MAJANDUS- JA
KOMMUNIKATSIOONI-
MINISTEERIUM

KÄSKKIRI

06.11.2024 nr 80

Küberturvalisuse strateegia 2024–2030 „Läbivalt IT-vaatlikum Eesti“ ja selle tegevuskava kinnitamine

Vabariigi Valitsuse 23. oktoobri 2002. a määruse nr 323 „Majandus- ja Kommunikatsiooniministeeriumi põhimäärus“ § 23 punkti 3 alusel, kooskõlas peaministri 12. augusti 2024. a korralduse nr 88 „Ministrite pädevus ministeeriumi juhtimisel ja ministrite vastutusvaldkonnad“ punktidega 2 ja 6:

1. Kinnitan „Küberturvalisuse strateegia 2024–2030 „Läbivalt IT-vaatlikum Eesti““ (lisa 1) ja selle tegevuskava (lisa 2).

2. Tunnistan kehtetuks majandus- ja infotehnoloogiaministri 5. juuli 2024. a käskkirja nr 55 „„„Küberturvalisuse strateegia 2024–20230 „Läbivalt IT-vaatlikum Eesti“ kinnitamine“.

(allkirjastatud digitaalselt)
Liisa-Ly Pakosta
justiits- ja digiminister

KINNITATUD
justiits- ja digiministri 06.11.2024 käskkirjaga nr 80
„Küberturvalisuse strateegia 2024–2030 „Läbivalt IT-vaatlikum Eesti“
ja selle tegevuskava kinnitamine“
Lisa 1

MAJANDUS- JA
KOMMUNIKATSIOONI-
MINISTEERIUM

KÜBERTURVALISUSE STRATEEGIA 2024–2030

„LÄBIVALT IT-VAATLIKUM EESTI“

SISSEJUHATUS

Eesti on avatud ja demokraatlik ühiskond, mille avalike teenuste digitaliseeritus on maailmas üks suurimaid. Juba mitukümmend aastat on Eesti inimesed harjunud sellega, et avalikud teenused on veebis mugavalt kättesaadavad, riigile usaldatud andmed on hästi kaitstud ning nii riigi kui ka erasektori arendatavaid teenuseid muudetakse järjest nüüdisaegsemaks ja personaalsemaks. Eesti pikaajaline kogemus, tehnoloogia kiire areng ja väikeriigi paindlikkus pakuvad selleks suurepäraseid võimalusi. Samas, mida digitaliseeritum riik, majandus ja ühiskond on, seda keerulisemaks muutub küberturvalisuse tagamine. Strateegia „Läbivalt IT-vaatlikum Eesti“ visioon on kujundada selline Eesti ühiskond, mille digitaalsete teenuste usaldusväärsus ja kerksus jääb vankumatuks ka märgatavalt halvenenud julgeolekuolukorras ning väga kiire globaalse tehnoloogilise arengu kontekstis. Ainult sel viisil saame hoida Eesti elanike suurt usaldust nii digiriigi kui ka sellega läbi põimunud erasektori digitaalsete teenuste vastu.

Strateegia koostamisel on arvestatud Euroopa Liidu võrgu- ja infosüsteemide uuendatud direktiivi (küberturvalisuse 2. direktiiv)[1] suuniseid riiklikele strateegiadokumentidele[2] ning riiklikku strateegiat „Eesti 2035“. Valdkondlikke küberjulgeoleku aspekte ja arenduseesmärke on kirjeldatud riigikaitse arengukavas[3], siseturvalisuse arengukavas[4] ja muudes valdkondlikes arengukavades (teadus- ja arendustegevus, haridus, välispoliitika), käesolevas dokumendis neis öeldut ei dubleerita.

Riigi keskses arengustrateegias „Eesti 2035“ on sätestatud: „Hoolitseme selle eest, et digitaalse ühiskonna küberriskid oleksid hästi hallatud ning Eesti küberruum kõrge usaldusväärsusega.“[5] Riigi julgeolekupoliitika alustes on omakorda välja toodud: „Digitaalses ruumis peame läbivalt kõigis infosüsteemides, organisatsioonides ja protsessides planeerima küber- ja infoturvet.“[6]

Arengukava „Eesti digiühiskond 2030“[7] raamistikus on käesolev, järjekorras neljas küberturvalisuse strateegia „Läbivalt IT-vaatlikum Eesti“ käsitletav küberturvalisuse valdkonna alusdokumendi ehk valge raamatuna.[8] Horisontaalse strateegiana on see suunatud Eesti küberturvalisuse tagamisse panustavate osapoolte – avaliku sektori (nii tsiviilvaldkond kui ka sõjaline riigikaitse), ühiskonna toimimiseks elutähtsate ja oluliste teenuste osutajate, valdkonnas tegutsevate ettevõtjate ning ülikoolide ja teiste teadusasutuste – vahel kokkulepete sõlmimiseks ning tervikliku, süsteemse ja kaasava kübervaldkonna poliitika elluviimiseks sobilike tingimuste loomiseks.

Käesolev strateegiadokument seab eesmärgid 2024.–2030. aastaks neljas põhivaldkonnas: riikliku küberturvalisuse arengu juhtimine, ühiskonna küberkerksuse suurendamine, küberkilbi tugevdamine (sh intsidentide seire ja tõkestamine) ning turvalise küberkeskkonna kujundamine Eestis ja mujal maailmas.

---

[1] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555, 14. detsember 2022, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148.

[2] https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32022L2555&qid=1706103351118, artikli 7 lõige 1.

[3] Riigikaitse arengukava 2022–2031, https://www.riigikantselei.ee/media/1451/download.

[4] Siseturvalisuse arengukava 2020–2030, https://www.siseministeerium.ee/media/748/download.

[5] Arengustrateegia „Eesti 2035“, https://valitsus.ee/media/4022/download, lk 27.

[6] Eesti julgeolekupoliitika alused, https://www.riigiteataja.ee/aktilisa/3280/2202/3001/julgeolekupoliitika_2023.pdf, lk 6.

[7] Hetkel kehtiv, kuid uuendatav versioon https://www.mkm.ee/media/6791/download.

[8] Valdkonnas „Eesti digiühiskond 2030“ on koostamisel või juba valminud veel kolm valget raamatut: andmete ja tehisintellekti valge raamat, personaalse riigi valge raamat ja e-ID valge raamat.

1. STRATEEGILINE KONTEKST

Kuna küberruum on olemuselt globaalne, peegelduvad üleilmsed ohud, trendid ja võimalused ka Eestis. Võrreldes eelmise strateegiaperioodiga[9] on üldine küber- ja julgeolekuohu tase maailmas selgelt tõusnud, mis omakorda on mõjutanud kogu ühiskonna valvsust. Seda on ajendanud nii järjest suurem sõltuvus digitaalsetest lahendustest kui ka tehnoloogia, sealhulgas tehisintellekti ja kvanttehnoloogia areng. Ründajate eesmärgid on muutunud mitmekesisemaks: lisaks rahalist tulu otsivatele küberkurjategijatele annavad küberruumis varasemast rohkem tooni ka poliitiliselt motiveeritud ründajad. Viimaste hulgas on nii riikide valitsustega seotud tehniliselt kõrgetasemelisi häkkerite rühmitusi[10] kui ka sotsiaalmeedias organiseerunud vabatahtlikke ehk häktiviste.

1.1. Riikide tegevus küberruumis

Eesti ja kogu läänemaailma jaoks on küberohtu märkimisväärselt suurendanud Venemaa agressioonisõda Ukrainas. See on näidanud, et lisaks kineetilise sõjategevuse toetamisele küberrünnetega vastase elutähtsa taristu pihta kasutatakse küberründeid hübriidsõja osana ka laiemalt. Küberrünnetega kogutakse luureinfot ning „karistatakse ebasõbralikke riike“ nende poliitiliste otsuste eest. Samuti võib suureneda tarneahelate ründamise oht, mille korral kompromiteeritakse mõnd paljudes toodetes kasutatavat tarkvaralist komponenti ning selle kaudu saadakse korraga ligi suurele hulgale organisatsioonidele üle maailma. Kaudsemalt mõjutavad Eesti küberruumi ka teised aktiivsed riikidevahelised konfliktid, nagu Iisraeli-Hamasi sõda.

Ehkki Eesti julgeolekukeskkonda, sealhulgas küberohupilti, on seni mõjutanud kõige otsesemalt Venemaa tegevus, vajavad pikemas perspektiivis rohkem tähelepanu ka teised küberruumis aktiivsed autoritaarsed riigid, näiteks Iraan, Põhja-Korea ja eriti Hiina.

Hiina tegevus küberruumis keskendub peamiselt küberluurele: kogutakse informatsiooni poliitiliste suundumuste, intellektuaalomandi ja huvipakkuvate sektorite teadustöö tulemuste kohta. Oma konkurentsivõimelise tehnoloogiasektori kaudu loob Hiina süstemaatiliselt haavatavusvõimalusi, mida tal on hiljem võimalik enda kasuks ära kasutada, ning seetõttu on ta huvitatud oma toodete laialdasest ekspordist.

Maailmas jätkub ka laiem interneti haldamise ja tehnoloogia politiseerimine ning üha rohkem kasutatakse küberründeid (sh tehnoloogia tarneahelad) riikidevahelises mõjutustegevuses. Kuna Venemaa isolatsioon globaalsest internetist ja läänemaailma kasutatavatest tarneahelatest süveneb, võib teda tulevikus järjest vähem kammitseda kartus, et küberrünnetega kahjustataks iseenda jaoks vajalikke teenuseid või tarneahelaid.

1.2. Lunavararünded ja muu küberkuritegevus

Lunavararünded on juba aastaid olnud tähelepanu all kui üks kahjulikemaid globaalse küberkuritegevuse ilminguid. Kurjategijate jaoks on tegemist tulusa ärimudeliga, lunarahamaksete globaalne kogusumma on aasta-aastalt kasvanud. Kuna ründeid on tehtud ka elutähtsate teenuste ja elutähtsa taristu vastu, on lunavararünnete ennetamine ja nendega toimetulemine seotud ka riigi üldise julgeolekuga. Eestis on selliseid rünnakuid viimasel kolmel aastal registreeritud keskmiselt paarikümne ringis. Ehkki erinevalt paljudest teistest riikidest ei ole seni meie ühiskonda tõsiselt häirivad ründed tabanud, tuleb ka selle

[9] Viimane Eesti küberjulgeoleku strateegia hõlmas ajavahemikku 2019–2022.
[10] Neist rääkides kasutatakse lühendit APT, mis tuleb ingliskeelsest terminist *advanced persistent threat* (’kinnisründeoht’).

võimalusega uuel strateegiaperioodil arvestada.

Eesti inimesi mõjutab igapäevaselt kõige rohkem tavapärane küberkuritegevus, eelkõige investeerimiskelmused ning pangakontode tühjendamine õngitsuste ja petukõnede abil. Politsei- ja Piirivalveameti hinnangul peteti 2023. aastal Eesti eraisikutelt välja kokku üle 8,3 miljoni euro.[11] Küberkuritegevuse mõju vähendamisel on oluline roll süsteemsel ja kõiki ühiskonnagruppe hõlmaval ennetusel.

1.3. Tehnoloogia ülemaailmsed arengusuunad

Eesti küberjulgeolekut mõjutavad ka üldised tehnoloogilised suundumused: 5G-tehnoloogia järjest laiem kasutuselevõtt, tehisintellekti ulatuslikum rakendamine nii avaliku kui ka erasektori teenustes, esemevõrgu (IoT) laienemine, järjest suurenev sõltuvus välismaa teenusepakkujatest, sh rohkemate andmete töötlemine pilvelahendustes ning pikemas perspektiivis ka kvantarvutite kättesaadavamaks muutumine.

Mitmed tehnoloogilised suundumused võimaldavad edaspidi ka tõhusamaid küberturvalisuse lahendusi luua, ent see eeldab tugeva küberturvalisuse sektori olemasolu, uute tehnoloogiate arendamist ja krüptograafiaalase pädevuse kasvatamist. Tehnoloogia kiire areng annab Eesti ühiskonnale ja majandusele mitmesuguseid arenguvõimalusi, kui omame piisavalt oskusteavet ja innovatsiooni soodustavat majanduskeskkonda.

Mida nutikamaks muutuvad meid ümbritsev keskkond ja tehnoloogia, seda haavatavamad on need ka küberrünnakutele. Tehisintellekti ülikiire areng loob küll uusi teenusepakkumise ja ressursisäästu võimalusi, kuid neidsamu lahendusi võidakse ära kasutada ka küberrünnetes.

Majanduse digitaliseerimine ehk neljas tööstusrevolutsioon hõlmab järjest enam valdkondi, muu hulgas toidutootmist, meditsiini, kaitse-, kosmose- ja muud tööstust, mis omakorda suurendab ristsõltuvust ning kasvatab küberruumi keerukust ja küberriske. Osas valdkondades on küberriskide juhtimise praktika veel algeline. Küberturvalisus on horisontaalne alustala teenuste digitaliseerimisel, haldamisel ja arendamisel.

1.4. Arengusuunad Euroopa Liidus ja NATO-s ning samameelsete riikide koostöö

Nii tehnoloogia areng, globaalse küberkuritegevuse levik kui ka geopoliitilistest pingetest ja konkurentsist tulenev ohupildi muutumine on suurendanud sarnaselt mõtlevate riikide vahel koostöövajadust ja -soovi. Ühinenud Rahvaste Organisatsioonis (ÜRO) toimuvad arutelud küberjulgeoleku teemade käsitlemiseks uue globaalse raamistiku loomise üle ning Eesti koos teiste samameelsete riikidega seisab hea selle eest, et rahvusvahelist õigust jõustataks ka küberruumis. Euroopa Liidu riigid on saavutanud põhimõttelise poliitilise kokkuleppe maailmas esimese omataolise tehisintellekti regulatsiooni kohta ning on lisaks küberturvalisuse direktiivile võtnud 2024. aasta märtsis vastu ka küberkerksuse määruse, mis ühtlustab ja karmistab Euroopa turule jõudvate digitaalsete toodete kvaliteeti. Kuna küberrünnete ja -intsidentide edukal haldamisel on üks võtmesõnu kiirus (nt suure mõjuga tarneahelarünnete puhul), otsitakse uusi võimalusi ka operatiivseks ja automatiseeritud ohuinfo vahetuseks. Üks võimalusi on näiteks Euroopa Komisjoni regionaalsete keskuste algatus, mille raames kaalub Eesti koos teiste Põhjala ja Balti riikidega võimalusi koostööd süvendada. 2016. aastast on suurenenud Euroopa Liidu (EL) ja Põhja-Atlandi Lepingu Organisatsiooni (North Atlantic Treaty Organization, NATO) vaheline küberkaitsekoostöö ning Eesti huvides

[11] Politsei- ja Piirivalveameti 16. jaanuari 2024 pressiteade, https://www.politsei.ee/et/uudised/kurjategijad-petsid-eesti-inimestelt-vaelja-vaehemalt-8-3-miljonit-eurot-11725.

on ka selle edasine tihendamine.

