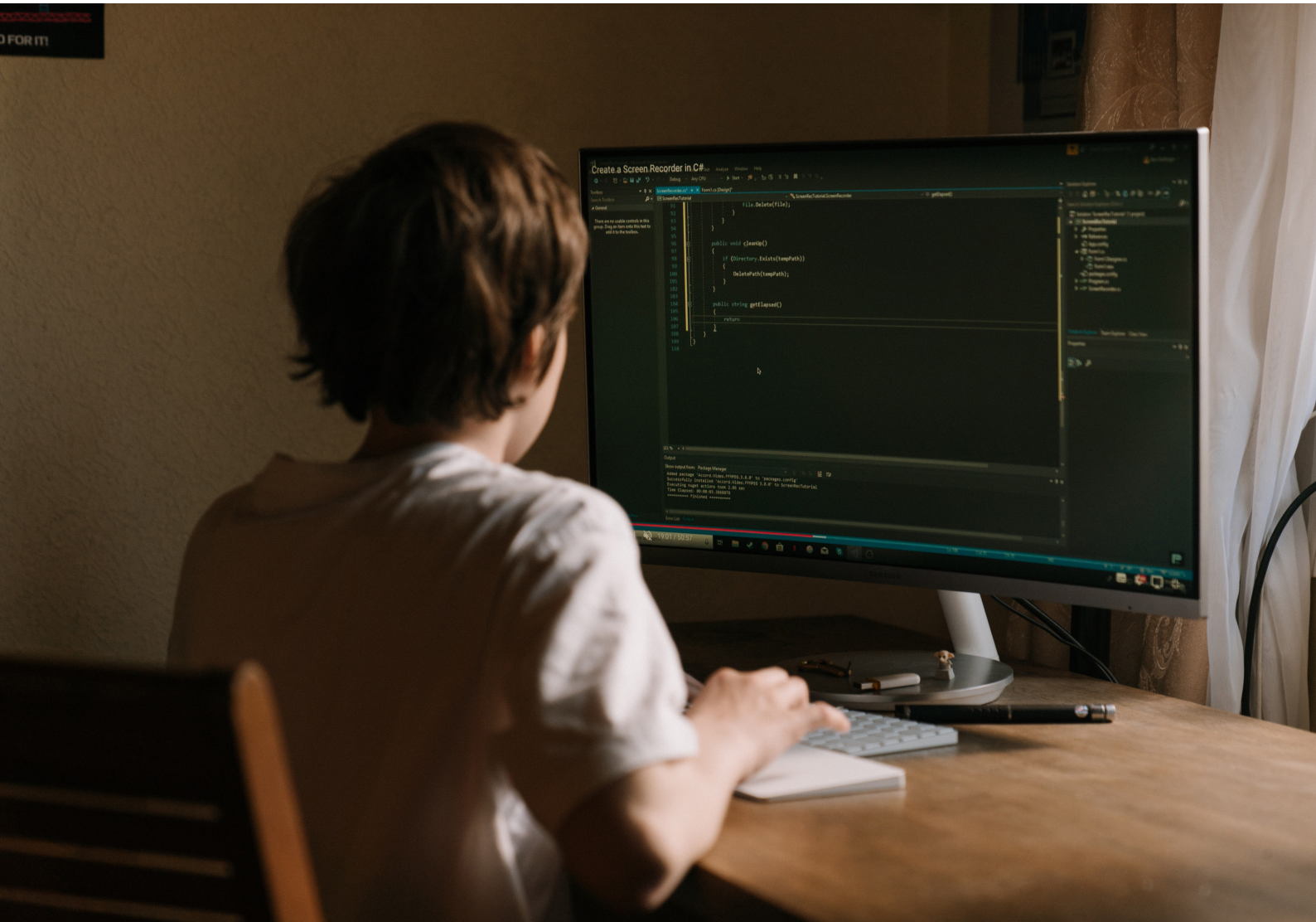
KATE-RIIN KONT

EESTI ELANIKKONNA TEADLIKKUS KÜBERTURVALISUSEST: ÜLEVAADE UURINGUTEST JA VÕIMALIKEST EDASISTEST SUUNDADEST



EESTI ELANIKKONNA TEADLIKKUS KÜBERTURVALISUSEST: ÜLEVAADE UURINGUTEST JA VÕIMALIKEST EDASISTEST SUUNDADEST

KATE-RIIN KONT

SISEKAITSEAKADEEMIA
ESTONIAN ACADEMY OF SECURITY SCIENCES

Esikaane foto: Pexels
Makett ja küljendus: Jan Garshnek
Keeletoimetaja: Siiri Soidro

