SOTSIAALMINISTEERIUM

Tervishoiuteenuse osutajad

Meie 04.03.2024 nr 5.2-2/594-1

Soovitused ja suunised terviseandmete töötlemisel ja kaitsel

Head koostööpartnerid!

Tervishoiusektori andmekaitse ja küberturvalisuse tase on üha määravama tähtsusega, mistõttu kutsun tervishoiuteenuse osutajaid üles nende teemadega senisest otsustavamalt tegelema. Edastan allolevad suunised ning palun tervishoiuteenuse osutaja juhtkonnal (nõukogul) vaadata üle küberturbe ja andmekaitse korralduslike nõuete, planeeritud koolituskavade ning kokkulepitud protsesside tegelik täitmine. Ühtlasi tänan ja tunnustan neid, kes on andmeturvalisuse küsimustega juba tõsiselt tegelenud.

Euroopa Liidu Küberturvalisuse Amet (ENISA) avalikustas oma tervishoiusektori küberohumaastiku aruandes, et lunavara moodustab 54% sektori küberjulgeolekuohtudest.[1] Riigi Infosüsteemi Ameti 2023. a aruandes rõhutatakse, et ohutase tõuseb veelgi ning ründajate ja sihtmärkide ring vaid laieneb. Viimaste seas on aina enam ühiskonna jaoks kriitilisi teenuseid pakkuvaid ettevõtteid.[2] Tarkvararike ei pruugi olla üksnes eraelu riivet ohustav, vaid selle tulemuseks võib olla oht inimeste elule ja tervisele (valeandmed tervisedokumentides).[3] Seetõttu on olulisel kohal just inimeste teadlikkus ning protsessid, et võimalikke negatiivseid järelmeid ennetada – seega on riskide kaardistus ja meetmete võtmine igapäevaosaks.

Andmetega seotud negatiivsetest uudistest ei ole puutumata teisedki riigid, olgu selleks andmete lekked Barcelona või Napoli haiglas, või töökindluse ehk teenuse takistamine Madeiral.[4] Kindlasti ei sooviks me sellist järelmit, kus haiglad peaks oma süsteemid lunaravarünnaku tõttu süsteemidest välja lülitama ning teenuse osutamine oleks tõsiselt häiritud.[5] Samas on siingi küsimus riskides ja nende taandamise meetmetes (näiteks hoides andmeid krüpteeritult, eraldi vms).[6] Seega valvsust ja teadlikkust eeldatakse üha enam, kuid tihti võib olla nõrgaks kohaks just inimene, mitte süsteem. Harvad pole ka juhud, kus sihitaksegi teadlikult teenuse osutaja partnereid.[7]

---

[1] ENISA, 05.07.2023, https://www.enisa.europa.eu/news/checking-up-on-health-ransomware-accounts-for-54-of-cybersecurity-threats

[2] Riigi Infosüsteemi Ameti küberturvalisuse aastaraamat. https://www.ria.ee/media/2653/download

[3] Tarkvaraline viga, mõjutades enim perearstikeskusi, 14.09.2023, https://www.tehik.ee/uudis/ulevaade-viga-perearst3-tarkvaras

[4] ENISA, 2023 september. Situational awareness report, Health Sector, Reporting period: 01 July – 31 August.

[5] Nt 100 haiglat üle Rumeenia oli oma süsteemid võrgust välja lülitanud pärast seda, kui nende tervishoiuhaldussüsteemi tabas lunavararünnak, 12.02.2024, https://www.bleepingcomputer.com/news/security/ransomware-attack-forces-100-romanian-hospitals-to-go-offline/

[6] Vt nt Majandus- ja kommunikatsiooniministeeriumi privaatsuskaitsetehnoloogiate selgitavat kontseptsiooni ja hindeid; Privaatsuskaitse tehnoloogiate kontseptsioon PET tehnoloogiate hinded.

[7] US today, https://eu.usatoday.com/story/news/health/2024/02/18/health-data-breaches-hit-new-record-2023/72507651007/

Vaatamata pidevale infovahetusele ei tajuta küberturvalisuse tagamise vajalikkust piisavalt. **Soovitan liituda Riigi Infosüsteemi Ameti kübertestiga,[8] mis võimaldab läbida testi igaühel ja tasuta ning saada nõustamist** (RIAI on selleks rahalised vahendid ca 500 000 eur). Seni on ameti andmetel registreerijaid palju, kuid reaalseid testi läbijaid vähe (133st perearsti või keskuse töötajast on testi läbinud 51 ning 10st haiglast on registreerinud end 1372 inimest kuid testi läbinud 583).

