RIIGI INFOSÜSTEEMI AMET

Teie 27.03.2026 nr 5-26-16/3

Meie 04.05.2026 nr 1.1-21/26627

Riigikohus
info@riigikohus.ee

Vastus põhiseaduslikkuse järelevalve asjas nr 5-26-16

Austatud Riigikohus

Saadame Teile vastused Riigi Infosüsteemi Ametile (RIA) esitatud küsimustele põhiseaduslikkuse järelevalve asjas nr 5-26-16.

1. Kui vangistust kandev kinnipeetav saab juurdepääsu konkreetselt teie hallata olevale veebilehele, siis milliseid reaalseid kuritarvitamise riske selline juurdepääs hõlmab, kui kinnipeetav sama veebilehe kaudu e-teenuseid kasutada ei saa? Kas ja kuidas kontrollite samu veebilehti selleks, et ära hoida vabaduses olevate isikute poolseid kuritarvitusi (nt kolmandate isikute poolt lisatud suhtlusvõimalused)?

Esiteks rõhutame, et me ei tuvastanud olulisi veebilehe eesti.ee (Teabevärav) kuritarvitamise riske juhul kui kasutajal pole võimalik kasutada e-teenuseid. Sellisel juhul saab Teabevärava külastaja tutvuda vaid avalikult kättesaadava infoga riigi teenuste kohta kas veebilehe või vestlusrobot Bürokratt kaudu. Me ei tuvastanud võimalusi võtta lubamatult ühendust kolmandate isikutega Eesti.ee veebilehe kaudu.

Ka sisselogimise tulemusel ei tuvastanud me kasutusjuhtu, kus Teabevärava kasutamist saaks vahetult pidada kuritarvitamiseks. Pigem saame rääkida olukordadest, kus Teabeväravat kasutatakse kaudselt mõne keelatud tegevuse ettevalmistamiseks. Näiteks andmejälgija kaudu saab kasutaja küll tutvuda tema isikuandmeid pärinud isikute isikuandmetega, kuid andmetega tutvumist iseenesest ei nimetaks me keelatud tegevuseks. Selleks oleks vajalikud temapoolsed edasised keelatud sammud andmeid pärinud isikute suhtes. Lisaks on teoorias võimalik ettevõtja rahastusvõimaluste kuritarvitamine, kuid siin vahendab Teabevärav vaid toetust pakkuva asutuse ja ettevõtja suhtlust ning ei kanna täiendavaid riske lisaks tavapärastele toetusvõimaluste kuritarvitamise riskidele.

Seoses Teie viitega suhtlusvõimalustele toome välja, et Postkasti teenuse kaudu saab kasutaja küll tutvuda talle saadetud kirjadega, kuid neid kirju saavad saata vaid riigiasutused ning kasutaja ei saa Postkasti kasutada kirjade välja saatmiseks.

2. Kas ja mida nimetatud asutused saavad teha selleks, et kuritarvitamise riske enda hallataval veebilehel vähendada või välistada? Milline oleks veebilehe haldaja selliste

meetmete võtmise ühekordne ja seejärel regulaarne rahaline kulu ja milles see seisneks?

Teabevärava turvalisuse tagab peamiselt see, et RIA rakendab Eesti infoturbestandardit ja järgib küberturvalisuse seaduse nõudeid. Praktikas tähendab see, et RIA-s on olemas infoturbe halduse süsteem ning tegevuskava RIA äriprotsesside kaitseks ja infoturbe-eesmärkide saavutamiseks. Teabeväravas rakendatakse küberintsidentide ennetuseks infoturbemeetmeid. Näiteks on kohustuslik korraldada läbistustestimist ja ilmnenud kriitilised vead enne kasutusse andmist parandada. Kuigi kõiki infoturbemeetmeid ei ole võimalik otstarbekuse ega turvalisuse kaalutlustel loetleda, on RIA läbinud kohustuslikud auditid.

Teabevärava veebilehe arenduses järgitakse kuritarvitamise riskide vähendamiseks turvalise arenduse põhimõtteid, sealhulgas koodiülevaatusi, serveripoolset sisendandmete valideerimist, autoriseerimise kontrolle ning tavapäraste veebirünnete vastaseid kaitsemeetmeid. Muuhulgas kasutajaliidese piirangutele ei tugineta ainsa kaitsemeetmena, kriitilised kontrollid rakendatakse serveripoolel (*backend*).

Need meetmed on vajalikud, sest näeme muuhulgas Teabevärava kasutamisel katseid tuvastada turvanõrkusi näiteks SQL süstimise ründeid SQL süstimist (*injection*).

Lugupidamisega

(allkirjastatud digitaalselt)

Lauri Kriisa
osakonnajuhataja

Lauri Kriisa
Lauri.Kriisa@ria.ee