Ameerika Ühendriigid on lunavararühmituste vastu võitlemisel, täisusaldamatuse turbekontseptsiooni (ingl *zero trust*) propageerimisel ning rakenduste turvalise loomise ja valideerimise (*security by design and default*) populariseerimisel võtnud maailmas enda kanda juhtrolli. Sama suund on võetud teabekaitse aluseks ka NATO-s ning see suurendab NATO võimekust töötada välja turvalisi teabevahetuse lahendusi. Sellele aitavad kaasa näiteks Eestis asuv kaitsevaldkonna iduettevõtete innovatsioonikiirendi DIANA ning küberjulgeolekualase teadus- ja arendustegevusega, sealhulgas küberõppuste ja küberharjutusväljadega tegelev Kaitseministeeriumi asutatud sihtasutus CR14.

Samuti teevad samameelsed riigid koostööd autoritaarsetest riikidest pärit tehnoloogiate riskide laiemal teadvustamisel.

2. RIIKLIKU KÜBERTURVALISUSE ARENGU JUHTIMINE

Läbivalt IT-vaatlikuma Eesti saavutamiseks on möödapääsmatu kujundada välja nüüdsetele vajadustele vastav riiklik institutsionaalne struktuur ja raamistik, mis arvestaks küberturvalisuse valdkonnas viimasel ajal toimunud muutusi. Digiriigi, sh elektroonilise teabe, kaitsmine eeldab valdkondadevahelist koostööd ja võimekuste ühist kasutamist. Selleks on omakorda vaja selgelt kindlaks määrata süsteemi osaliste pädevused, rollid ja volitused, tagada kaasav planeerimine ning kujundada toimiv kogukond. Nii avalik kui ka erasektor on nimetanud küberturvalisuse strateegilist tervikjuhtimist ja koordinatsiooni ühe peamise kitsaskohana, mida on vaja arendada.

Eesti eelmine, aastateks 2019–2022 koostatud küberstrateegia nägi ühe suurema väljakutsena asjaolu, et küberturvalisuse valdkonnas puudub koherentne strateegiline juhtimine.[12] Strateegias pakuti ühe lahendusena välja luua terviklik, mitme asutuse pädevusi koondav üksus või keskus, mille täpsem ulatus selguks kõikehõlmava ministeeriumidevahelise küberauditi abil.[13]

Muutunud julgeolekuolukorra tõttu tuleb järgnevatel aastatel üle vaadata küberturvalisuse, teabekaitse ja kriisiohje õigusruum, et see vastaks parimale praktikale ning tagaks Eesti riigi teenuste ja toimimise turvalisuse. Küberturvalisuse seaduse revisjoni käigus on Majandus- ja Kommunikatsiooniministeerium pakkunud võimalust hinnata ja ette valmistada vajalikud seadusemuudatused parimate rahvusvaheliste praktikate ülevõtmiseks, täpsustada riigisisest juhtimiskorraldust ning osaliste ülesandeid, õigusi ja kohustusi.

2.1. Valdkonna juhtimine ja poliitika kujundamine

Olukord

Küberturvalisuse valdkonda juhib ja koordineerib Eestis Majandus- ja Kommunikatsiooniministeerium (MKM). Küberturvalisuse korraldamisel osalevad mitmed asutused ja isikud, nende hulgas ministeeriumid, kohaliku omavalitsuse üksused ning elutähtsate ja ühiskondlikult oluliste teenuste osutajad, kes kujundavad ja viivad ellu strateegia prioriteete nii iseseisvalt kui ka organisatsioonide ja valitsemisalade vahel.

Küberturvalisuse tagamist ning küberintsidentide ennetamist ja lahendamist küberturvalisuse seaduses (KüTS) sätestatud ulatuses koordineerib Riigi Infosüsteemi Amet (RIA). Tarbijakaitse ja Tehnilise Järelevalve

[12] KÜBERTURVALISUSE STRATEEGIA (mkm.ee) lk 12.
[13] KÜBERTURVALISUSE STRATEEGIA (mkm.ee), lk 26.

Amet töötab Euroopa parlamendi ja nõukogu määruse (EL) 2019/881[14] alusel küberturvalisuse sertifitseerimisasutusena. Küberdiplomaatia on Välisministeeriumi portfellis. Sõjalise riigikaitsega seotud kübertegevus ja NATO-ga tehtav koostöö on Kaitseministeeriumi valitsemisalas. Siseministeerium vastutab küberkuritegevuse vastu võitlemise eest. Valdkonda kureeriv MKM ühtlustab küberjulgeoleku poliitika eesmärke küberjulgeoleku nõukogu (KJN) kaudu, kaasates kõiki ministeeriume. Lisaks on moodustatud mitmesuguseid küberkoordineerimisüksusi, millest olulisim on küberpoliitika nõukoda (KPN), kuhu kuuluvad riigiasutuste, erasektori ja teadusasutuste esindajad. Eesti küberökosüsteemi ülejäänud osalised on loetletud käesoleva strateegia lisas 1.

Vabariigi Valitsuseni (VV) jõuavad olulisimad küberteemad igal nädalal kübervaldkonna olukorra ülevaatena, samuti ajendatuna mõnest suuremast riigisisesest intsidendist. Perioodiliselt tehakse küberolukorrast ülevaateid kantsleritele ja valitsuse julgeolekukabineti nõupidamistel viibivatele valitsuse liikmetele. Samuti teavitatakse küberturvalisuse kogukonda (infoturbejuhte, elutähtsa taristu omanikke ja teenuste pakkujaid) ohuhinnangutest ja olukorrast küberruumis[15] ning edastatakse valdkondlikke uudiskirju[16]. Detsentraliseeritud juhtimismudeli tõttu on keskne poliitikakujundamine raskendatud ning rahastamine on pigem asutuste- kui valdkonnakeskne.

Alates 2018. aastast on Eestis olnud küberturvalisuse valdkonna keskne õigusakt KüTS, millega muu hulgas võeti üle Euroopa parlamendi ja nõukogu direktiiv (EL) 2016/1148 ehk küberturvalisuse 1. direktiiv. 2022. aastal võeti vastu Euroopa parlamendi ja nõukogu direktiiv (EL) 2022/2555 ehk küberturvalisuse 2. direktiiv, mis täiendab oluliselt varasema direktiivi sätteid ning tuleb ka Eesti õigusesse üle võtta[17]. Lisaks on Euroopa Liidus kehtestatud finantssektorile spetsiifilised küberturvalisuse nõuded.[18] Samuti on NATO küberturbenõuetest lähtuvalt uuendatud salastatud teabe IT-süsteemide küberkaitse nõuded riigisaladuse ja välisteabekaitse seaduses[19] (RSVS). Menetluses on Euroopa Liidu küberkerksuse, kübersolidaarsuse, küberturvalisuse ja teabekaitse määrused, NATO pilveturvalisuse rakendusdirektiivid ning liikmesriigi toimimist reguleerivad sertifitseerimisskeemid, mis toovad kaasa vajaduse kohandada ka Eesti õigusakte ja määrata riigile pandud kohustuste täitmiseks baasrahastus. 2024. aastal otsustati alustada ka Euroopa Liidu küberstrateegia uuendamist (viimane kehtiv versioon 2020. aastast), mille raames tuleb üle vaadata senised rollid, vastutus ja koostöövormid, mis võivad mõjutada käesoleva küberturvalisuse strateegia arengusuundi.

Selle kõige taustal aset leidev tehnoloogiline areng mõjutab kõiki küberohupildi aspekte, mistõttu peame Eestis suutma ühiskonnana nendega kohaneda. Tehnoloogia areng ei ole enam seotud kitsalt digilahendustega, vaid igapäevaeluga üldiselt. Eesti riik on läbi ja lõhki digiriik. Teisisõnu, küberturvalisus kontseptsioonina ei ole enam vajalik üksnes tehnoloogiate kaitsmiseks, vaid ühiskonna toimimiseks ja selle

---

[14] Euroopa Parlamendi ja nõukogu määrus (EL) 2019/881, 17. aprill 2019, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus), https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32019R0881.

[15] Vt https://www.ria.ee/kuberturvalisus/kuberruumi-analuus-ja-ennetus/olukord-kuberruumis, https://www.mkm.ee/digiriik-ja-uhenduvus/kuberturvalisus/riigi-kuberturvalisuse-tagamine.

[16] Vt https://www.mkm.ee/digiriik-ja-uhenduvus/kuberturvalisus/riigi-kuberturvalisuse-tagamine.

[17] Ülevõtmise tähtaeg on 2024. aasta oktoobris.

[18] Euroopa Parlamendi ja nõukogu määrus (EL) 2022/2554, 14. detsember 2022, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011, https://op.europa.eu/et/publication-detail/-/publication/8ebf4cce-305c-11ee-9e98-01aa75ed71a1/language-et.

[19] Riigisaladuse ja salastatud välisteabe seadus–Riigi Teataja

tulevikukindluse tagamiseks.

Tugevad ja nõrgad küljed

Kuna mitmed küberturvalisuse valdkonna tegevused on eri ministeeriumite vastutada, on strateegia ja poliitika planeerimisel oluline eesmärgid ühildada.

Seni pole analüüsitud, kas eri asutuste täidetavad funktsioonid on mõistlik ühte asutusse konsolideerida. Suund selliste konsolideeritud küberasutuste tekkeks on viimastel aastatel võetud nii Euroopa Liidus (nt Tšehhi, Holland, Prantsusmaa, Belgia, Leedu, Läti) kui ka paljudes samameelsetes riikides (nt Suurbritannia, Singapur), kuid asutuste ülesannete ulatus ning nende paiknemine riigihalduses on riigiti erinevad (mõnes riigis kaitseministeeriumi alluvuses, teistes otse peaministri alluvuses).

KüTS-iga on loodud esmane seadusandlik alus küberturvalisuse tagamiseks ning see lähtub riskipõhisusest. Riskipõhist lähenemist tuleb juurutada ka seotud õigusaktides. See võimaldab paindlikult rakendada just neid meetmeid, mis asjaolusid arvestades tagavad parimal viisil eesmärgi täitmise. Uued tehnoloogiad ja arenev ohupilt tekitavad vajaduse uuesti hinnata regulatsioonide paindlikkust ja proportsionaalsust, õiguste ja kohustuste tasakaalustatust ning subjektide ringi. Kehtivates õigusaktides esineb ebaühtlust ja ebaselgusi nõuete ja sihtrühma kohustuste osas. Kuna Euroopa Liidu, NATO ja muid rahvusvahelisi õigusakte on lühikese aja jooksul tulnud mitmeid, vajab nii nende kui ka riigisiseste õigusaktide korrektne ja kooskõlaline rakendamine erilist tähelepanu ja ühtset koordinatsiooni. Elektroonilise side seadusega on algust tehtud tarneahela riskide minimeerimisega. Ka teiste valdkondade ühtlustamiseks peavad eesmärgid olema tihedamalt sidustatud riigi küberturvalisuse eesmärkidega.

2024. aastal on Euroopa Liidu õigusaktidest tulenevalt suurenenud kübervaldkonna standardiseerimisega seotud teemade hulk (nt küberturvalisuse 2. direktiivil ja küberturvalisuse määrusel põhinevad sertifitseerimiskavad, küberkerksuse määrus, küberturvalisuse strateegia), mistõttu tuleb laiemalt hakata koordineerima riigisiseseid tegevusi (st looma võimekust, planeerima ressursse ning kaasama seotud osapooli, partnereid ja olenevalt olukorrast ka teisi turuosalisi). Eesti rahvusvaheline juhtroll küberturvalisuse kulumudeli algatuse käivitamisel on olnud puudulik ning esineb lünki Euroopa Liidu suunalises ja riigisiseses koordineerimises ning liikmesriikide küberkoostöös.

Eesmärgid, milleni soovime strateegiaperioodil jõuda

- Küberturvalisuse valdkond on keskselt tugevalt juhitud ja koordineeritud, poliitikakujundamisse kaasatakse kõiki olulisi osapooli, Vabariigi Valitsuse tasandil ollakse regulaarselt nähtaval ning arvestatakse siseturvalisuse, andmekaitse, riigikaitse ja majanduse vajadusi.
- Erinevatele sihtrühmadele seatavad küberturbealased kohustused on proportsionaalsed ja eesmärgipärased, arvestades nende rühmade tegevust ja sellega seotud küberturbeohu mõju ühiskonnale.
- Riiklik koordineerimine ja valdkonna ekspertide vaheline koostöö on tõhustatud.
- Keskse ja ajakohase küberturvalisuse valdkonna arengu riskipildi saamiseks on KJN-is jälgitud küberturvalisuse strateegia täitmist ja seiratud, uuendatud arengusuundi.
- Euroopa Liidu ja NATO direktiivid on Eesti õigusesse üle võetud. Õigusaktides on tagatud mõisteselgus, tasakaal riigikaitseliste, ettevõtlusvabaduse ja küberturvalisuse nõuete vahel, tehnoloogianeutraalsus, riskipõhisus, sh tarneahela riskide minimeerimine, ning kasutajakeskus. Ühtlasi on antud piisavalt aega nendega seotud nõuete rakendamiseks.

Nende eesmärkide saavutamiseks vajalikud tegevused

- Õigusruumi arendamisel ja küberturvalisust mõjutavate valikute langetamisel tuleb võtta arvesse rahvusvahelisi suundumusi, valitsevat ohupilti, julgeolekuolukorda ning teisi küberturvalisuse, infoturbe ja andmekaitsega seotud muutusi.
- Tuleb analüüsida küberturvalisuse pädevusi koondava asutuse või keskuse loomist, mis parandaks riiklikul tasemel koordineerimist ja valdkonna ekspertide koostööd, ning teha analüüsist lähtuv otsus hiljemalt 2027. aastal.
- KJN peab regulaarselt seirama käesoleva strateegia eesmärkide poole liikumist ja selleks võetavaid meetmeid, sealhulgas eesmärkide uuendamist.
- Koos partnerasutustega tuleb hinnata küberturvalisuse 2. direktiivi ülevõtmist, ühtlustada kehtivaid küberturvalisust ja andmekaitset reguleerivaid õigusakte (RSVS, avaliku teabe seadus, elektroonilise seadus jt). Samuti tuleb KüTS-i ajakohastada, mille käigus hinnatakse ja korrastatakse kohustatud isikute ringi ning kohustuste ja järelevalvemeetmete proportsionaalsust, vähendades tarneahela ja muid asjakohaseid riske, näiteks luues õiguslikud võimalused selliste meetmete jõustamiseks, mille abil saab senisest operatiivsemalt intsidente ennetada.