Perearstid, kiirabid ja haiglad on kohustatud rakendama Eesti infoturbestandardi E-ITS.[9] Perearstidele on pakutud erinevaid koolitusi, korraldatud ameti poolt perearstide infopäevi ja vajadusel nõustatakse jooksvalt. Samuti on amet rahastanud ja korraldanud turvalisuse hindamise läbiviimist 15-s haiglas, viies läbi teemakohaseid õppuseid. Andmekaitse Inspektsioonil on samuti erinevaid juhiseid[10] ning siingi on võimalus kasutada inspektsiooni nõuandeliini.[11] Olulised ja lihtsasõnalised kokkuvõtted on ära toodud ka inspektsiooni lehel nagu andmetöötluse põhimõtted, andmetöötleja vastutus ning andmeturve ja selle eesmärgid jms.[12] Ka neil juhistel on oluline osa kõigis töötlemisprotsessides.

Lõimitud andmekaitse ei ole mitte niivõrd õiguslik mõiste, kuivõrd mõtteviis ja organisatsioonikultuur, sest norme rakendavad ja tehnoloogiat kasutavad ikkagi inimesed. Seega, ükskõik, kui head on kehtestatud korrad ja juhendid, ei ole neist kasu, kui töötajad selle teadmisega midagi teha ei oska või ei saa. **Andmekaitse peab olema asutuse tegevusse ning tema infosüsteemidesse sisse ehitatud enne isikuandmete töötlemisega alustamist.** Ohte tuleb ette näha ja ära hoida enne nende realiseerumist. Andmekaitsealase teadlikkuse tõstmise kõrval on sama oluline infoturbealase teadlikkuse tõstmine, sest ka küberturvalisus sõltub inimeste teadlikkusest (nt õngitsuste ja rünnete ära tundmine vms).

Rõhutan, et kuigi teenuse osutajalt eeldatakse teenuse dokumenteerimist, et tagada kvaliteetsete teenuste osutamine ja patsiendi õiguste kaitse, siis andmete haldamisel ja nende säilitamisel **on eraelu riive vähendamisel ja võimalike rünnete ärahoidmisel olulisel kohal just teadlikkus ja ennetus**. Nõuete järgimata jätmine toob kaasa vastutuse (olgu siis järelevalve asutuse rahatrahvi,[13] isiku nõude või kriminaalvastutuse). Vastutustundlik andmetöötlus austab seega andmesubjektide ehk patsientide eraelu ja õigusi. See tähendab, et vastutav töötleja teab ja rakendab parimaid meetmeid isiku õiguste tagamiseks. See tähendab ka teadlikult sõlmitud lepinguid ja andmekaitsekokkuleppeid teiste kaasatud osapooltega.[14]

Kokkuvõttes on oluline märkida, et esmane on kindlasti inimeste teadlikkuse tõstmine. Selleks, et tagada tegelik muutus, tuleks need, tänasel päeval niivõrd olulised teemad, näha ette selgelt juhatuse aasta tegevuseesmärkides. **Usun, et vaid teadlikult tegutsedes ja tegevusi järjepidavalt hinnates, saavutame parema taseme teenuste tagamisel ja andmete turvalisusel ning säilib usaldus ka teenuse osutamise vastu tervikuna.**

Lugupidamisega

(allkirjastatud digitaalselt)
Maarjo Mändmaa
kantsler

---

[8] Riigi Infosüsteemi Amet, kübertest, https://www.ria.ee/kuberturvalisus/kuberruumi-analuus-ja-ennetus/kubertest
[9] Tervishoiuteenuste korraldamise seadus, § 10 lg 2, § 17 lg 1^2, § 22 lg 4^2. Vt tutvustavata seminari, https://www.ria.ee/eesti-infoturbestandardi-e-its-kaasamisseminar-9-11-2023
[10] Inspektsiooni juhised, nt isikuandmete töötleja üldjuhend, https://www.aki.ee/kiirelt-katte/juhendid
[11] Inspektsiooni nõuandetelefon on abiks pöördujatele õigete vastusteni jõudmiseks, https://www.aki.ee/meist/vota-uhendust/nouandetelefon
[12] Inspektsioon, andmetöötlejale, https://www.aki.ee/isikuandmed/andmetootlejale/andmetootluse-pohimotted
[13] Suurim määratud summa on tänase seisuga Rootsis määratud, https://edpb.europa.eu/news/national-news/2022/swedish-authority-privacy-protection-imy-fines-region-uppsala-breaches-its_en
[14] Andmekaitse üldmäärus, art 5(1)f: Isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid.

Nele Nisu
Nele.Nisu@sm.ee