



Anneli Talvik
OÜ Kodudoktori PAK Sinu Arst
info@perearst.ee

Meie 18.01.2024 nr 8-1/23-0296/24127

VÄLJAVÕTE

Menetluse lõpetamine

Austatud Anneli Talvik

I Sissejuhatus

Riigi Infosüsteemi Amet (edaspidi RIA) algatas 19.09.2023 saadetud järelepärimisega (8-1/23-0296/231400) OÜ Kodudoktori PAK Sinu Arst (edaspidi ka PAK) suhtes riikliku järelevaevmenetluse, mille eesmärgiks on kontrollida PAK poolt küberturvalisuse seaduse (edaspidi KüTS) §-des 7 ja 8 sätestatud nõuete täitmist.

Järelevaevmenetluse läbiviimisel kontrolliti nõuetekohast täitmist järgmiste tegevuste osas:

1. korrad, eeskirjad, poliitikad vms, mis reguleerivad Tervisekeskuse infoturbe protsessi, arvutite kasutamist, kaugtöö tegemist, IT ja teiste tehniliste süsteemide haldamist;
2. kasutajaõiguste ja süsteemidele ligipääsuõiguste andmine;
3. andmetest varukoopiate tegemine ja varukoopiate töökindluse kontrollimine;
4. Tervisekeskuse kasutusel olevast tarkvarast ajakohase ülevaate olemasolu;
5. süsteemides tehtavate toimingute logimine toimingu tegija, liigi ja tegemise ajaga;
6. süsteemide tehniline logimine ja logihaldus;
7. viirusetõrje ja ründetuvastuse lahendus;
8. süsteemide turvalisuse ja toimepidevuse tagamine (sh füüsilise turvalisuse tagamine);
9. ülevaade arvutivõrgust ja seal paiknevate seadmete seostest (esitada võrgulahendust kirjeldav joonis);
10. KüTS § 8 küberintsidenditest teavitamise kohustus.

RIA küsis välja asjassepuutuvad dokumendid, analüüsis neid ning viis läbi kohapealse kontrolli, mille käigus intervjueris ning täpsustas tehnilisi aspekte PAK vastava valdkonna eest vastutavate esindajatega. Kohapealne kontroll toimus 26.10.2023 (Kontrollakt asjas nr 8-1/23-0296, allkirjastatud 07.12.2023).

Järelevaevmenetluse käigus tuvastatud asjaolud põhinevad RIA-le esitatud dokumentide analüüsil ning PAK valdkonna eest vastutavate esindajate ütlustel.

III Lõppjärelendus

KüTS § 7 ja § 8 kohaselt on PAK kohustatud:

1. rakendama alaliselt organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid küberintsidendi ennetamiseks; küberintsidendi lahendamiseks või teenuse toimepidevusele või süsteemi turvalisusele avalduva mõju ennetamiseks ja leevendamiseks;
2. tagama riskihalduse protsessi (sh riskianalüüsi) olemasolu võrgu- ja infosüsteemi turvalisust ja teenuse toimepidevust mõjutavate ning küberintsidendi tekkimist põhjustavate riskide järjepidevaks haldamiseks;
3. tagama dokumenteeritud süsteemi turvaeeskirjade ja turvameetmete rakendamise kirjelduse olemasolu ja ajakohasuse;
4. tagama süsteemi turvalisust ohustava tegevuse või tarkvara tuvastamiseks süsteemi seire ja edastama teavet süsteemi turvalisust ohustava tegevuse või tarkvara kohta Riigi Infosüsteemi Ametile (CERT-EE);
5. võtma kasutusele abinõud küberintsidendi mõju ja leviku vähendamiseks, sealhulgas vajaduse korral piirama süsteemi kasutamist või juurdepääsu süsteemile.

Lähtuvalt käesolevas dokumendis väljatoodust jõudis RIA järelevalvetoimingute tulemusena järeldusele, et tulenevalt eelkirjeldatud asjaoludest on PAK asunud aktiivselt rakendama nõuetekohaselt organisatsioonilisi ja infotehnilisi turvameetmeid küberintsidentide ennetamiseks, lahendamiseks ja nende tekkimise vältimiseks. XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX.

**Lähtuvalt eeltoodust ja vastavalt haldusmenetluse seaduse § 43 lõike 4 punktile 1 lõpetame PAK-i suhtes algatatud järelevalvemenetluse, kuivõrd järelevalvemenetluse käigus ei tuvastanud RIA olulisi puudusi infoturbe meetmete rakendamisel ning jõudis järeldusele, et PAK tegeleb aktiivselt asjakohaste infoturvameetmete rakendamisega ulatuses, mis loob eeldused küberintsidentide ennetamiseks ja lahendamiseks ning infoturbeteadlikuks teenuseosutamiseks. XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXX.**

RIA soovib jätkata senist praktikat turvameetmete alalise rakendamise osas KüTS § 7 lõike 5 (E-ITS) nõudeid järgides ning hoida pidevas protsessis PAKi personali infoturbeteadlikkus, infoturvet reguleerivate juhiste ja kinnitatud töökorralduslike reeglite ajakohasus, arvestades seejuures muutuvat infoturbe olukorda laiemalt. XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXX.

Isikul, kes leiab, et järelevalvemenetluse lõpetamise otsusega rikutakse tema õigusi, on 30 kalendripäeva jooksul arvates sellise asjaolu teadasaamisest õigus esitada vaie Riigi Infosüsteemi Ameti peadirektorile (Pärnu mnt 139 a, 15169 Tallinn, e-post info@ria.ee) haldusmenetluse seaduses sätestatud korras või Tallinna Halduskohtusse (Tallinna Kohtumaja, Pärnu mnt 7, 15082 Tallinn, e-post tlnhktallinn.menetlus@kohus.ee) halduskohtumenetluse seadustikus sätestatud korras.

Lugupidamisega

(allkirjastatud digitaalselt)

XXXXX XXXXX
juhtivekspert
peadirektori volitusel

XXXXX XXXXX
XXXXXXXXXXXXXXXXXXXX@ria.ee