Mõõdikud

- Euroopa Liidu Küberturvalisuse Ameti (ENISA) välja töötatud küberindeksi EU-CSI[20] põhjal on Eesti tulemus kõigis mõõdetavates valdkondades vähemalt liidu keskmist kõrgem.
- Eesti kuulub jätkuvalt Rahvusvahelise Telekommunikatsiooni Liidu (ITU) küberturbe indeksi (ingl *global cybersecurity index*) alusel esimese kümne riigi hulka (2020. aastal 3. kohal, hinnatakse iga nelja aasta tagant).
- Küberturvalisuse strateegia eesmärkide rakendamise iga-aastane ülevaade KJN-is. – Jah/ei.
- Küberturvalisuse pädevust ja riiklikku koordinatsiooni on analüüsitud ja otsus tehtud. – Jah/ei.
- KüTS-i revisjon on läbi viidud ja seadust rakendav sihtrühm on korrastatud. – Jah/ei.
- Euroopa ja NATO küberturvalisuse direktiivid on Eesti üle võtnud. – Jah/ei.

2.2. Küberturbe rahastamine

Olukord

Eelmise strateegia valmimise ajal oli Eesti küberturvalisuse korraldus selgelt alarahastatud ning projektipõhine. Aastatel 2020–2024 kasvas riigi digiühiskonna arengukava maht 52,6 miljonilt eurolt 149 miljoni euroni ning küberturvalisuse osa sellest kasvas 3,9 miljonilt (7,4%) 16,1 miljoni euroni (10,8%).[21]

Muutunud julgeolekuolukorra tõttu on ministeeriumitel, nende valitsemisala asutustel ja põhiseaduslikel institutsioonidel võimalik kasutada Vabariigi Valitsuse reservist vahendeid ettenägematuteks kulutusteks ja küberturvalisuse taseme tõstmiseks MKM-i poolt heaks kiidetud tegevuste rahastamisel.[22]

Eesti erasektori küberturvalisuse rahastamine on jätkuvalt ebapiisav ning ettevõtted mõistavad tihti alles pärast küberintsidendi esinemist, et nad pidanuks juba varem küberturvalisusesse investeerima. Selleks, et ka väiksemad ja keskmise suurusega ettevõtted panustaksid oma küberturvalisusesse rohkem, on RIA koostöös EAS-i ja KredExi ühendasutusega 2023. aasta märtsist pakkunud katseprojekti raames küberturvalisuse taseme kaardistamise ja arendamise toetust. Toetusmeetme üks oluline nõue on taotleja

[20] EU Cybersecurity Index, https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/eu-cybersecurity-index.
[21] Andmed pärinevad 2020.–2024. aasta riigieelarve seadustest.
[22] Vabariigi Valitsuse reservist vahendite eraldamise ja eraldatud vahendite kasutamise kord, https://www.riigiteataja.ee/akt/112022019004.

omaosalus. Niimoodi innustatakse erasektorit ka omalt poolt panustama küberturvalisusesse, edendades samal ajal küberturvalisuse teenuste turgu. Taoliste meetmete loomine, arendamine ja püsimine aitab suurendada küberturvalisuse rahastamist erasektoris, kuid nimetatud katseprojekt saab 2024. aasta septembris läbi.

Küberturvalisuse kompetentsi kasvatamine toimub samuti projektipõhiselt. 2022. aastast on RIA täitnud Euroopa küberturvalisuse kompetentsikeskuste võrgustiku Eesti riikliku koordinatsioonikeskuse (NCC-EE) rolli, edendamaks küberturvalisuse tööstuse, tehnoloogia ja teaduse arengut. Üks keskuse eesmärke on tuua Eesti kübervaldkonna ettevõtetesse rahvusvahelisi teadusgrante ja investeeringuid. Selleks on NCC-EE-d seni rahastatud projektipõhiselt Euroopa Liidu vahenditest, aga ka teadus- ja arendustegevuse ning innovatsiooni ja ettevõtluse (TAIE) arengukava vahenditest. Samamoodi projektipõhiselt on rahastatud ka näiteks noorte küberharidust, talentide poliitikat ja täiendõpet, tihti üksnes sellisel juhul, kui eestvedajad suudavad Euroopa Liidu projekti jaoks mõne ministeeriumi eelarvest omaosaluse leida.

Sihtotstarbelisest reservist on taotletud vahendeid Euroopa Liidu direktiivide ülevõtmisega seotud kulude kompenseerimiseks KüTS-i subjektidele ja asjaomase valitsemisala asutustele, kelle ülesanded muutuvad.

Tugevad ja nõrgad küljed

Senise suuresti projektipõhise rahastamismudeli asemel tuleb kindlustada püsiv rahastus olemasolevate riiklike küberteenuste käitamiseks, edasiseks arendamiseks ning leida lisavahendeid uute vajaduspõhiste teenuste väljaarendamiseks ja uutest Euroopa Liidu õigusaktidest[23] riigile tulenevate kohustuste täitmiseks.

Avaliku sektori asutuste kulutused küberturvalisusele on väga erinevad ning ühtset metoodikat kulude piisavuse hindamiseks on keeruline välja töötada. Oluline on parandada avaliku sektori teadlikkust, et IT-valdkonna eelarve sisse on ääretult vajalik panustada küberturvalisuse eelarvesse. See teadmine on vajalik erasektorilegi – nii neile, kes on seadusega kohustatud küberturvalisusega tegelema, kui ka neile, kes teevad seda lähtudes turumajanduslikust vajadusest.

Riigil on võimalik küberturvalisuse poliitikat kujundada eeskuju näidates ja suurkliendi rollis olles. Toetused ja rahastustaotlused, mis on mõeldud digitaliseerimisele, peavad arvestama ka küberturvalisuse komponentidega seotud kulu. IT-hangete ja koostöölepete puhul tuleb muu hulgas lisada julgeolekuolukorrast lähtuvad küberturvalisuse nõuded, hoidmaks või parandamaks teenuste turvataset, samuti tuleb rakendada riskihindamist, pöörata tähelepanu tarneahela rünnakutele ning seirata, turvatestida ja kontrollida lepingus fikseeritud nõuete täitmist.

Eesmärgid, milleni soovime strateegiaperioodil jõuda

- Tagada eelarvevahendite piisavust teenuste turvaliseks käitamiseks ja arendamiseks.
- Riigi küberturvalisuse baasteenuste rahastamine on pikaajalist planeerimist võimaldaval tasemel järjepidevalt tagatud kokkulepitud tasemel.

Nende eesmärkide saavutamiseks vajalikud tegevused

- Analüüsida MKMi poolt tellitud kulumudeli rakendamist Eestis ja alg- ning sihttaset eesmärkide saavutamiseks[24].

[23] Vt peatükk 2.1. „Valdkonna juhtimine ja poliitika kujundamine“.
[24] Küberturbe kulumudel_v2.0.pdf (mkm.ee)

- Analüüsida sobivat riigi küberturvalisuse komponendi sihttaseme suurust, mida avaliku sektori asutused peavad oma IKT eelarvesse planeerima.
- Töötada välja kübervaldkonna teadus- ja arendustegevuse ning innovatsiooni ja ettevõtluse (TAIE) pikaaegne plaan, mis arvestaks ka küberturvalisuse strateegia eesmärke.

Mõõdikud

- Küberturvalisuse baasteenuste rahastus on ette nähtud riigieelarve vahenditest. – Jah/ei.

3. ÜHISKONNA KERKSUSE SUURENDAMINE

Eesti ühiskonna, inimeste, asutuste, ettevõtete ja eluviisi kaitsmine küberohtude eest on seda edukam, mida laiapindsemalt ning mõtestatumalt sellega tegeletakse. Küberturvalisuse ohtude, riskide ja meetmete puhul tuleb arvestada nii olemasolevaid kui ka tulevikkus tekkida võivaid tehnoloogilisi ohte. Küberjulgeolek on oluline igas tehnoloogia sektoris, alates koduelektroonikast ja lõpetades kosmosetehnoloogiaga. Valdkondlik areng peab arvestama riiklikke võimeid, infoturbe arengu seiret ja küpsushindamist, mis omakorda pakub tuge riigiülesele kriisijuhtimisele ja riikliku julgeoleku tagamisele. Erinevad sihtgrupid vajavad erinevat lähenemist ning oma rolli mängivad ka piiratud ressursid.

3.1. Ajakohane ohupilt

Olukord

Pidev valmisolek kaitsta Eesti digiriiki ja -ühiskonda ning meie inimestele viimaste aastakümnetega harjumuspäraseks saanud eluviisi sõltub suuresti sellest, kui teadlik on riik küberruumis toimuvast. See hõlmab arusaamist tegelikest ja võimalikest ohtudest, tehnoloogia arengust ning rahvusvahelistest suhetest lähtuvatest trendidest. Praegu näeb RIA väljaspool riigivõrku ja KüTS-i kohuslasi aset leidvatest intsidentidest ainult jäämäe tippu, mistõttu tuleb olukorrateadlikkust parandada. See aitaks võimalikult laia kasutajaskonda esilekerkivatest ohtudest senisest kiiremini ja täpsemalt teavitada ning nende võrgu- ja infosüsteemide kaitseks võimalikult täpsed praktilised juhised koostada.

Näiteks tehakse üha sagedamini ründeid terviseasutuste vastu, kuna küberkurjategijad sihivad eelkõige selliseid organisatsioone, mille süsteemid on elutähtsa mõjuga ning sisaldavad mahukaid ja tundlikke andmeid. Euroopa Liidu digikümnendi strateegias on üks keskseid 2030. aastaks seatud eesmärke see, et liidu kodanikel oleks täielik juurdepääs oma digitaalsele terviseloole, mis prioriseerib terviseteenuseid.

Tugevad ja nõrgad küljed

Riigi keskne küberturbe ohupildi analüüsija ning sellest riigiasutuste, ettevõtete ja avalikkuse teavitaja on RIA. Valitsuse tasandile jõuavad küberohupildiga seotud küsimused harvem, kui tänane geo- ja julgeolekupoliitiline olukord lubaks eeldada. Kuigi koostöö riigiasutuste ja erasektoriga on tihe, on RIA kui keskse küberasutuse tasandil puudu täielik sektoriaalne ja üleriigiline küberohupilt, mille olemasolu avardaks märkimisväärselt ohtudealast vaatevälja.

Eesmärgid, milleni soovime strateegiaperioodil jõuda

- Küberohtude võimalikult kiireks ennetamiseks, tuvastamiseks ning tõkestamiseks loob RIA Eesti küberruumi kohta tervikliku ohupildi, mis võimaldab eri ühiskonnagruppidele senisest paremini ennetusalast tuge pakkuda.
- Vabariigi Valitsus, Riigikogu, ministeeriumid, riigiasutused, ettevõtted ja tavakasutajad on tänu terviklikumale ohupildile ja tegevusjuhistele teadlikumad küberruumis valitsevast olukorrast, neid on juhendatud kaitsemeetmeid rakendama ning asutused mõistavad paremini, miks ja kuidas oma teavet küberohtude eest kaitsta.

Nende eesmärkide saavutamiseks vajalikud tegevused

- MKM-il ja RIA-l tuleb internetiteenuse pakkujatega kokku leppida, kuidas oleks kõige otstarbekam küberohupilti anonümiseeritud kujul luua, arvestades isikute põhiõigusi ja ettevõtlusvabadust.

Mõõdikud

- Üleriigilise ohupildi loomisse panustavate asutuste ja ettevõtete asjaomased õigused ja kohustused on kokku lepitud. – Jah/ei.
- Üleriigiline küberohupilt jõuab sihtrühmadeni senisest täielikumal kujul. – Jah/ei.

3.2. Laiapindne ennetus

Olukord

Küberohtude pideva arengu ja kasvuga toimetulekuks on vaja, et kõik ühiskonnaliikmed oleksid neist teadlikud ning oskaksid võimalikke intsidente ennetada. Ilmselt ei ole võimalik saavutada sajaprotsendilist edu, kogu elanikkonda korraga uuele tasemele viia ei ole võimalik. Elanikkonna harimine on tõhus läbi sihistatud kampaaniate. Oluline sihtgrupp on noored, kelle käitumisharjumusi aina varem mõjutades väldime probleemide kasvu tulevikus.

Ühiskonna turvalisuse kindlustamisel on oluline panustada eri sidusrühmade, sealhulgas ettevõtete ning avaliku sektori töötajate ja võtmeisikute, aga ka laiema elanikkonna küberteadlikusse käitumisse. Üks tõhusaid meetmeid on iga-aastane kübertest, mille läbimine tuletab meelde hea tava ja turvalise käitumise põhialused. 2023. aastal, kui RIA kübertesti käiku lasi, läbis selle üle 15 000 inimese, mida võib pidada heaks tulemuseks. Ka erasektor pakub võimalusi kontrollida ja täiendada oma küberturbeteadmisi. Organisatsioonides on kindlasti vaja tagada, et töötajad oleksid infoturbereeglitega kursis.

Laiapindse ennetuse kaudu kujundatakse kõigi osapoolte ohuteadlikku käitumist, et küberkuritegevust ja küberintsidente ära hoida või nende mõju vähendada. Sotsiaalreklaami kasutamine ning mõjuisikute kaasamine on suurendanud küberturvalisuse nähtavust. Kõikide meetmete koosmõjuna oli 2023. aasta septembri seisuga Eestis alla 10% neid, kes ei olnud võtnud ühtegi meedet, et küberruumis oma isiklikku turvalisust või privaatsust tagada.[25]

Tugevad ja nõrgad küljed

Küberturvalisusealane teadlikkus on riigi ja erasektori võtmeisikute hulgas endiselt ebapiisav ning vajab edendamist ka ühiskonnas laiemalt ennetamaks küberintsidente ja küberkuritegude ohvriks sattumist. Küberturvalisuse tagamist ei tajuta isikliku vastutusena ega organisatsiooni põhitegevuse riskina, vaid sellesse suhtutakse enamasti kui mingisugusesse keerukasse tehnilisse teemasse, millega peab tegelema keegi teine.

