



Heidi Ait  
Terviseagentuur OÜ  
info@terviseagentuur.ee

Meie 07.03.2024 nr 8-1/23-0274/24392

## VÄLJAVÕTE

### Menetluse lõpetamine

Austatud Heidi Ait

### I Sissejuhatus

Riigi Infosüsteemi Amet (edaspidi RIA) algatas 08.09.2023 saadetud järelepärimisega (8-1/23-0274/231334) Terviseagentuur OÜ (edaspidi ka PAK) suhtes riikliku järelevamenetluse, mille eesmärgiks on kontrollida PAK poolt küberturvalisuse seaduse (edaspidi KüTS) §-des 7 ja 8 sätestatud nõuete täitmist.

Järelevamenetluse läbiviimisel kontrolliti nõuetekohast täitmist järgmiste tegevuste osas:

1. korrad, eeskirjad, poliitikad vms, mis reguleerivad PAK 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. PAK 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 küberintsidentidest 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 19.10.2023 (Kontrollakt asjas nr 8-1/23-0274, allkirjastatud 03.01.2024).

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

## II Järelevamenetluse käigus tuvastatud asjaolud:

2.1 PAK on koostanud infoturvet reguleerivad korrad ja eeskirjad. PAK edastatud dokumentidest selgub, et süsteemse infoturbe haldusega on PAK alustanud enne järelevamenetluse algust. PAK on läbi viinud riskianalüüsi ja koostanud infoturbe poliitika. Infoturbepoliitika vajab veel täiendamist. PAK on tööle võtnud E-ITS rakendamise koordineerimisega tegeleva töötaja.

2.2 XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX  
XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX  
XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX.

2.3 XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX  
XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX  
XXXXXXXXXXXX.

2.4 XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX  
XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX  
XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX  
XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX.

2.5 XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX  
XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX  
XXXXXXXXXXXX.

2.6 XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX  
XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX.

2.7 XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX  
XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX  
XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXX.

2.8 PAK on kehtestanud infoturvet käsitlevates dokumentides intsidentidest teavitamise CERT-EE'le.

## III Lõppjärelus

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

