroll saatis 13.09.2023 auditeeritud asutustele märgukirjad, mis sisaldasid detailseid soovitusi** infoturbereeglite täiendamise (nt ruumide sulgemine ja kolmandate isikute liikumine kontoriruumides), kontoriruumide valvestamise ning videovalve salvestiste ja juurdepääsulogide säilitamise kohta.

Auditeeritute vastused: Auditeeritud asutused nõustusid enamiku Riigikontrolli tähelepanekute ja soovitustega ning esitasid oma plaanid puuduste likvideerimiseks ja vajalike turvameetmete rakendamiseks. Üksikute tähelepanekute osas otsustasid auditeeritud asutused riske aktsepteerida ja/või rakendada riski vähendamiseks muid lisaturvameetmeid.

/allkirjastatud digitaalselt/

Ines Metsalu-Nurminen
auditiosakonna peakontrolör

Riigikontrolli soovitused ja auditeeritute vastused

Riigikontroll saatis 13.09.2023 auditeeritud asutustele auditi detailsete tulemuste kohta märgukirjad, mis sisaldasid täpsemaid soovitusi serveri- ja kontoriruumide füüsilise turvalisuse parendamise kohta. Auditeeritud asutused nõustusid enamiku Riigikontrolli tähelepanekute ja soovitustega ning esitasid oma plaanid puuduste likvideerimiseks ja vajalike turvameetmete rakendamiseks. Üksikute tähelepanekute osas otsustasid auditeeritud asutused riske aktsepteerida ja/või rakendada riski vähendamiseks muid lisaturvameetmeid.

Täpsemad soovitused serveri- ja kontoriruumide füüsilise turvalisuse parendamise kohta ning auditeeritute vastused on asutusesiseseks kasutamiseks, lähtudes avaliku teabe seaduse § 35 lg 1 p-st 9.

Auditi iseloomustus

Auditi eesmärk

Eesmärk oli hinnata, kas serveriruumides, serveriruumide toimimiseks vajalikes ruumides ja kontoriruumides rakendatakse ettenähtud turvameetmeid ja kas riskid on vähendatud aktsepteeritavale tasemele.

Hinnangu andmise kriteeriumid

Auditi üldhinnangu andmisel võeti aluseks järgmised olulisemad kriteeriumid:

- Riigiasutuste serveriruumides ja serveriruumide tööks vajalikes tehnilistes ruumides on rakendatud turvameetmed, mis tagavad ruumide füüsilise turvalisuse.
- Riigiasutustes on rakendatud sisekontrollisüsteem, mis vähendab volitamata isikute ligipääsu riski hoonetesse ja ruumidesse aktsepteeritavale tasemele.

Auditi ulatus ja käsitlusviis

Auditi objektiks olid serveriruumid, serveriruumide tööks vajalikud tehnilised ruumid ja kontoriruumid ekspertvalimisse kuuluvates asutustes ja hoonetes. Ekspertvalimisse võeti serveriruumid, milles majutatakse riigi andmekogusid. Kontoriruumidest võeti ekspertvalimisse riigi IT-kompetentsikeskuste kontoriruumid ning ka kontoriruumid, mis asuvad serveriruumidega samas hoones.

Asutused, mille kasutuses olevad serveriruumid kuulusid ekspertvalimisse:

- Riigi Infokommunikatsiooni Sihtasutus,
- Rahandusministeeriumi Infotehnoloogiakeskus,
- Maksu- ja Tolliamet,
- Maaeluministeerium,
- Põllumajanduse Registrite ja Informatsiooni Amet,
- Eesti Rahvusringhääling,
- Tervise ja Heaolu Infosüsteemide Keskus,
- Keskkonnaministeeriumi infotehnoloogiakeskus,
- Registrite Infosüsteemide Keskus,
- Siseministeeriumi infotehnoloogia- ja arenduskeskus ning
- Riigi Info- ja Kommunikatsioonitehnoloogia Keskus.

Asutused, mille kasutuses olevad kontoriruumid kuulusid ekspertvalimisse:

- Riigi Infokommunikatsiooni Sihtasutus,
- Riigi Info- ja Kommunikatsioonitehnoloogia Keskus,
- Maaeluministeerium,

- Põllumajanduse Registrite ja Informatsiooni Amet,
- Keskkonnaministeeriumi infotehnoloogiakeskus,
- Registrite Infosüsteemide Keskus,
- Rahandusministeeriumi Infotehnoloogiakeskus,
- Siseministeeriumi infotehnoloogia- ja arenduskeskus ning
- Tervise ja Heaolu Infosüsteemide Keskus.

Auditeerimisperioodiks on ajavahemik jaanuarist septembrini 2023. aastal.

Auditi lõpetamise aeg

Auditi toimingud lõpetati juunis 2023.

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

Kontaktandmed

Auditi kohta saab lisainfot Riigikontrolli kommunikatsiooniüksusest
tel +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 80090.

Riigikontrolli postiaadress on:

Kiriku 2/4,
15013 TALLINN
tel +372 640 0700,
faks +372 661 6012
riigikontroll@riigikontroll.ee

Riigikontrolli varasemaid auditeid infoturbe valdkonnas

01.02.2023 – **Andmekogude juurdepääsuhaldus**

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

Kõik aruanded on kättesaadavad Riigikontrolli koduleheküljelt www.riigikontroll.ee