Väikese ja keskmise suurusega ettevõtete (VKE) teadlikkus küberruumis levivatest ohtudest on väike, samuti ei tee VKE-d piisavalt investeeringuid küberturvalisuse parandamiseks ega võimalike tarneahela

[25] Statistikaameti uuring „Infotehnoloogia leibkonnas 2023. aastal“. Seda küsimust küsitakse RIA tellimusel ja tulemused ei ole Statistikaameti veebilehel avalikult nähtavad.

riskide vähendamiseks.[26]

Küberohtude kasvu ning esemevõrgu (IoT) kiire laienemise tõttu suureneb kõigi küberruumis toimijate vastutus küberturvalisuse tagamise eest. Endiselt ei rakendata piisavalt küberhügieeni parimaid praktikaid ega minimeerita oma seadmete kuritarvitamise võimalusi.

Eesmärgid, milleni soovime strateegiaperioodil jõuda

- Laiapindse ennetuse tulemusena on Eesti ühiskond küberteadlik. Kõigil küberruumis tegutsejatel on vajalikud teadmised ohtudega toimetulekuks ning intsidentide ennetamiseks.
- Elanikkonna küberhügieeni tase on tõusnud ning vähenenud on nende elanike hulk, kes ei ole küberruumis oma isikliku turvalisuse või privaatsuse tagamiseks astunud mitte ühtegi sammu.
- Küberkuritegude arv on Eestis laiapindse ennetuse ning RIA ja PPA koostöö tulemusena vähenenud.
- Kasvanud on avaliku ja erasektori, sh VKE-de võtmeisikute teadlikkus küberturvalisuse olulisusest organisatsiooni põhitegevuse tagamisel.
- Küberturbeteadlikkuse testid on riigiasutuste, elutähtsate teenuste osutajate ning ettevõtete töötajate hulgas nende küberteadmiste testimiseks ja täiendamiseks laialdaselt kasutusel.

Nende eesmärkide saavutamiseks vajalikud tegevused

- Koostöös Haridus- ja Teadusministeeriumiga on vaja arendada digi- ja küberoskusi kõigis vanuserühmades.
- Tuleb hinnata mõjupõhiselt küberkuritegevuse trende, nendest lähtuvalt arendada vastavat tehnoloogilist võimekust ja oskusi ning rakendada muid meetmeid ühiskonna kaitsmiseks ja teadlikkuse parandamiseks.
- Ühiskonnas tuleb teadvustada valitsevaid küberohte ja igaühe vastutust nende vähendamisel. Jagada nõuandeid riskide maandamiseks.
- Koostöös erasektoriga on vaja töötada välja VKE-de küberteadlikkust parandavaid meetmeid ja neid ellu viia.
- Avaliku sektori keskselt hallatavatele seadmetele juurdepääsu saamiseks peab kasutaja läbima esmalt kübertesti.

Mõõdikud

- Turvariski tõttu e-teenustest hoidumine. – Alla 10% (allikas Statistikaamet).
- Üle 90% elanikkonnast on võtnud oma isikliku turvalisuse või privaatsuse tagamiseks vajalikke meetmeid.[27]
- Küberkuritegude arv väheneb.

3.3. Infoturbestandardi rakendamine

Olukord

2022. aastal jõustusid ühiskonna toimimise seisukohast olulistele süsteemidele kehtestatud nõuded, mille lahutamatuks osaks on infoturbestandardite – Eesti infoturbestandardi (E-ITS) ja ISO/IEC 27001 – rakendamine. E-ITS on RIA loodud eestikeelne infoturbesüsteem, mis on kooskõlas Eesti õigusruumiga ning ühtlasi rahvusvahelise standardiga ISO/EC 27001. E-ITS jõustus 2022. aasta detsembris ja enamik kohuslasi

[26] Statistikaameti uuring „Infotehnoloogia ettevõttes 2022. aastal“. Neid andmeid ei koguta RIA tellimusel ning need on Statistikaameti veebilehel avalikult nähtavad.
2022. aastal RIA tellimusel Kantar Emori tehtud uuring „Küberturvalisus ettevõttes“. Uuring ei ole avalikult nähtav.
[27] Statistikaameti uuring „Infotehnoloogia leibkonnas“. Seda küsimust küsitakse igal aastal RIA tellimusel ja tulemused ei ole Statistikaameti veebilehel avalikult nähtavad.

on asunud seda rakendama. RIA kogub standardi rakendajatelt tagasisidet ja soovitusi, kuidas seda ajakohastada ja parandada.

Tugevad ja nõrgad küljed

E-ITS-i meetmete suur hulk toob organisatsioonidele kaasa arvestatava halduskoormuse, eriti esmakordsel infoturbe rakendamisel. Standardi modulaarne olemus võimaldab selle kasutusele võtta ükskõik kui suurtes või väikestes organisatsioonides. Samas võib väiksema organisatsiooni puhul osutuda probleemiks infoturbeoskustega töötajate puudumine, mille tagajärjel võib mahuka haldussüsteemi rakendamine takerduda. Seetõttu on rakendajad oma tagasisides toonud välja ootuse selliste lahenduste väljatöötamiseks, mis hõlbustaksid E-ITS-i kasutuselevõttu just väiksemates organisatsioonides. Samuti on meetmete rakendamise ja selle kontrollimise lihtsustamiseks vaja tulevikus leida automatiseeritud lahendusi.

Infoturbestandardi rakendamise tulemusena saab asutus tervikliku ülevaate oma küberturbe olukorrast ja riskidest. Samas on senine kogemus välja toonud, et sugugi mitte kõik, kes peaksid infoturbestandardit rakendama, ei ole sellest teadlikud ning on neid, kes rakendavad meetmeid eelkõige formaalselt, sisulistesse riskidesse süvenemata. Probleem on ka see, et tarneahela organisatsioonid ei ole huvitatud lõimitusest infoturbe süsteemsesse rakendamisse ning vahendeid nende mõjutamiseks on vähe.

E-ITS on Eesti oludega arvestav standard, ent kuna seda pole veel rahvusvaheliselt tunnustatud, võib organisatsioonidel tekkida vajadus rahvusvaheliselt tunnustatud ISO/IEC 27001 sertifikaadi järele. Vaja on leida võimalusi, kuidas E-ITS-i ja ISO/IEC 27001 omavahel paremini sobitada.

Eesmärgid, milleni soovime strateegiaperioodil jõuda

- Organisatsioonid ja nende juhid on teadlikud oma infoturbekohustustest ning rakendavad teadlikult turvameetmeid, lähtudes riskipõhisest mõtteviisist, ja nõuavad seda ka oma tarneahelalt.
- E-ITS-i on igal aastal koostöös kogukonnaga uuendatud. Tegemist on Eesti õigusaktidega kooskõlas oleva kogukondliku standardiga, mis arvestab uusi ohte ja tehnoloogia arengut.
- Organisatsioonid, kellel on vaja tõendada oma infoturbehalduse süsteemi toimimist rahvusvahelisel tasemel, saavad seda teha ka E-ITS-i rakendades ja E-ITS-i auditit läbides.

Nende eesmärkide saavutamiseks vajalikud tegevused

- Vaja on tugevdada E-ITS-i positiivset kuvandit sektoripõhiste eestkõnelejate abil.
- Vaja on laiendada infoturbestandardi koolituste pakkumist, kaasates ka erasektorit.
- Vaja on välja töötada lahendused E-ITS-i meetmete rakendamise automatiseerimiseks, et hõlbustada E-ITS-i kasutuselevõtu väiksemates asutustes ja organisatsioonides.
- Organisatsioonidele tuleb luua võimalused E-ITS-i rakendamist ja toimivust mõõta ning mõõtmistulemuste põhjal hinnata E-ITS-i rakendamise tulemuslikkust eri tüüpi asutuste lõikes
- Tuleb analüüsida küberohtude ja tehnoloogia arengut ning korrastada kaitsemeetmeid E-ITS-i uuendamisel.
- Analüüsi põhjal tuleb luua E-ITS-i ja ISO/IEC 27001 sertifikaadi vaheline vastavusmehhanism ning taotleda E-ITS-i rahvusvahelist tunnustamist.

Mõõdikud

- E-ITS-i on igal aastal vastavalt ohupildile uuendatud ja seejuures on arvestatud parimaid rahvusvahelisi praktikaid. – Jah/ei.
- E-ITS-i rakendamise tulemusena on 2027. aastaks selliseid asutusi, kellel esineb infoturbes olulisi puudujääke, vähemalt 50% vähem. – Hinnang antakse RIA järelevalvemenetluse põhjal.

3.4. Turvaline alusarhitektuur ja nüüdisaegsed turbepõhimõtted

Olukord

Kuna kaitstavate andmete ja infosüsteemide hulk aina suureneb, aga terviklik ohupilt pigem halveneb, liigub tänapäeva infoturve üldiselt selles suunas, et vältida turvaintsidentide jõudmist lõppkasutajani nii palju, kui see on vähegi võimalik. Intsidentide tekkimisel peaks kaasnev kahju olema võimalikult väike ja hallatav. Riigi seisukohast tähendab see suurema tähelepanu pööramist turbeaspektidele teenuste arendamise ja nende elutsükli jooksul kui ka seismist selle eest, et valitsusasutused järgiksid nüüdisaegseid turbepõhimõtteid ja kasutaksid uusimaid turbelahendusi.

Kõik arendused peavad lähtuma lõimturbe (ingl *security-by-design*) põhimõttest, mille korral on turvalisust arvestatud juba teenuse- või tootearenduse algetappides. Näiteks tarkvaraarenduses tuuakse turvalisusega seotud aspektid esile juba projekteerimisel, mitte ei lisata neid hilisemas etapis või pärast tarkvara kasutuselevõttu. Sellise lähenemise korral on turvalisus integreeritud läbivalt, kogu tarkvara elutsükli jooksul – alates nõuete kindlaksmääramisest kuni projekteerimise, arendamise, testimise, turuletoomiseni. Rakendades on võimalik turvariske oluliselt kahandada, parandada tarkvara üldist kvaliteeti ning vähendada kulutusi, mis tekiksid turvanõrkuste kõrvaldamisest toote turuletoomise järel.

Kiire tehnoloogiline areng ning esemevõrgu (IoT) laienemine põhjustab omakorda uute küberohtude teket. Kvantarvutite tulek kujutab potentsiaalset ohtu praegustele krüptograafilistele algoritmidele, kuna need arvutid suudavad lahendada keerulisi arvutusi palju kiiremini kui tavalised arvutid. See võib tulevikus ohustada laialdaselt levinud digitaalse turvalisuse meetodeid, mistõttu on oluline arendada kvantarvutitele vastupidavaid krüptograafilisi lahendusi, et tagada andmete püsiv turvalisus.

Tugevad ja nõrgad küljed

Paarikümne aasta pikkuse ajalooga Eesti digiriigis on tänapäeval nii avalikus kui ka erasektoris kasutusel palju vananenud süsteeme ehk taakvara (hinnanguliselt 40% avalikest e-teenustest). Taakvara (ingl *legacy*) on infosüsteem, tehnoloogia või tarkvara, mis endiselt töötab, aga ei vasta enam tänapäevastele infoturbe- ja andmekaitsenõuetele. Sageli ei ole selliste teenuste omanikel ka täielikku ülevaadet nende arhitektuurist, sõltuvusseostest ja peamistest nõrkustest, sest puudub vajalik dokumentatsioon. Süsteeme hoitakse käigus, ent pikemas perspektiivis ei ole need jätkusuutlikud. Ka täna arendatavad teenused võivad mõne aasta pärast muutuda taakvaraks, kui nende elukaar ja uuendamise vajadused ei ole kohe algusest peale terviklikult läbi mõeldud.

Peale taakvara on avaliku sektori infosüsteemidesse kogunenud aja jooksul ka palju digikeltsa. See hõlmab ebavajalikke faile, kasutusest kõrvale jäetud rakendusi, vananenud seadmeid ja muud taolist, mille säilitamine kulutab tarbetult palju andmemahtu ning võib kätkeda ka turvariske. Ehkki mõnes valitsemisalas korraldatakse juba praegu regulaarseid digikoristuspäevi, tuleks seda praktikat laiendada (nt erasektori algatatud üle-eestilise digikoristuspäeva[28] raames).

Tulevikus ilmneda võivate ohtude leevendamiseks osaleb Eesti rahvusvaheliste projektide koostöös ning oleme seotud kvantarvutite ja sensortehnoloogia uurimisrühmadega. Eesti digiriigi toimekindluse tagamiseks peavad kasutusel olevad turbelahendused olema usaldusväärsed ja ajakohased, mistõttu rakendatavate turvameetmete hindamine nõuab teaduspõhist lähenemist ning krüptograafia kompetentsikeskuse loomist. Nii Eesti õigusruumist tulenevalt kui rahvusvahelise nõudena on küberturvalisuse vaates oluline hinnata süsteemides kasutatavate turbelahenduste, sh krüptograafia ja

[28] Vikipeedia artikkel „Digikoristuspäev“, https://et.wikipedia.org/wiki/Digikoristusp%C3%A4ev.

selle rakendamise vastavust nõuetele. Iseseisev võimekus selles valdkonnas Eestil puudub. Riigina toetume teiste riikide hindamistele, mis toob kaasa nii ajalise kui ka rahalise kulu. Eesti riik on selles valdkonnas esimesi samme tegemas, et riigina tekiks meil esmane iseseisev sideturbelahenduste hindamisvõimekus aastaks 2026.

Pilvetehnoloogia arengu, tarneahela riskide ja hübriidtöökohtade üha laialdasema leviku tõttu vajavad uut lähenemist ka võrguturbe põhimõtted. Klassikalise lähenemise kohaselt keskendub võrguturve väliste ohtude vastu kindlustamisele, ent äsja nimetatud suundumuste tulemusena on piir võrguturbe mõistes „sisemise“ ja „välimise“ vahel hägustunud ning kaitstakse mõlemat. Seetõttu on mitmed riigid (nt USA, Jaapan, Saksamaa ja Prantsusmaa) liikumas aina enam niinimetatud täisusaldamatuse turbemudeli poole. Selle mudeli kohaselt ei usaldata vaikimisi mitte kedagi ning mistahes ressursi kasutamiseks on vaja iga kasutaja tuvastada ja veenduda tema õiguses ressurssi kasutada. Sellist lähenemist toetab asjaolu, et andmed liiguvad üha enam mitmesugustesse pilvelahendustesse, kus turbemeetmete rakendamine on teenusepakkuja ja teenuse kasutaja vahel hajutatud.