ISBN 978-9985-67-396-6 (pdf)

www.sisekaitse.ee/kirjastus

SISUKORD

EESSÕNA

Kogu Euroopas suureneb küberrünnete ja küberkuritegude arv ja keerukus. Eesti oli juba 2007. aastal märkimisväärselt digitaliseerunud riik, kus oli hea juurdepääs internetile, digitaalsed isikutunnistused, 80% internetipangandust, elektrooniline maksukogumine ja meditsiinilise kaugjälgimise suur kasutusmäär. BBC andmetel oli Eesti Euroopa Liiduga ühinedes 2004. aastal tehnoloogiliselt arenenum kui Prantsusmaa või Itaalia (Lungescu, 2004; Woodward, 2003). 2007. aasta aprillis toimusid koordineeritud ja ulatuslikud teenusetõkestusrünnakud Eesti valitsuse infrastruktuuri, finantsteenuste pakkujate ja kodumaise meedia vastu. Kolme nädala jooksul 27. aprillist kuni 18. maini 2007 rünnati Eesti internetitaristu komponente ja veebisaite, meilipostkastid täitusid rämpsposti ja õngitsuskirjadega (Schmidt, 2013). Kui ründeid riigiserveritele võis tõlgendada kui poliitilist protesti, siis süstemaatiline kommertsstruktuuride ründamine viitab riigi vastu suunatud organiseeritud tegevusele, nimetatagu seda siis küberrünneteks või küberterrorismiks. Rünnati panku, et halvata majandustegevust, ja meediaväljaandeid, et tõkestada info edastamist. Rünnakutega häiriti lisaks suurtele tegijatele ka väikefirmade igapäevaelu: koormati e-postiservereid, võrguseadmeid ja veebiservereid sedavõrd, et ettevõtete normaalne äritegevus oli häiritud (Randel, 2008). Kuigi need polnud Eestis esimesed küberrünnakud, osutusid need kõige keerukamateks ja selgelt poliitiliselt motiveeritud rünnakuteks ning on saanud tuntuks ka nime all digitaalne Pearl Harbor. Pärast rünnakuid algas Eestis poliitiline arutelu küberjulgeoleku üle ning rünnak suunas ka liitlased kooskõlastatud tegevuse ja koostöö poole. Sellest ajast alates on Eesti olnud küberturvalisuse ja küberkaitse teemalise rahvusvahelise debati esirinnas (Aaviksoo, 2010) ning küberturvalisuse strateegia 2019–2022 kohaselt on küberjulgeolek ja -turvalisus nüüdseks aktsepteeritud nii riigi ja majanduse toimimise kui ka sise- ja välisjulgeoleku lahutamatu osana (Küberturvalisuse strateegia 2019–2022, lk 3).

Küberturvalisuse komponendid ja nende haldamine hõlmab nii protsesse, tehnoloogiaid kui ka inimesi. Kuigi protsessid ja tehnoloogiad saab luua teoreetiliselt turvaliseks, siis nende tegelik turvalisus sõltub inimestest, kes neid kasutavad. Väidetavalt põhjustavad 83% küberjulgeoleku intsidentidest inimlikud asjaolud. See viitab sellele, et inimlik element jääb peamiseks sihtmärgiks volitamata juurdepääsu saamiseks tehnoloogilistele süsteemidele. (Yeng *et al.*, 2021). Lisaks on oluline, kas inimesed kasutavad tehnoloogiat turvaliselt ning teavad ja järgivad turvalisuse reegleid täielikult ja õigesti. Seega võivad inimesed tahtlikult või tahtmatult muutuda ohuks igale infoturbelahendusele ning just inimfaktorit peetakse infoturbe nõrgimaks lüliks.

1. KÜBERTURVALISUS JA SELLEGA SEOTUD MÕISTED

Kuigi termineid „küberturvalisus" ja „infoturvalisus" kasutatakse sageli sünonüümidena, siis von Solms ja van Niekerk (2013) on väitnud, et kuigi küberturbe ja infoturbe vahel on oluline kattuvus, ei ole need kaks mõistet täiesti analoogsed. Nende väitel ületab küberturvalisus traditsioonilise infoturbe piire, hõlmates mitte ainult teaberessursside, vaid ka muude varade, sealhulgas inimese enda kaitset. Infoturbe puhul on viide inimfaktorile tavaliselt seotud inimeste rollidega turvaprotsessis. Küberturvalisuses on inimteguril lisamõõde, nimelt inimesed kui potentsiaalsed küberrünnakute sihtmärgid või isegi teadmatult küberrünnakus osalejad (von Solms ja van Niekerk, 2013, p. 97). Dhillon (2007, 19) viitab ka andmeturbe terminile, mis tähistab tegelike andmete kaitset infosüsteemis. Andmete turvalisus sõltub suurel määral infosüsteemi turvalisusest, kus andmed asuvad.

