Riigi Infosüsteemi Amet

# 10+ soovitust tippjuhile küberturvalisuse tagamisel

*2019*

1

## Toeta infoturbejuhi tööd

Sul on vaja kedagi, kes teostaks süsteemset kontrolli infovarade, personali ja tööprotseduuride üle. Seda rolli saab täita edukalt vaid juhul, kui infoturbejuht on kaasatud asutusse juhtimisse, on iseseisev IT osakonnast ning ülejäänud organisatsioon tajub tema poolt antavate suuniste puhul tippjuhi toetust. Võimalusel löö kokku erinevatest õigusaktidest tulenevad rollid andmehalduse korraldamisel, nagu näiteks infoturbejuht ning andmekaitse spetsialist.

2

## Lähtu standardist

Asutuse infoturbe korraldus võiks olla üles ehitatud standardile või parimale praktikale. See annab võimaluse nõuda info- ja võrguturbe korraldamisel kehtestatud reeglite järgimist ning süsteemset aruandlust. Standard annab vastused küsimusele: kuidas korraldada infovarade haldust, juurdepääsude ja kasutajaõigustega seonduvat; kuidas varundada andmeid ja kaitsta andmekandjaid jne. RIA standardite ja järelevalve osakond toetab vajadusel teie asutust ning aitab leida just teile sobiva meetmete kogumi.

***Täpsem info:*** ***standard@ria.ee***

3

## Planeeri vahendid infoturbeks

Küberturvalisusele suunatavad vahendid sõltuvad turbenõuetest teenusele ning asutuse äririskidest. Nõua IT juhilt nende riskide hindamist (kui vaja, konsulteeri ettevõtlus- ja tehnoloogiaministri määrusega riskianalüüside koostamise nõuete ja turvameetmete kirjelduse kohta) ning asutuse IKT eelarve kinnitamisel küberturvalisusega seonduvate kulude eraldi välja toomist. RIA kriitilise informatsiooni infrastruktuuri osakond (KIIK) aitab vajadusel riskianalüüside koostamise metoodika ning teabega.

***Täpsem info:*** ***kiik@ria.ee***

4

## Testi teenuste ja süsteemide turvalisust regulaarselt.

Leppige asutuses kokku põhimõtetes, et enne uute teenuste või olemasolevate teenuste uute versioonide kasutuselevõttu tuleb alati läbi viia turvatestid. Nõua oma põhiteenuste süsteemset testimist vähemalt kahe aasta tagant, selleks vajalike lepingute olemasolu ning rahaliste vahendite planeerimist eelarvesse.

***Täpsem info:*** ***kiik@ria.ee***

5

## Kasuta Digitesti asutuse küberhügieeni parendamiseks.

Küberturvalisus sõltub töötajate teadlikkusest. Paraku näitab kogemus, et käitumismustrid on tihtipeale hoolimatud ning riskantsed. Cybexeri loodud Digitesti platvorm võimaldab kiirelt ja minimaalsete kuludega anda asutuse töötajatele põhiteadmised küberhügieenist ja tagab operatiivse ülevaate asutuse turvanõrkustest. See on omakorda heaks sisendiks täiendavate koolituste tellimiseks. Koolituste korraldamisel on abiks RIA, kes korraldab erinevaid teavitusüritusi nii tavakasutajatele kui erinevatele tehnilistele ekspertidele.

***Täpsem info:*** ***kiik@ria.ee***

6

## Investeeri võrgu kaitsesse ning seiresse

Kasuta sissetungi tõkestamise ja avastamise seadmeid ning nõua infoturbejuhilt, et võrguliiklust salvestataks ning analüüsitaks. Võrguliikluse võiks salvestada vähemalt ühe nädala, soovitavalt aga ühe kuu ulatuses. Võrguliikluse seirevõimekuse (sh sissetungi avastamine, kogu võrguliikluse salvestamine ja indekseerimine) saab luua kasutades vabavaralisi komponente, samas on vajalikud investeeringud riistavarasse. Võrguliikluse seire ja kaitse korraldamisel pakub täiendavat tuge CERT.EE ning soovitame kaaluda CERT.EE Suricata for All projektiga liitumist. Viimane lihtsustab vabavaral põhineva võrguliikluse seirelahenduse ehitamist, võimaldab saada rünnete ja pahavara tuvastamiseks CERT.EE käest reegleid ja abi.

***Täpsem info: cert@cert.ee***

7

## Krüpteeri andmevahetus

Üks peamiseid ründevektoreid seondub asutuse e-kirjavahetuse kuritarvitamisega. Nõua, et asutuse andmevahetus, eelkõige meilivahetus oleks krüpteeritud ning teie asutuse meiliaadresside võltsimine oleks kurjategijatele tehtud võimalikult keeruliseks (märksõnadena SPF poliitika, DKIM tempel ja DMARC protokoll). RIA koduleheküljelt võib leida selle tarbeks 2019. aastal uuendatud juhendi turvalisest meilivahetusest avalikus sektoris. Samuti on terviklik loetelu soovitusi e-mailide turvalisuse tagamisel leitav Ameerika ühendriikide sisejulgeolekuministeeriumi DHSi veebilehelt cyber.dhs.gov.

***Täpsem info: cert@cert.ee***

8

## Nõua CERT.EE teavitamist turvanõrkustest ja intsidentidest

Ära hoia küberintsidente enda teada ning jaga teavet Eesti küberruumi seiret teostava CERT.EEga. Iga intsidendi teade on vajalik tervikpildi hoidmiseks ning tihtipeale ka teiste kasutajate riskide maandamiseks. Kiire teavitus ning infovahetus CERT.EEga aitab kaasa riskide maandamisele riigis tervikuna. Kohustus intsidentidest teavitada on riigiasutustel ning KüTSis nimetatud erasektori teenuseosutajatel, samas on oodatud kõikide teiste asutuste teavitused.

***Täpsem info ja raporteerimine: cert@cert.ee***

9

## Nõua kriitiliste logide pidamist

Leppige kokku põhimõtted logide pidamise kohta, sest see aitab hiljem tuvastada võimalikud kuritarvitused ning teenusega seonduvad probleemid. Oluline on, et lepitaks kokku, milliseid kriitilisi logisid talletatakse ning soovitav on logisid säilitada vähemalt ühe aasta jagu.

***Täpsem info: cert@cert.ee***

10

## Kaardista riskid ning oma kriisiplaani

Hinnake ära oma äririskid ning valmistage ette plaan B, ehk kuidas teha nii, et küberintsident ei halvaks teie teenuste kättesaadavust. Oluline on omada tegevuskava kriisihalduseks, aga sellest ei piisa – kriisiplaani tuleks süsteemselt ka asutuses läbi harjutada.

***Kriisiharjutuste osas aitab teadmiste ja stsenaariumidega: kiik@ria.ee***

## Kasuta turvalist riigivõrku* (soovitus puudutab riigiasutusi)

Riigivõrk on riigi poolt osutatav internetiteenus, mille kvaliteedi ja turvalisuse eest vastutab RIA. CERT.EE teostab riigivõrgu turvaseiret Eesti parima ohuindikaatorite loetelu, tehnilise ja sisulise võimekuse toel. Riigivõrguga liitumine parandab märkimisväärselt teie asutuse küberturvalisust ning tagab ka terviklikuma vaate Eesti küberruumis toimuvast. Kui te riigivõrku kasutada ei soovi, soovitame CERT.EE tarbeks paigaldada sensorid.

***Täpsem info: kaido.plovits@ria.ee***