Turvalise alusarhitektuuriga seondub ka internetiprotokolli teema. Olemuselt on internetiprotokoll (IP) tehniline lahendus, mis võimaldab internetis andmevahetust internetiprotokolli aadresside ehk IP-aadresside põhjal. 1980. aastate algusest kasutusel olev internetiprotokoll IPv4 hakkab moraalselt vananema, mille üks ilminguid on see, et enam ei jätku unikaalseid IP-aadresse. Seetõttu kasutab mitu erinevat seadet üht ja sama aadressi, mis on infoturbe seisukohast aga taunitav. Lahenduseks on uue põlvkonna internetiprotokolli IPv6 kasutuselevõtt, mida Eestis erasektor tasapisi ka juba teeb (nt Telia). Paljud riigid (sh India, USA ja Hiina) on liikumas ainult IPv6-põhiste teenuste poole. Ka Eesti peab riiklikul tasandil esitama oma IPv6-alase ambitsiooni, kuna meie konkurentsivõime ja turvalisuse säilitamiseks on see vajalik.

Eesmärgid, milleni soovime strateegiaperioodil jõuda

- Strateegiaperioodi lõpuks on vähenenud riigi olulise tähtsusega andmekogude ja teenuste sõltuvus taakvarast vähemalt poole võrra.
- Avaliku sektori asutused vähendavad süsteemselt digikeltsa.
- Avalikus ja erasektoris rakendatakse elutsüklipõhist arendus- ja turvapoliitikat, mis on osa igast tehnoloogia arendamise etapist ning tagab turvanõuete pideva arvestamise kuni rakenduse kasutuselt kõrvaldamiseni.
- Avalikus sektoris on kehtestatud selged infoturbenõuded ja IT-teenuste korraldamise miinimumnõuded (keskhaldus, keskselt reguleeritud avalike pilveteenuste kasutamine jms), mille ajakohasust KJN-is regulaarselt seiratakse.
- Olla valmis uute tehnoloogiate (sh kvantarvutuse) tulekuks, arvestades tehnoloogilisi suundumusi.
- Kasvatada riiklikku krüptograafiaalast teadmust ja pilveteenuste rakendamise kompetentsi.
- Riiklik teave on hoitud heaks kiidetud/sertifitseeritud kvantkindlate sideturbe (sh krüpto-) lahendustega.
- Eestis on olemas kvanttarkvara arendamiseks vajalik võimekus ja huvi, et kuuluda Euroopa kvantökosüsteemi.
- Kogu strateegiaperioodi jooksul liiguvad keskvalitsusasutused täisusaldamatuse turbearhitektuuri suunas.
- Järjepidevalt kaasajastatakse digitaalsete teenuste turvaintsidentide ennetamise võimekust internetiprotokolli IPv6 rakendamise kaudu. Aegunud tehnoloogiad eemaldatakse kasutuselt.

Nende eesmärkide saavutamiseks vajalikud tegevused

- Rahastustaotluste ja -otsuste tegemisel tuleb prioriseerida taakvara vähendamist.
- Avaliku sektori asutustel tuleb seada eesmärgid digikeltsa vähendamiseks ning osaleda iga-aastastel digikoristuspäevadel.
- Riigi uute digitaalsete teenuste arendamisel ja olemasolevate teenuste uuendamisel tuleb lähtuda lõimturbe põhimõttest ja mittefunktsionaalsete nõuete rakendamisest. See tähendab, et teenuste kavandamisel ja arendamisel võetakse igas etapis arvesse turvalisuse riske ning teenuse või toote elukaar planeeritakse terviklikult, kooskõlas E-ITS-i meetmetega.
- Vaja on luua teaduslikud kompetentsikeskused pilvetehnoloogiate ja krüptograafiliste lahenduste rakendamiseks, et tagada andmete kvantkindlus.
- Riiklikult lepitakse kokku ja kiidetakse heaks krüptograafiat sisaldavate andme- ja sideturbelahenduste hindamise metoodika ja selle rakendamist.
- Tuleb uurida tehnoloogilisi suundumusi ja tulevikutehnoloogiaid, sealhulgas tehisaru ja kvanttehnoloogiaid, jagada parimaid praktikaid ning töötada välja nende rakendamise meetmed.
- Järk-järgult tuleb juurutada täisusaldamatuse turbeprintsiipi.
- Strateegiaperioodi jooksul tuleb hinnata riigi enim kasutatavate digitaalsete teenuste ühilduvust uue põlvkonna internetiprotokolliga IPv6 ning luua teekaart IPv6 rakendamiseks avalikus sektoris.

Mõõdikud

- 2030. aastaks on avalike teenuste sõltuvus taakvarast (avaliku võrgu kaudu tarbitavate teenuste puhul) vähenenud 20%-ni.
- Kehtestatud on IT-teenuse korraldamise miinimumnõuded. – Jah/ei.
- Riigis on pandud alus krüptograafia ja pilveteenuste kompetentsikeskustele. – Jah/ei.
- Teadus- ja arendustegevuse uuringud ja analüüsid on läbi viidud ning tulemused on rakendatavad. – Jah/ei.
- 2030. aastaks on täisusaldamatuse arhitektuuri küpsusmudeli järgi saavutatud edasijõudnu tase (CISA kasutatavas küpsusmudelis[29] tase „Advanced“).
- 2030. aastaks on avalikult tarbitavatest riigi e-teenustest vähemalt 80% IPv6 võrgus.

3.5. Elutähtsate teenuste kriisikindluse suurendamine

Olukord

Mitmed hiljutised kriisid on tõestanud, et elutähtis taristu ja elutähtsad teenused on konflikti osapoolte jaoks oluline sihtmärk. Lähis-Idas 2023. aastal intensiivistunud konflikt mõjutas esimest korda otseselt Eestit tööstusautomaatika ründamise kaudu. Venemaa sõda Ukrainas ei ole jätnud kahtlustki, et võimalik vastane võib vajaduse korral kahjustada tahtlikult meie elutähtsat taristut. Tööstuse automatiseerimine on viimastel aastatel saanud hoogu juurde, kuid sageli puuduvad operaatoritel piisavad teadmised küberohtudest ja küberturvalisusest. Seni on arutelu olnud pigem teoreetiline, kuid nüüd on ka praktiline näide ja kogemus muu hulgas käsitsi juhtimise alternatiivi säilitamise, käsitsi juhtimisele ülemineku planeerimise ning õppustel läbiharjutamise vajalikkusest olemas.

Rünnakud taristule ja riigi toimimiseks olulistele süsteemidele ei ole ainult konfliktidest tingitud, ründeid toimub ka muul ajal. Rünnaku taga võib olla vaenulik riik või kuritegelik rühmitus. Kõikidel juhtudel püüab ründaja tekitada olukordi, mille kahjulik mõju oleks võimalikult suur. Selliste olukordade ettenägemine ning adekvaatse küberkaitse loomine on reeglina tulemuslikum, kui organisatsioonis on küberturvalisus

[29] Vt lähemalt https://www.cisa.gov/zero-trust-maturity-model.

juhtkonna tasemel seiratav ning küberriske peetakse äririskide osaks. Leidub ka suuri ETO-sid, kus küberturbejuhti ei ole või täidab seda funktsiooni taristujuht.

Tänases julgeoleku olukorras, elutähtsate teenuste osutamisel ei piisa enam tavapärasest toimepidevuse tagamisest, vaid peame olema valmis ka riigikaitselisteks stsenaariumiteks.[30] Eesti on seni suutnud kübervaldkonna intsidentidele ja kriisidele reageerida adekvaatselt. Omandatud õppetundidest on tehtud järeldusi ning võetud ennetavaid meetmeid. Valdavalt on kriisiõppustes kajastatud ka küberaspekt ning kriisiplaanide tegemisel on teadvustatud IKT-lahenduste toimimise olulisust ja infovarade kaitset.

Üks viimaste aastate suurimaid uuendusi on RIA küberreservi loomine 2022. aasta sügisel. Kui 2017. aasta detsembris ID-kaardi kriisi ajal õnnestus RIA-l *ad hoc* baasil kaasata kriisi lahedamisse pädevaid isikuid nii avalikust kui ka erasektorist, siis nüüdseks on loodud ja läbi proovitud maailmas seni ainulaadne küberreservi süsteem.[31]

Tugevad ja nõrgad küljed

Keskne seire võimaldab Eesti küberruumis tuvastada haavatavaid seadmeid ja süsteeme. Paraku ei ole leitud veel tõhusat lahendust, kuidas probleemsete omanikega ühendust võtta ning veenda neid viivitamata olukorda parandama.

Küberturvalisuse nõuded on riiklikult kehtestatud väga laiale ringile avaliku sektori organisatsioonidele, elutähtsate teenuste osutajatele ja erasektori ettevõtetele. Infoturbenõuded ja IT-teenuse korraldamise miinimumnõuded ei lähtu ühtsetest põhimõtetest ning ühiskonna küberturvalisuse taset ei ole võrreldavate kriteeriumite alusel ETO-de, elutähtsa taristu ja KüTS-i subjektide lõikes hinnatud. Palju rangeid küberkaitse nõudeid on kehtestatud sellistele ettevõtetele ja avaliku sektori asutustele, mille teenuste mõju ühiskonna toimimisele või sõltuvus küberkomponendist on väike. See killustab niigi piiratud ressursse ega võimalda keskenduda pakilisemate lünkade kõrvaldamisele.

Asutuste ja organisatsioonide juhtkonna arusaamine küberohtudest ning adekvaatsest kaitsest on kasin, tippjuhid ei tunne piisavalt suurt vastutust küberturvalisuse eest ning pahatihti suhtuvad sellesse kui organisatsiooni tegevusega paratamatult kaasnevasse kahjusse.

ETO-de tööstusautomaatika operaatorite ohuteadlikkus on ebapiisav nii riikliku taustaga toimijate kui ka lunavararünnakuid korraldavate kriminaalide osas. Lisaks operaatorite teadlikkuse parandamisele tuleb arendada keskset seirevõimekust just tööstusautomaatika võrkude ja seadmete seire alal.

Riigi kriisihalduses tehtud muudatused ei kajasta adekvaatselt ja tasakaalustatult elutähtsa taristuga seotud küberriske. Teenuse toimepidevuse tagamise üldised meetmed peavad olema tasakaalus kübermeetmetega. Küberturbe komponenti tehtavatel investeeringutel puudub lisandväärtus, kui perimeetri turvalisus puudub või elektrivarustus on ebastabiilne. Samuti ei ole mõtet investeerida taristu füüsilisse kaitsesse, kui ohuteavitustes viidatud turvanõrkustest ei saada jagu piisavalt kiiresti ja ettenähtud meetmeid kasutades. Olemasolevad riiklikud kriisihalduse juhtimismudelid ei kajasta selgeid prioriteete teenuste toimepidevuse tagamisel rahu ja kriisi ajal, teenuste vahelisi ristsõltuvusi ega muid kriisireguleerimisega seotud nõudeid (keskkond, ühenduvus, eskaleerimine jms).

Küberreserv sai loodud väga kiiresti ja protsess on alanud väga edukalt. See aga ei tähenda, et kõik on valmis, pigem vastupidi – terviklikku kontseptsiooni ei ole seni veel kirja pandud ega kokku lepitud.

[30] Riigikaitse arengukava 2022–2031, https://www.riigikantselei.ee/media/1451/download.
[31] Vt https://www.ria.ee/uudised/suur-kuberoppus-pani-proovile-riigi-kuberreservi.

Õppuste käigus on ilmnenud mitmed vajakajäämised, reservi töö korraldamine vajab parandamist ja mõningad protseduurid täpsustamist. Tähelepanu tuleb pöörata küberintsidentide lahendamisele muude kriiside raames ning küberreservi kaasamisele ja lõimimisele muude valdkondade kriisihaldusega.

Eesmärgid, milleni soovime strateegiaperioodil jõuda

- Elutähtsate teenuste turvanõrkuste seiret on tõhustatud ning loodud on olulise tähtsusega võrgu- ja infosüsteemide omanike otseteavitamise võimalus.
- Elutähtsad taristud ja teenused on varustatud riikliku julgeoleku aspektist lähtuvate turvameetmetega, mis võimaldavad vastu seista nii praegustele kui ka tulevastele ohtudele.
- Korrastatud kriisihalduse juhtimismudel arvestab riiklikke võimeid, teenustevahelist ristsõltuvust, prioriteete ja eskaleerimisvõimalusi, et tagada riiklik (küber)julgeolek. Tagatud peab olema oluliste digiteenuste toimepidevus nii rahu kui ka kriisi ajal.
- Rakendatakse küberreservi kontseptsiooni, küberreservi toimimine ja kriiside lahendamisse kaasamine on sujuv.

Nende eesmärkide saavutamiseks vajalikud tegevused

- Vaja on analüüsida võimalusi, kuidas tuvastada olulise tähtsusega võrgu- ja infosüsteemide omanikke (turvanõrkuste põhjal) ning kuidas neid vahetult teavitada.
- Olulise tähtsusega võrgu- ja infosüsteemide omanikke tuleb kohustada ohuteavitustes nimetatud võrgu- ja infosüsteemide turvanõrkusi ettenähtud meetmetega kõrvaldama. Vaja on luua keskne seirevõimekus tööstusautomaatika võrkude ja seadmete jälgimiseks.
- Leppida kokku metoodika ja kriteeriumid, mille alusel diferentseerida küberturvalisuse nõudeid, arvestades teenuse mõju ühiskonna toimimisele.[32]
- Tuleb korrastada kriisijuhtimise õigusruumi ning tagada, et kübervaldkonna kriisimeetmed oleksid proportsionaalsed muude meetmetega.
- Riiklikest võimetest ja stsenaariumitest lähtuvalt täpsustada toimepidevuse nõudeid, kuidas tagada elutähtsate ja digiteenuste kriisikindlus, ning hakata neid rakendama.
- Kriisiolukorraks valmistudes tuleb ette näha küberturbe komponendist sõltumatud lahendused.
- ETO-de toimepidevuse korraldamisel on vaja arvestada laiaulatusliku küberrünnaku võimalusega.
- Toimepidevuse tagamiseks peab olulise tähtsusega süsteemide, sealhulgas tööstusautomaatika puhul jääma alternatiivina alles käsitsi juhtimise võimalus.
- Proovile on vaja panna digiteenuste kriisikindlust ning küberreservi toimimist ja kaasamist, tegemaks kindlaks riiklike võimete piirid, ressursi kvalifikatsioon ja oskuste tase.