Digikeskkonnas on küberturvalisus laiem kui info- või andmeturve, olles küll nende kahe valdkonnaga tihedalt seotud, kuid infoturve on selle keskmes. Infoturvalisus viitab teabe kaitsmise kõikidele aspektidele. Enamasti liigitatakse need aspektid kolme kategooriasse: konfidentsiaalsus (*confidentiality*), terviklikkus (*integrity*) ja teabe kättesaadavus (*availability*) (üldtuntud ka kui CIA kolmnurga mudel) (Whitman ja Mattord, 2009, lk 7-8). „Konfidentsiaalsus" viitab teabe kaitsele avalikustamise eest autentimata isikutele, samas kui „terviklikkus" viitab teabe kaitsele lubamatute muudatuste eest. „Kättesaadavus" tähendab, et teave peaks olema volitatud isikutele nõudmisel kättesaadav. Mõnikord lisatakse loendisse aruandekohustuse nõue. Eelnevast tulenevalt on selge, et infoturve ei ole toode ega tehnoloogia, vaid protsess (Mitnick ja Simon, 2002, lk 4).

2. EESTI RIIGI TEGEVUSED KÜBERTURVALISUSE TAGAMISEL

Küberkuritegevus on suur ja kasvav probleem. Üks küberkurjategijate sihtvaldkondi on tervishoid. Riigi Infosüsteemi Amet (RIA) kirjutas 2019. aasta aastaraamatus, et suur probleem on küberintsidendid tervishoiuvaldkonnas ja terviseandmete lekked. RIA teeb tööd selle nimel, et tervishoiuvaldkond suudaks informatsiooniga turvalisemalt ümber käia. Kuid isikuandmeid korjavad ka paljud teised organisatsioonid, näiteks raamatukogud ja arhiivid oma kasutajate kohta. Samuti võime vaid ette kujutada, mis juhtuks, kui kellegi hooletuse tõttu kaob kogu Eesti digiteeritud kultuurimälu. Praegune teadmine küberkuritegevusest põhineb peamiselt tehniliste aspektide uurimisel, kuid mida aeg edasi, seda rohkem tähelepanu on hakatud pöörama ka inimlikele asjaoludele.

Riigi Infosüsteemi Ameti andmetel „Eestis on alates 2007. aastast riiklikul tasemel tegeletud aktiivselt küberturvalisuse tagamisega, et kindlustada riiklike institutsioonide ja elutähtsate teenuste turvalisust ja kättesaadavust igas olukorras" (Vaks, 2013). 2008. aasta küberjulgeoleku strateegia (Küberjulgeolekustrateegia 2008–2013) oli Eesti esimene riiklik strateegiadokument, mis tunnistas küberjulgeoleku ja -turvalisuse valdkondadeülesust ning vajadust koordineeritud tegevuse järele. See oli ka üks esimesi kübervaldkonna strateegiatest maailmas – küberjulgeolekut ja -turvalisust hakati riigi julgeoleku ja turvalisuse aspektina tajuma alles pärast 2007. aastal toimunud Eesti-vastaseid küberrünnakuid (Küberturvalisuse strateegia 2019–2022).

Riigi Infosüsteemide Amet tegeleb lisaks Eesti arvutivõrkudes toimuvate küberintsidentide registreerimisele ja käsitlemisele ka järelevalvega elutähtsate teenuste osutamiseks kasutatavate infosüsteemide üle, aga ka turvalisuse tagamisega teadlikkuse suurendamise kaudu ehk koolituste korraldamisega asutuste infoturbejuhtidele ja tavakasutajatele. Eesti Raamatukoguhoidjate Ühing on koostööpartner Riigi Infosüsteemi Ameti korraldatud küberturvalisuse kampaaniates. RIA korraldas 2019 sügistalvel teavituskampaania „Ole IT-vaatlik!", mis jätkus 2020. aastal. Jätkukampaania ajal keskenduti küberteadlikkuse suurendamisele venekeelsete vanemaealiste seas, kes ei ole internetiohtudest nii hästi informeeritud. Raamatukoguhoidjate teadlikkuse parandamiseks toimusid RIA veebipõhised koolitused Tallinnas, Harjumaal ja Ida-Virumaal. Novembris ja detsembris oli avatud ka küberturvalisuseteemaline infoliin vanemaealistele (Tõiste, 2021). Seega võime väita, et kõikide organisatsioonide juhid ja töötajad peavad olema rohkem teadlikud aina keerulisemaks muutuva küberkuritegevuse ohtudest.

