



Mall Petersen
Osäühing Saku Tervisekeskus
info@tervisekeskus.ee

Meie 25.04.2024 nr 8-1/23-0207/24707

VÄLJAVÕTE

Menetluse lõpetamine

Austatud Mall Petersen

I Sissejuhatus

Riigi Infosüsteemi Amet (edaspidi RIA) algatas 03.07.2023 saadetud järelepärimisega (8-1/23-0207/231025) OÜ Saku Tervisekeskus (edaspidi ka PAK) suhtes riikliku järelevalvemenetluse, mille eesmärgiks on kontrollida PAK poolt küberturvalisuse seaduse (edaspidi KüTS) §-des 7 ja 8 sätestatud nõuete täitmist.

Järelevalvemenetluse 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 küberintsiidentidest 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 14.08.2023 (Kontrollakt asjas nr 8-1/23-0207, allkirjastatud 26.09.2023).

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

II Järelevalvemenetluse käigus tuvastatud asjaolud:

2.1 XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX.

2.2 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.

2.5 XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX.

2.6 XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX.

2.7 XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXXXX XXXXXXXXXXXX.

2.8 PAK on korraldanud infoturvet käsitlevates dokumentides intsidentidest teavitamise.

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;
1. tagama riskihalduse protsessi (sh riskianalüüsi) olemasolu võrgu- ja infosüsteemi turvalisust ja teenuse toimepidevust mõjutavate ning küberintsidendi tekkimist põhjustavate riskide järjepidevaks haldamiseks;
2. tagama dokumenteeritud süsteemi turvaeeskirjade ja turvameetmete rakendamise kirjelduse olemasolu ja ajakohasuse;
3. 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);
4. võtma kasutusele abinõud küberintsidendi mõju ja leviku vähendamiseks, sealhulgas vajaduse korral piirama süsteemi kasutamist või juurdepääsu süsteemile.

XXXXX XXXXX
XXXXXXXX XXXXXXXX@ria.ee