Mõõdikud

- Riiklik kriisihalduse juhtimismudel on korrastatud. – Jah/ei.
- Küberintsident ei ole põhjustanud ühegi elutähtsa teenuse pikaajalist katkestust.
- Kõigi olulise tähtsusega infosüsteemide toimimine on taastatud ühe ööpäeva jooksul pärast intsidenti.
- Loodud on küberreservi kontseptsioon. – Jah/ei.

4. TUGEV KÜBERKILP – INTSIDENTIDE SEIRE JA TÕKESTAMINE

IT-vaatlikuma Eesti aluspõhimõte on, et iga inimene käitub küberruumis teadlikult ja vastutustundlikult ning iga infosüsteemi omanik vastutab selle turvalisuse eest. Riiklik küberturvalisuse keskus aitab sellele kaasa, suurendades teadlikkust küberruumis levivatest ohtudest ning pakkudes avaliku sektori digitaalsete

[32] Vt alapeatükk 2.1. Valdkonna juhtimine ja poliitika kujundamine

teenuste kaitseks ajakohaseid tehnilisi meetmeid.

Olukord

Eesti küberruumis toimuvaid turvaintsidente jälgib ja registreerib RIA küberturvalisuse keskuse intsidentide käsitlemise osakond (CERT-EE), kes avaliku sektori intsidentide puhul aitab neid ka lahendada. Võimaluste piires aitab CERT-EE küberintsidente lahendada ka väljaspool avalikku sektorit, eriti aktiivsete ründelainete ajal. Tavaolukorras piirdub abi enamasti standardsete soovituste andmisega ettevõtetele, asutustele ja eraisikutele.

Eesti eripära seisneb selles, et riik pakub riigiasutustele ja kohaliku omavalitsuse üksustele keskset andmesideteenust. Seda nimetatakse riigivõrguks. Ohu suurenedes saab CERT-EE rakendada riigivõrgule lisakaitsemeetmeid, samuti on tagatud tõhus seire riigivõrgus toimuva üle. Mujal Eesti IP-ruumis toimuvat näeb CERT-EE üksnes osaliselt: ohupilt pannakse kokku erinevate tehniliste tööriistade abil ja intsidentide registrisse tulnud teavituste põhjal. Erinevalt riigivõrgust ei ole ülejäänud Eesti IP-ruumis CERT-EE-l võimalik ohu suurenedes lisakaitsemeetmeid võtta.

Tugevad ja nõrgad küljed

Seoses küberturvalisuse 2. direktiivi ülevõtmisega suureneb Eestis nende ettevõtete ja asutuste arv, millele laieneb KüTS ning mis peavad hakkama järgima senisest rangemaid küberturvalisuse nõudeid. See on tekitanud ühiskonnas ootuse, et lisaks õigusaktide kehtestamisele võtab riik suurema rolli ka küberturvalisuse tagamisel. 2022. aastal astuti sel teel esimesed sammud. Nimelt, CERT-EE hakkas pakkuma avalikule sektorile tehnilist lisakaitsekihti ummistusrünnete eest, mille maht on seoses Ukrainas peetava Venemaa agressioonisõjaga mitmekordistunud. Samuti on tõhustatud riigivõrgu üldist vastupidavust erinevat tüüpi küberrünnetele.

RIA võimekus seista keskse asutusena vastu küberohtudele ei ole halb, aga muutunud julgeolekuolukorra ja halvenenud ohupildi tõttu tuleb seda strateegiaperioodil tugevdada. Paranema peab CERT-EE võimekus teavitada Eesti ettevõtjaid ja asutusi olulise tähtsusega turvanõrkustest ning anda konkreetseid soovitusi nende kõrvaldamiseks. Avaliku sektori intsidentide ennetamiseks on peale üldise küberhügieeni taseme hoidmise vaja järjest rohkem tegeleda ka spetsiifiliste ohtude, näiteks täpselt sihitud õngitsuste ennetamisega. Samuti peaks Eesti sarnaselt paljude teiste riikidega kasutama rahvusvahelise eetiliste häkkerite kogukonna abi, testimaks avalikke teenuseid turvanõrkuste suhtes.

Eesmärgid, milleni soovime strateegiaperioodil jõuda

- CERT-i kaitsemeetmete sihtrühm on selgelt prioriseeritud.
- Üleriigiline infoturbe seirekeskus (SOC) on loodud ja toimiv ning ühenduses strateegiliste partneritega.
- Eesti ettevõtete vastu suunatud küberrünnakute õnnestumise tõenäosus on vähenenud tänu paremale sektoriaalsele nähtavusele, automatiseeritud seirele ning ohuteavitusele. Ohte leevendavaid kaitsemeetmeid arendab ja pakub kohalik küberturbesektor.
- Riik pakub tuge vaenulikest riikidest lähtuvate küberohtude ennetamiseks (sh lihtsamad läbistustestid).
- Kriitilise mõjuga turvanõrkusi puudutav info ja nende kõrvaldamise juhised jõuavad õigel ajal elutähtsa taristuni ning Eesti ettevõtete ja inimesteni.

Nende eesmärkide saavutamiseks vajalikud tegevused

- Vaja on rakendada täiendavat kaitsekihti ehk riiklikku küberkilpi prioriseeritud sihtrühmale (nt elutähtsatele teenustele ja taristule).

- Vaja on analüüsida riigikaitse ja julgeoleku aspektist lähtuvalt riigivõrgu sihtrühma.
- Avalikule sektorile tuleb pakkuda optimaalseid keskseid infoturbeteenuseid (nt ummistusrünnete kaitse, keskhaldusega seadmed valitsusasutustes).
- Ohuteadmuse jagamise alal tuleb erasektoriga koostööd teha.
- Kriitilise mõjuga turvanõrkuste kohta on vaja luua hästi toimiv üleriigiline otseteavituste ja järelkontrolli süsteem.
- Järjepidevalt tuleb parandada elutähtsa taristu infoturbejuhtide ja avaliku sektori töötajate küberohualast teadlikkust, arvestades Eestis kasutusel olevat riist- ja tarkvara.
- Vaja on laiendada turvanõrkuste ennetavat otsimist kulutõhusal moel olulisimate avaliku sektori teenuste puhul.

Mõõdikud

- Strateegiliste partneritega toimuv infovahetus on paranenud ja automatiseeritud. – Jah/ei.
- 2030. aastaks seatud sihttase: CERT-EE-lt kriitilise mõjuga turvanõrkuse kohta teavituse saamise järel viib vähemalt 80% adressaate (ettevõtted, asutused) enne järelkontrolli läbiviimist sisse turvauuenduse.

5. TURVALISE KÜBERKESKKONNA KUJUNDAMINE EESTIS JA MUJAL MAAILMAS

Kuigi inimeste arvult ja territooriumilt on Eesti väike, saame mõtestatult tegutsedes suunata küberkeskkonda sobivas suunas mitte ainult kodumaal, vaid palju laiemalt. Lisaks Euroopa Liidu õigusloomes ning poliitiliste protsesside ja strateegiliste suundade kujundamises osalemisele peame proovima edendada samu suundumusi ka globaalselt, ÜRO protsesside ja täpselt sihistatud arengukoostöö kaudu.

Arvestades Eesti ettevõtete ees seisvat digitaliseerimise ja automatiseerimise survet, on mõistlik käsitleda küberturvalisuse olulisust ka kõigi riiklike digitaliseerimist ja automatiseerimist võimestavate meetmete puhul. Endiselt on Eestis ettevõtjaid, kes peavad küberturvalisust ja sellega seonduvat ainult IT-spetsialistide tehniliseks probleemiks. Nad ei pruugi täielikult mõista küberjulgeoleku tähtsust või peavad seda oma äritegevuse puhul mitteoluliseks. Nii avalik sektor kui ka küberturvalisuse organisatsioonid peavad tegema edaspidigi jõupingutusi, et selgitada küberohtude reaalsust, kontrollmeetmete olemust ja nende rakendamise mehhanisme.

5.1. Rahvusvaheline küberkoostöö

Olukord

Eesti silmapaistev digiriigi maine on avanud meile palju erinevaid uksi küberjulgeoleku-alaseks koostööks teiste riikidega. Suuremad digiarengu ja küberjulgeoleku üritused nagu Tallinn Digital Summit, E-riigi Akadeemia (eGA) aastakonverents, CyCON konverents näitavad, et Eesti on jätkuvalt globaalne tõmbekeskus. Eestit külastavad mitmeid delegatsioone ning Eesti esindajatelt oodatakse rahvusvahelistes organisatsioonides kui mitte juhtrolli, siis aktiivset kaasumist küberjulgeolekut puudutavates teemades. Nõudlus Eesti kogemuste ja ressursside järele on jätkuvalt ületamas võimalusi seda pakkuda. Eesti välis- ja julgeolekupoliitika seisukohalt prioriteetne küberkoostöö meie lähimate liitlaste (Ameerika Ühendriigid, Ühendkuningriigid, Prantsusmaa, Saksamaa ning Põhja-Balti piirkond) ja rahvusvaheliste organisatsioonidega (EL, NATO, ÜRO, OSCE, jt) on andnud hea raamistiku rahvusvahelise Ukraina abistamise koalitsiooni nagu Tallinna mehhanism ja IT-koalitsiooni algatamiseks.

Üha teravam geopoliitiline olukord ning küberrünnakute suur roll rahvusvahelistes konfliktides (eriti just Venemaa sõjalises agressioonis Ukraina vastu) on selgelt näidanud, et Eesti senine poliitika olla küberjulgeolekualase info aktiivne pakkuja ja oma kogemuste jagaja on tugevdanud Eesti jaoks olulisi partnerlussuhteid. Info ja kogemuste vahetamise kõrval on kasvanud ootused Eesti kaasumisele rahvusvahelise tasandi poliitikate kujundamisel (eriti uute tehnoloogiate kontekstis). Kasvutrendis on teravamast geopoliitilisest olukorrast tingituna ka küberrünnakute rahvusvahelised omistamised. Eesti on osalenud pea kõigis olulisemates omistamiste koalitsioonides, kuid pole seni veel ise ühtegi omistamisavaldust algatanud.

Eesti on Venemaa Ukraina-vastase agressiooni kontekstis jätkuvalt tunnustatud kui üks aktiivsemaid küberohtudega seotud info jagajaid, mille tulemusena on õnnestunud Euroopa Liidu ja NATO liikmesriikide vastu kavandatud rünnakuid ära hoida. Jätkame proaktiivset lähenemist ning jagame ka tulevikus samameelsetele riikidele ja partneritele küberohtudega seotud infot. Eesti toetus Ukrainale küberkonfliktis tugevdab meie kuvandit usaldusväärse koostööpartnerina ning näitab, et suudame teiste väikeriikide hulgas positiivselt silma paista. Venemaa agressioon Ukraina vastu on tõestanud, et tänapäeval eeldab kerksuse tagamine füüsilises relvastatud konfliktis ka digiühiskonna kerksuse tagamist. Eesti julgeoleku jaoks on Ukrainas toimuva sõjalise konflikti õppetunnid väga olulised. Need annavad võimaluse Eestil kui digitaalselt ühel maailma arenenuimal riigil koos Ukrainaga küberjulgeoleku küsimustele globaalselt tähelepanu pöörata ja selle kaudu tutvustada Eestis loodud lahendusi.

Täiesti uue taseme on saavutanud ka kübervaldkonnas abi andmine. Nimelt, Eesti aktiivsel osalusel loodi 2023. aastal Tallinna mehhanism[33] ja IT-koalitsioon, mis koordineerivad rahvusvahelise abi andmist vastavalt tsiviil- ja kaitsesektoris. Tallinna mehhanism on peamine abi andmise kanal kõigile olulisimatele doonoritele. See on hea alus, loomaks uut sünergiat Eesti antava kahepoolse ja Eesti koordineeritava mitmepoolse toetuse puhul.

Eesti on panustanud Kariibi mere piirkonna arengusse ja sealse küberturvalisuse edendamisse. 2019. aastal käivitati RIA alluvuses Euroopa Liidu küberalast arengukoostööd koordineerima mõeldud projekt EU CyberNet[34], mida on saatnud edu. Loodud on Dominikaani Vabariigis tegutsev kompetentsi- ja koolituskeskus LAC4, mis toetab rahvusvahelist koostööd piirkonna riikide ja Euroopa Liidu vahel. Lisaks esimesele projektitoetusele on 2026. aastani tagatud ka jätkurahastus. Eesti on selles piirkonnas euroopalikke väärtusi esindav digiriik ja küberturvalisuse eestkõneleja ning ühtlasi osaline Hiina ja Venemaa mõju tasakaalustavas koalitsioonis. Eesti kavandab Aafrikas ja Kagu-Aasias ka edasisi kübervõimearendusega seotud tegevusi, mis looksid täiendavat sünergia IKT-alase arengukoostöö projektidega.

Projekti EU CyberNet raames on RIA juhtimisel loodud Euroopa Liidu küberarengukoostöö võrgustik, mis hõlmab nüüdseks üle 500 eksperdi ja 150 organisatsiooni. Laiapindne kaasamine on arengukoostöö edu alus ning võrgustikul on suur potentsiaal tulevaste projektide toetamisel.

Jätkame aktiivset panustamist Euroopa Liidu siseturu turvalisena hoidmisse optimaalse administratiivse koormusega.

---

[33] Tallinna mehhanism, https://www.vm.ee/rahvusvaheline-oigus-ja-kuberdiplomaatia/digi-ja-kuberdiplomaatia/tallinna-mehhanism.
[34] EU CyberNet, https://www.eucybernet.eu/.

Tugevad ja nõrgad küljed

Eesti küberkoostöö teiste riikidega on seni toimunud peamiselt läbi kahepoolsete algatuste või osaluse rahvusvaheliste organisatsioonide töös, mis on eri valdkondade ja institutsioonide lõikes ebaühtlaselt jaotunud. Vajaka on jäänud süsteemsest ja koordineeritud lähenemisest ning terviklikust üldpildist koostöövõimaluste ja -mehhanismide valikul.