Küberturvalisuse strateegia koostati ühtse protsessina koos infoühiskonna arengukavaga 2020 ning elukestva õppe strateegiaga 2014–2020. Esimene põhineb arusaamal, et eduka e-riigi loomiseks ja arendamiseks peavad infoühiskonna arendamine ja küberturvalisuse tagamine toimuma samal ajal. Küberturvalisuse eesmärk ühiskonnas on tugevdada vastupanuvõimet küberohtudele ning tagada tingimused selleks, et kõik kodanikud ja ettevõtjad saaksid ja oskaksid tõhusalt ja turvaliselt kasutada usaldusväärseid ja hästi toimivaid IKT-võimalusi, teenuseid ja digitaalseid vahendeid. Elukestva õppe strateegia digipöörde programmi elluviimise käigus sooviti tagada, et digioskuseid puudutavad kompetentsid sisaldavad ka küberturvalisust ning õppekavadesse integreeritakse lisaks digitehnoloogiale ka küberturvalisusega seonduvaid elementaarseid teadmisi. Eesmärk oli digivõimaluste teadlik ja tark integreerimine õppeprotsessi ja selle kaudu digipädevuse arendamine (mh turvalisusega seotud kompetentside) üldhariduse valdkonnas. Uus digiühiskonna arengukava 2030 toob esile konkreetsed seosed siseturvalisuse arengukavaga 2020–2030. Mõlemas arengukavas rõhutatakse identiteedihaldust. Siseturvalisuse arengukavas on seatud eesmärk luua usaldusväärne, uuenduslik ja inimkeskne identiteedihaldus. Lisaks rõhutatakse vajadust suurendada nii elanike kui ka organisatsioonide teadlikkust küberkuritegevuse ohtudest ja nendest hoidumise võimalustest. Nii võimendatakse küberturvalisuse strateegias paika pandud prioriteetseid tegevusi mõlemas arengukavas ja suurendatakse küberruumi ohutust.

Üks võimalus teadvustada küberohte ning suurendada eri sihtgruppide ja elanikkonna teadlikkust küberturvalisusest on korraldada teabepäevi, seminare ja võistlusi. Nii näiteks on ettevõtte CTF TECH juba kolmandat aastat järjest korraldanud küberürituste seeriat Cyber Battle of Estonia, mis on suunatud 15–24-aastastele noortele. Võistluse põhieesmärk on tutvustada kübermaailma noortele, kes omandavad praktiliste küberkursuste kaudu esimesed teadmised kübervaldkonnas. 30. septembril 2022 toimus Sisekaitseakadeemia sisejulgeoleku instituudi korraldatud seminar „Raamatukogude roll ohutuma küberruumi loomisel", mille eesmärk oli selgitada, miks on küberteadlikkus oluline raamatukogutöötajatele ja laiemalt meile kõigile. Seminaril tutvustati ka äsja lõppenud uuringu „Raamatukogutöötajate teadmised, suhtumine ja käitumine infoturbe valdkonnas" esmaseid tulemusi.