Jätkame osalemist rahvusvahelistes formaatides info ja kogemuste vahetamiseks. Selline koostöö on aluseks paremate suhete loomisele ja usalduse tugevdamisele, et üheskoos panustada küberrünnakute heidutusse ja nende toimepanijate väljaselgitamisse. Seejuures on oluline ka Eestil endal arendada tehnilisi ja analüütilisi võimalusi, et peale liitlaste omistamisavalduste toetamise suudaksime ka ise omistamisavaldusi algatada. Vastasel juhul on oht, et Eesti kaotab usalduse sellistes koostööformaatides osalemiseks. Eesti ei näe vajadust uue küberjulgeoleku konventsiooni järele, vaid toetame kokkulepitud kübernormide ja küberusaldusmeetmete rakendamist.

Ukraina kaitsmist toetavad kahepoolsed tegevused on selge põhjus, miks Euroopa Liidu ja NATO liikmesriigid on usaldanud Eestit vahendite ja toetustegevuse koordineerimisel. Militaarvaldkonnas on Eesti IT-koalitsiooni[35] juhtriik, tsiviilvaldkonnas Tallinna mehhanismi initsiaator. Edukas toimetamine Ukrainas on aluseks sarnastele abi andmise moodustele ka mujal kriisikolletes, pakkudes Eestile võimalusi täiendavaks osaluseks nii arengukoostöös kui ka äridiplomaatias.

Ladina-Ameerikas ja Aafrikas on Eesti teenäitaja digi- ja küberküsimustes. Lisaks Eesti enda rahalisele panusele oleme võimendanud oma tegevust ka välisrahastusega projektide abil. Selliste, näiteks Euroopa Liidu rahastatud arengukoostöö projektide juhtimine on Eesti jaoks oluline ka edaspidi.

Teenuste ja küberkompetentsi arendamine kolmandates riikides võiks motiveerida Eesti küberettevõtteid ja IKT-sektori liidreid laienema. Oleme loonud võimalusi e-riigi teenuste ekspordiks, kuid seni on nende võimaluste kasutamine olnud pigem tagasihoidlik.

Eesmärgid, milleni soovime strateegiaperioodil jõuda

- Eesti on rahvusvahelisel areenil arvestatav ja tugev partner.
- Eestile on tagatud igakülgne rahvusvaheline toetus ning partnerriigid on valmis reageerima Eesti vastu suunatud küberrünnetele.
- Koos peamiste Euroopa Liidu ja NATO liikmesriikidega on reageerimisvalmidus õppustel proovile pandud.
- Eesti on endiselt oluline partner Ukrainale ning toetab küberkaitse arendamist.
- Eesti IKT-sektori ettevõtete eksporti on välisturgudel jõuliselt edendatud.
- Eesti tegevus turvalise digiühiskonna arendamiseks Ladina-Ameerikas ja Aafrikas toetab sihtriikide võimekust ennetada ja tõrjuda küberründeid ning pärssida rahvusvahelist küberkuritegevust.
- EU CyberNet on Euroopa Liidu tõhusalt toimiv pikaajalise mandaadiga küberarengukoostöö võrgustik.

Nende eesmärkide saavutamiseks vajalikud tegevused

- Prioriteetriikide puhul tuleb keskenduda praktilisele koostööle: regulaarne ohupiltide vahetamine, ühisõppuste korraldamine ning küberturvalisuse vallas parimate praktikate, tehnoloogiate ja

[35] Vt lähemalt https://www.kaitseministeerium.ee/et/uudised/eesti-luksemburg-ja-ukraina-kaivitasid-ramsteinis-ukraina-toetamiseks-it-koalitsiooni.

teadmiste jagamine, sealhulgas elutähtsa taristu küberturvalisuse suurendamine ja erasektori kaasamine.
- Eesti kaitsemeetmete planeerimisel ja arendamisel tuleb küberdomeenis arvesse võtta riskiriikide ohuhinnanguid ning Ukraina kogemust ja õpituvastusi Venemaa agressioonisõjaga seoses.
- Vaja on parandada Eesti tehnilist ja analüütilist võimekust algatada omistamisavaldusi.
- Majandus- ja Kommunikatsiooniministeeriumil ning Välisministeeriumil tuleb tagada rahvusvaheliste kübervaldkonna meetmete riigisisene koordineerimine ning osalemine liikmesriikidevahelises küberkoostöös.
- Eesti toetab Ukraina küberturvalisuse arendamist, kaasates võimaluse korral ka Eesti IKT-sektori ettevõtteid.
- Jätkatakse EU CyberNeti võrgustiku arendamist ja kindlustatakse selle pikaajaline rahastamine.

Mõõdikud

- Kõigi prioriteetriikidega on strateegiaperioodil läbi viidud vähemalt üks küberõppus.
- Eesti on küberrünnakutega seoses algatanud vähemalt ühe rahvusvahelise avaliku omistamise.
- Tallinna mehhanismiga liitunud riikide arvu kasv strateegiaperioodi jooksul.
- Tallinna mehhanismi kogueelarve järjepidev kasv aastatel 2024–2027.
- Arengukoostöö tegevuste eelarvest 0,1% on suunatud küberturvalisusele.
- IKT-valdkonna arenguabist 10% on suunatud küberturvalisusele.

5.2. Kogukond ja järelkasv

Olukord

Eesti küberturvalisuse tugevaks küljeks on läbi aastate olnud kogukondlik mõtteviis, mille kohaselt igaüks peab vastutama enda küberturvalisuse eest, aga üheskoos suudame rohkem. Eesti väiksus on ühtlasi meie tugevus: kogukonna liikmed tunnevad üksteist ning istuvad kõrvuti konverentsidel ja „saunalaval“, isegi kui nende tööandjad on konkurendid. Seda tugevust tuleb hoida ja arendada, sest ainuüksi automatiseerimise ja masinate omavahelise suhtlusega ei suuda riik kodanike ja ühiskonna küberturvalisust tagada.

Strateegia elluviimisel ja laiemalt küberturvalisuse ühiskondlikul tagamisel on oluline jagada riigis teadmust mõttekodade, ülikoolide ja teadusasutuste ning erasektori partneritega. Riik kasutab mõttekodade kui strateegiliste partnerite võimekust Eesti valdkondliku kompetentsi ja rahvusvahelise koostöö arendamisel.

RIA, riigi IT-majad, ministeeriumid, ülikoolid, eraettevõtted ning sihtasutused ja mittetulundusühingud on juba aastaid korraldanud regulaarseid ja kogukonnale tuttavaid üritusi. Erasektori kogukondlike ürituste jätkusuutlikkus lähtub suuresti vaba turumajanduse põhimõtetest ja osalustasudest, seevastu riigi korraldatud jätkusuutlikud kogukonnaüritused omavad sümboolset mõju.

Tugevad ja nõrgad küljed

Eesti küberturvalisuse kogukond on mitmetahuline ja kirev seltskond. Ka edaspidi tuleks kaasata üksikisikuid ja ettevõtteid, kes ei pruugi olla teadlikud kogukondlikust lähenemisest. See tähendab, et eraldi tähelepanu tuleks pöörata nendele, kes on kogukonnas olnud vähem esindatud – küsimus on soolises tasakaalus, regionaalsetes erinevustes ja keelelises esindatuses. Eesti ei ole küberruumis kunagi üksi, meid toetab ülemaailmne küberkogukond, teiste hulgas Euroopa partnerid ja panustajad kaugematest riikidest. Eesti küberkogukond on seda tugevam, mida mitmekesisemalt ja avatumalt me suhtleme.

Küberturvalisuse valdkonnas on spetsialiste puudu nii Eestis, Euroopas kui ka mujal maailmas. Seetõttu on vaja pöörata eraldi tähelepanu kogukonna arendamisele läbi haridusalgatuste koostöös partneritega. Teadlikkus küberhügieenist on üksnes alguspunkt – ka siin tuleks teha rohkem ksoostööd koolidega, et juba algklassides õpiksid lapsed märkama küberruumis varitsevaid ohte. Alates põhikoolist on vaja pöörata eraldi tähelepanu reaalainetele, arvutiteaduste ja küberturvalisuse valdkonna karjäärivõimalustele. Kutse- ja kõrgharidus reageerib ühiskondlikele muutustele tavaliselt üsna kiiresti, kuid kübervaldkonnas näeme vajadust senisest kiirema sekkumise järele. Laiapõhjalise küberkaitse ülesehitamiseks ning praeguse taseme hoidmiseks on oluline tagada spetsiifiliste küberturbeoskustega noorte pealekasv ning haridusvõimaluste süstemaatiline laiendamine valdkondades, mis võivad noortele tunduda esimese hooga liiga keerulised, näiteks kõrgemal matemaatikal põhinev krüptograafia ja kvantarvutid. Vaja on suurendada küberturbe alustala – turbelahendusi, sealhulgas krüptograafiat – tundvate õpilaste hulka kõrgkoolides. Samuti tuleb lähiaastatel jõuda olukorrani, kus küberhügieeni ja -turvalisuse teadmised moodustaksid lahutamatu osa kõikide kooliastmete õppekavadest.

Küberturvalisus karjäärimudelina on olnud väga meestekeskne valdkond. Seega tuleks spetsialistide ringi laiendamiseks otsida olemasolevate algatuste[36] kõrval uusi võimalusi, kuidas äratada tüdrukute huvi selle valdkonna vastu, eelkõige eas, kus nad hakkavad tegema karjäärivalikuid. Ka elukestva õppe käigus ümberõppe programmide kaudu naiste kaasamine võiks olla üks võimalikke kiireloomulisi lahendusi kübervaldkonna tööjõupuudusele.

Küberturvalisuse tagamisel on Eesti seni toetunud eraettevõtete pakutud lahendustele ja kodumaisele oskusteabele. Innovatsioon tekib erasektoris, toetudes investeeringutele ja teadusasutustele. Tihti jääb innovatsioon aga riiulile, sest erinevalt ründavast riigist ei pruugi Eestis (ja Euroopas) olla piisavalt palju platvorme, mis aitaksid uuenduslikel lahendustel jõuda katsetuse faasi või lausa turule. Vaja on rohkem katsetamist, regulaarset ja sihipärast investeerimist haridusse ja teadusse (sh küberspetsialistide järelkasvuks), riigipoolseid garantiisid või tuge ning eraettevõtete julgust. Seejuures on mõistlik lähtuda Eesti teadus- ja arendustegevuse ning innovatsiooni ja ettevõtluse (TAIE) arengukavas 2021–2035[37] sätestatud eesmärkidest. Lisaks on riigil teaduse ja arenduse valdkonnas vaja pöörata tähelepanu kodumaise oskusteabe arendamisele ning teadlikkuse suurendamisele, et ka uute tehnoloogiate küberturvalisusega pikemas plaanis toime tulla.

Eesmärgid, milleni soovime strateegiaperioodil jõuda

- Eesti küberkogukond on avatud ja mitmekesine.
- Eesti haridussüsteem toetab pädevate küberspetsialistide järelkasvu.
- Küberhügieen ja -turvalisus on lõimitud kõikide kooliastmete õppekavadesse.
- Kohalik tulevikutehnoloogiaid puudutav teadmus kasvab tuntavalt, lähtudes küberturvalisuse sektori riiklikest eesmärkidest (sätestatud TAIE arengukavas aastateks 2021–2035) ning innovatsiooni ja ettevõtlust soosivast keskkonnast.

Nende eesmärkide saavutamiseks vajalikud tegevused

- Tuleb soodustada rotatsiooni erinevate riigiasutuste ja -struktuuride vahel, et edendada vajaliku kompetentsi ja heade praktikate levikut ning luua uut teadmust.
- Riik peab panustama eraalgatuslikesse kogukonna üritustesse.

[36] Rühmitused CyberTomorrow ja Women in IT.

[37] Teadus- ja arendustegevuse, innovatsiooni ning ettevõtluse (TAIE) arengukava 2021–2035 | Haridus- ja Teadusministeerium (hm.ee)

- Vaja on toetada reaalteaduste, arvutiteaduste ja küberturvalisuse valdkonna karjäärivalikute populariseerimist, muu hulgas tüdrukute ja naiste hulgas, kaasates kogukonna liikmeid mõjuisikutena.
- Koostöös Haridus- ja Teadusministeeriumiga tuleb arendada digi- ja küberoskusi kõigis haridusastmetes.
- Majandus- ja Kommunikatsiooniministeerium peab koostöös Haridus- ja Teadusministeeriumiga koostama ettepanekud, kuidas täiendada õppekavasid küberhügieeni ja -turvalisuse teemadega.
- Vaja on välja töötada küberturbealased mikrokraadiprogrammid.
- Vaja on luua raamistik kodumaise oskusteabe arendamiseks teadus- ja arendustegevuse rahastamise kaudu ning seada strateegilised prioriteedid uuringute vallas.
- Kohalikke küberturvalisuse valdkonna ettevõtteid tuleb tugevdada kogukondlike tegevuste ja keskselt jagatava ohuteadmusega.

Mõõdikud

- Haridusastmetesse on lisatud küberturvalisuse õpetus.
- Küberhügieen ja -turvalisus on lõimitud kõikide kooliastmete õppekavadesse. – Jah/ei.
- Vähemalt kaks Eesti kõrgkooli pakuvad küberturbealaseid mikrokraadiprogramme.

KOKKUVÕTE

Eesti riiklik küberstrateegia aastateks 2024–2030 „Läbivalt IT-vaatlikum Eesti“ on koostatud ajal, mil globaalne julgeolekuolukord on võrreldes harjumuspärasega märgatavalt halvenenud. Sellest tulenevalt on fookus võrreldes eelmise, aastatel 2019–2022 kehtinud küberturvalisuse strateegiaga suunatud eelkõige julgeoleku ja turvalisuse kindlustamisele. Siiski on küberturvalisuse arengut käsitletud võimalikult komplektselt, hõlmates küberaspekte alates kesksete turbelahenduste arendamisest ja elutähtsate teenuste toimimise kindlustamisest kuni laiapindse ennetuse ning piisava järelkasvu tagamiseni. Kõigis neis valdkondades on seatud konkreetsed eesmärgid, nimetatud nende eesmärkide täitmiseks vajalikud tegevused ning esitatud eesmärkide saavutamise ja võetavate meetmete seiret võimaldavad mõõdikud. Strateegia kinnitamisele järgneb selle rakenduskava koostamine.

Varasema strateegiaga võrreldes võib käesoleva dokumendi arenguhüpetena käsitleda ambitsiooni ühtlustada kehtivaid riigikaitselisi, küberturvalisust ja andmekaitset reguleerivaid õigusakte ning tagada riigi küberturvalisuse baasteenuste eelarvevahendite piisavust pikaajalist planeerimist võimaldaval tasemel. Riiklikust julgeolekust ja küberohupildist lähtuvalt prioriseerime elutähtsate teenuste seire tõhustamist, toimepidevuse taseme tõstmist, tulevikukindluse ja kriisikindluse suurendamist. Need eesmärgid saavutame infoturbealaste ja IT-teenuste korraldamiseks vajalike miinimumnõuete kehtestamise, küberkilbi tugevdamise, küberreservi arendamise ja testimise ning tulevikutehnoloogiate riskihindamise tulemuste rakendamise kaudu.

Riiklik küberturvalisuse juhtimine peab toetama sihtrühma vajadusi ning olema digiteenuste turvalisemaks muutmisel läbivalt intsidente ja kriise ennetav. Esimest korda on kirja pandud selge siht arendada küberoskusi kõigis Eesti elanikkonna vanuserühmades. Püstitatakse eesmärk täiustada keskselt pakutavaid kaitseteenuseid, tõhustada erasektoriga tehtavat koostööd ning jätkata küberhügieeni ja -turvalisuse alal senisest sihistatumat laiapindset ennetustööd. Kirja on pandud ka aja jooksul kinnistunud vajadus hakata teatud määral diferentseerima küberturvalisuse seaduse subjektidele sätestatavaid nõudeid, arvestades nende pakutavate teenuste reaalset mõju ühiskonna toimimisele.

Lisaks luuakse koostöös internetiteenuse pakkujatega senisest terviklikum ning ohtude kiiremat ennetamist ja tõkestamist võimaldav küberruumi ohupilt. Sarnaselt eelmise küberstrateegiaga on siingi

sätestatud, et tuleb kõikehõlmavalt analüüsida küberturvalisuse riiklikku arhitektuuri ja teha vastavad otsused hiljemalt 2027. aastaks. Otsustavalt tuleb eemale liikuda väga haavatavast taakvarast ning keskkonnale kahjulikust, aina kuhjuvast digikeltsast. Loomulikult tuleb igapäevaselt pingutada ka selle nimel, et Eestis loodava küberkeskkonnaga sarnane keskkond kujundataks nii Euroopa Liidus kui ka teistes samameelsetes riikides maailmas laiemalt.

Kuna käesolev suunadokument lubab küberuumi turvalisust ja julgeolekut strateegiaperioodi lõpuks selgelt tugevdada, saab järgmine strateegia keskenduda rohkem nendele eesmärkidele, mida ei seata mitte riigisektorile, vaid näiteks erasektori ja iduettevõtete toetamisele nende küberturvalisuse taseme tõstmiseks. Strateegiat uuendatakse küberohupildist ja riiklikust julgeolekuolukorrast lähtuvalt vähemalt kord kahe aasta jooksul.

LISA 1. Strateegia rakendamisse kaasatavate asutuste ja sidusrühmade loetelu

Riigikantselei tagab küberturvalisuse integreerimise riigikaitse planeerimisdokumentidesse, on kriisireguleerimispoliitika väljatöötamisel juhtrollis ja koordineerib asjaomaste valitsusasutuste tegevust.

Vabariigi Valitsuse julgeolekukomisjon kujundab valitsuse pädevuses olevates küsimustes julgeoleku-, riigikaitse- ja kriisireguleerimispoliitika seisukohad ning koordineerib täidesaatva riigivõimu asutuste tegevust riigikaitse ja kriisireguleerimise planeerimisel, arendamisel ja korraldamisel.

Küberjulgeoleku nõukogu tegutseb Vabariigi Valitsuse julgeolekukomisjoni juures ning kujundab asutuste vahel koordineeritud seisukoha küberjulgeoleku küsimustes ja tagab küberturvalisuse strateegias kokku lepitud tegevuste täitmise seire vähemalt kaks korda aastas. Küberjulgeoleku nõukogu liikmed on kõik ministeeriumid, Riigikantselei ja Prokuratuur ning Riigi Infosüsteemi Ameti, Andmekaitse Inspektsioon, Politsei- ja Piirivalveamet, Kaitsepolitseiamet, Välisluureamet ning Tarbijakaitse ja Tehnilise Järelevalve Amet. Riigikaitse vaadet esindab Kaitseväe kõrval Kaitseliit kui vabatahtlik, sõjaväeliselt korraldatud ja sõjaväeliste harjutustega tegelev riigikaitseorganisatsioon.

Majandus- ja Kommunikatsiooniministeeriumi riikliku küberturvalisuse osakonna põhiülesanne on üleriigilise küberturvalisuse tagamise juhtimine, korraldamine ja koordineerimine nii riigisiseselt kui ka rahvusvaheliselt, arengukavade väljatöötamine ning nende elluviimise ja tulemuslikkuse seire, algatuste eestvedamine, kogukonna hoidmine ja küberturvalisuse valdkonna õigusloome kujundamine. Küberturvalisusega on seotud ka ministeeriumi ülesanded digiühiskonna ja digiarengu, majandus- ja ettevõtlustegevuse, teadus- ja arendustegevuse, innovatsiooni, piiriüleste avalike teenuste ja muu taolise arendamisel, toetamisel ja korraldamisel.

Riigi Infosüsteemi Amet (RIA) täidab mitmekülgseid ülesandeid riigi infosüsteemi ja küberturvalisuse valdkonnas ning on ühtlasi riigi keskne küberasutus Euroopa Liidu võrgu- ja infosüsteemi kaitse direktiivi (NIS) mõistes. RIA üks osa on küberturvalisuse keskus, mis arendab infoturbemeetmeid ja nõustab nende rakendamisel, korraldab elutähtsa taristu küberturvalisust ning täidab kriisijuhtimise ülesandeid laiaulatuslike küberintsidentide puhul, samuti tagab küberohtude ja -riskide seire, tõkestab olulise tähtsusega küberintsidente ning analüüsib Eesti ja rahvusvahelise küberruumi arengusuundi. Lisaks pakub RIA sideteenuse osutajatele interneti alustaristut kindlustavaid teenuseid läbi Eesti internetivõrke ühendava internetisõlmpunkti RTIX, mis tagab võrkudevahelise liikluse ka sellises olukorras, kus ühendus teiste riikidega on häiritud. Samuti täidab RIA Eesti küberturvalisuse valdkonnas tööstuse, tehnoloogia ja teadusuuringute koordineerimisüksuse ülesandeid ning viib ellu Euroopa Liidu võimearendusprojekte.

Tarbijakaitse ja Tehnilise Järelevalve Amet on riiklik küberturvalisuse sertifitseerimise asutus, mis haldab andmeside ja ühenduvuse vallas raadiosageduste kasutamist, ka riiklikus kriisiolukorras (kõrgendatud kaitsevalmiduse, erakorralise seisukorra ja sõjaseisukorra ajal).

Riigi Info- ja Kommunikatsioonitehnoloogia Keskus (Riigi IT Keskus ehk RIT) osutab Majandus- ja Kommunikatsiooniministeeriumi hallatava asutusena riigis arvutitöökoha ja serveri baastaristu teenuseid. RIT osutab teenuseid ligikaudu 25 000-le avaliku sektori töökohale.

Riigi Infokommunikatsiooni Sihtasutus (RIKS) on Majandus- ja Kommunikatsiooniministeeriumi haldusalas olev mittetulunduslik sihtasutus, mis tagab riigiasutuste ja teiste riigieelarveliste institutsioonide sidealase teenindamise ning eriotstarbelise ja operatiivside. Peale selle osutab RIKS

operatiivraadiosideteenuseid ning andmekeskuste ja riigi mereside- ja telefoniteenuseid. 2022. aastal alustas RIKS Eestis satelliitandmeside lahenduse väljatöötamise, et tagada riigi olulisimate teenuste osutamine.

Siseministeerium tagab siseturvalisuse arengukava ja sellega seotud programmide tegevuste elluviimise ning panustab valdkonnaüleste koostöö- ja koordinatsioonimehhanismide ning ühtse olukorrapildi loomisse.

Siseministeeriumi Infotehnoloogia- ja Arenduskeskus (SMIT) tagab siseturvalisusega seotud infosüsteemide halduse ja arenduse. SMIT loob ja haldab siseturvalisuse jaoks vajalikke infosüsteeme, mis on mõeldud kasutamiseks eelkõige Politsei- ja Piirivalveametile, Päästeametile, Häirekeskusele, Sisekaitseakadeemiale ja Siseministeeriumile, aga ka näiteks Rahandusministeeriumile, Kaitseministeeriumile, Justiitsministeeriumile ja Maanteeametile.

Politsei- ja Piirivalveametis töötavad veebikonstaablid, kes jälgivad sotsiaalmeediat ning teevad koostööd noorte turvalisust puudutavate organisatsioonidega. Veebikonstaablid jagavad avalikkusele teavet internetis levivate ohtlike suundumuste kohta, mis võivad kahjustada noorte ja laste heaolu.

Keskkriminaalpolitsei küberkuritegude büroo ülesanne on küberkuritegude avastamine, tõkestamine ja menetlemine.

Kaitsepolitseiameti pädevuses on riigi põhiseadusliku korra ja territoriaalse terviklikkuse vägivaldsele muutmisele suunatud tegevuse kohta teabe kogumine ja selle töötlemine ning riigi vastu suunatud luuretegevuse ennetamine ja tõkestamine.

Kaitseministeerium koostöös Kaitseväe, Kaitseliidu ja Välisluureametiga panustab küberturvalisuse tagamisse ennekõike sõjalise kaitsega seotud tegevuste elluviimise kaudu.

Kaitseväe küberväejuhatuse põhiülesanded on operatsioonide läbiviimine küberruumis Kaitseministeeriumi vastutusalas juhtimistoetuse korraldamiseks, küber- ja juhtimistoetuse alaste võimete arendamise juhtimine ja koordineerimine ning küberrelvaliigi väljaõppe korraldamine.

Kaitseliidu küberkaitseüksus (KKÜ) on Eesti küberruumi kaitseks loodud vabatahtlik organiseeritud ühendus. Selle liikmeskonda kuuluvad küberkaitse seisukohalt olulistel positsioonidel olevad spetsialistid, IT-oskustega patriootiliselt meelestatud inimesed, sealhulgas noored, kes on valmis andma oma panuse riigi küberkaitsesse. KKÜ teeb küberturvalisuse reservi raames tihedat koostööd RIA-ga.

Välisluureamet korraldab elektroonilist teabeturvet ehk salastatud IT-süsteemide küberkaitset ja kontrollib selleks kehtestatud nõuete täitmist. Annab Eestit puudutavate väliste julgeolekuohtude kohta luureinfot kogudes olulise panuse Eesti riigikaitse ja julgeolekupoliitika kujundamisse. Ameti kogutud luureinfo tagab vajaliku eelhoiatuse meid ohustavate sündmuste korral, moodustades seeläbi Eesti riigikaitse eesliini.

Sihtasutus CR14 on Kaitseministeeriumi asutatud riiklik äriühing, mis põhineb enam kui kümneaastasel küberharjutusvälja kogemusel õppuste, testimise, valideerimise ja eksperimenteerimise valdkonnas. Ühtlasi esindab CR14 Kaitseministeeriumiga kokkulepitud ulatuses Eestit suhetes NATO küberkaitsekoostöö keskusega (CCDCOE).

Haridus- ja Teadusministeeriumi roll küberoskuste suurendamisel on kindlasti kasvamas, kuna ühe

arenguvajadusena on toodud esile asjaolu, et haridussüsteemis tuleks küberturvalisust käsitleda digipädevuse arendamise raames kõigil haridusastmetel. Ministeeriumi haldusalas olev Haridus- ja Noorteamet haldab digipädevuse ja digiturvalisuse keskkonda https://digipadevus.ee/.

Justiitsministeerium kujundab õigus- ja kriminaalpoliitika abil turvalist ühiskonda. Küberturvalisuse korraldamise valdkonnas on Justiitsministeeriumi roll tagada avaliku teabe ning andmekogude pidamise ja andmete töötlemisega seotud õigusaktide ajakohasus.

Andmekaitse Inspektsioon on Justiitsministeeriumi valitsemisalas tegutsev valitsusasutus, kes seisab hea isikuandmete kaitse ja avaliku teabe kättesaadavuse eest ning on digitaalses elukorralduses turvalise andmetöötluse kujundaja ja järelevalvaja.

Registrite ja Infosüsteemide Keskus (RIK) on Justiitsministeeriumi haldusalas tegutsev asutus, mis arendab ja haldab olulisi registreid ja infosüsteeme, näiteks e-äriregistrit, e-notarit, e-kinnistusraamatut, kohtuinfosüsteemi, kriminaalhooldusregistrit, kinnipeetavate registrit, karistusregistrit, e-toimikut ja elektroonilist Riigi Teatajat.

Rahandusministeerium vastutab küberturvalisuse tagamisega seotud külgnevate harude poliitikakujundamise eest (nt virtuaalvääringutega kauplemist reguleeriv õigusloome) ja tagab finantssektori kaasatuse. Rahandusministeerium on eelarveprotsesside kaudu kaasatud kõigisse poliitikavaldkondadesse.

Finantsinspektsioon kehtestab küberturvalisuse tagamisel konkreetselt finantssektoriga seotud eeskirju ja õigusakte, teostab järelevalvet, edendab teabevahetust ning teeb finantssektori küberturvalisuse meetmete ühtlustamiseks koostööd rahvusvaheliste partneritega.

Eesti Pank teeb tihedat koostööd Finantsinspektsiooniga, koordineerides tegevust ka Euroopa Keskpangaga, millest lähtuvad euroalaülesed suunised mõjutavad Eesti finantsasutuste küberturvalisuse nõudeid ja standardeid.

Rahandusministeeriumi infotehnoloogiakeskus (RmIT) pakub IT-teenuseid Rahandusministeeriumile, Rahapesu Andmebüroole, Maksu- ja Tolliametile, Statistikaametile, Riigi Tugiteenuste Keskusele ning Riigi Info- ja Kommunikatsioonitehnoloogia Keskusele. Peale selle on tema portfellis eri valitsusasutuste välisveebid, millele pakutakse pilvetehnoloogial põhineva valitsusportaali platvormil majutus- ja haldusteenuseid.

Välisministeerium on Eesti digi- ja küberdiplomaatia eestvedaja ja välispoliitika kujundaja. Ministeerium koordineerib Eesti rahvusvahelist tegevust kübervaldkonnas ning vastutab arenguabi koostöö koordineerimise eest.