3. ELANIKKONNA KÜBERTURVALISUSE TEADLIKKUSE UURINGUD EUROOPAS JA MUJAL MAAILMAS

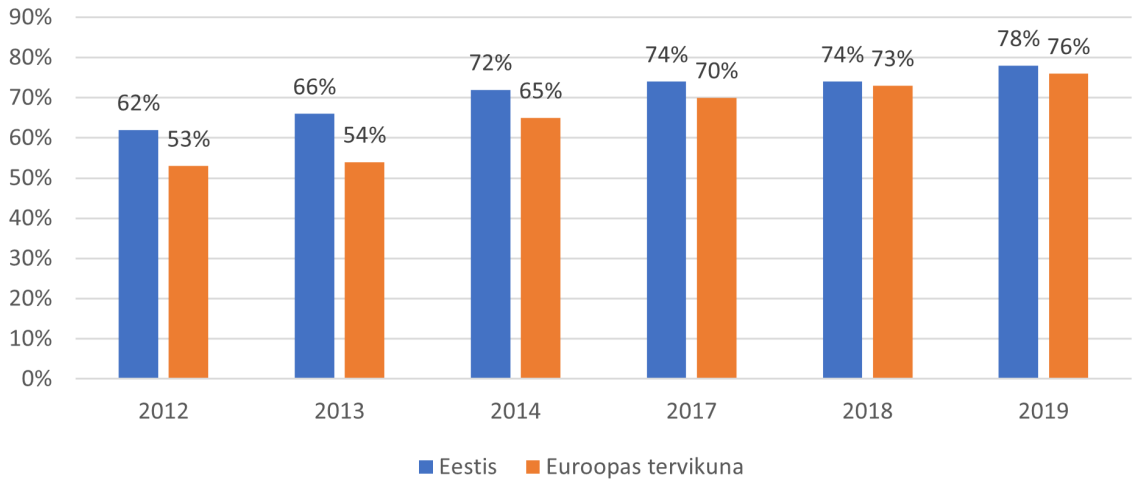
Küberkuritegevus on Euroopa majanduse jaoks kriitiline oht, seetõttu peetakse väga oluliseks regulaarselt jälgida nii elanikkonna kui ka ettevõtete küberturvalisuse teadlikkust ning käitumist internetis. Küberturvalisuse ja küberkuritegevusega seotud laiaulatuslikke uuringuid tehakse mitmel poole maailmas. Kahtlemata on üks ülevaatlikumaid Eurobaromeeter oma avaliku arvamuse uuringute sarjaga, mis võimaldab võrrelda kõigi EL-i liikmesmaades domineerivaid hoiakuid. Eesti vastajad on osalenud kõikides allpool nimetatud uuringutes ja nende uuringute kokkuvõtteraportitest saame väga hea ülevaate eestlaste küberhügieeni trendidest.

Esimene küberturvalisuse avalik uuring toimus ajavahemikus detsember 2005 – jaanuar 2006. Uuring oli osa EL-i turvalisema interneti programmist, mille eesmärk oli varustada lapsevanemaid ja õpetajaid internetiohutuse tagamiseks vajalike teadmistega. Kuigi osa küsimusi esitati kõigile (7560 vastajat), esitati enamik küsimusi vaid juhul, kui vastaja leibkonnas elas mõni laps (3791 vastajat). Uuringu aruandes analüüsiti üldist internetikasutust Euroopas, seejärel interneti kasutamist laste seas: millisel määral ja millistel saitidel on lapsed internetis kahjuliku ja ebaseadusliku sisuga kokku puutunud; meetmed, mida vanemad võtavad, et kaitsta oma lapsi internetti kasutades, ning teadlikkust ja teavet turvalisemast internetist (Safer Internet, 2006).

Järgmised küberturvalisuse uuringud toimusid kolmel järjestikusel aastal: 2012, 2013 ja 2014. 2013. ja 2014. aasta uuringutes korrati enamikku 2012. aastal küsitud küsimustest, et saada ülevaadet küberjulgeolekualaste teadmiste, käitumise ja hoiakute arengust Euroopa Liidus. Vastajad olid valitud erinevatest sotsiaalsetest ja demograafilistest rühmadest, intervjuud toimusid inimeste kodudes ja vastavas riigikeeles. Põhivalimi ülesehitus oli juhuslik (tõenäosuslik) ning proportsionaalne rahvastiku suurusega (riigi kogukatvuse jaoks) ja rahvastikutihedusega. Vastajate arv on kõikides uuringutes suur, jäädes 26 500 ja 28 000 inimese piirimaile. Uuringute tulemustest on näha, et elanike teadlikkus küberturvalisusest kasvab aasta-aastalt ning järjest enam hakatakse tähelepanu pöörama alla 16-aastaste laste internetikäitumisele.

Alates 2017. aastast korraldatakse regulaarselt Eurobaromeetri uuringut eurooplaste suhtumisest küberturvalisusesse. Uuringu eesmärk on mõista EL-i kodanike teadlikkust, kogemusi ja arusaamu küberturvalisuse probleemidest ning tulemusi võrreldakse võimaluse korral varasemate uuringutega. Vastajate arv on samas suurusjärgus ja ka metoodika on samasugune kui varasemate uuringute puhul. Iga uuringu aruande alguses vaadeldakse vastajate internetikasutust ja seadmeid, mida kasutatakse internetile juurdepääsuks, ning tegevusi, mida nad võrgus teevad, käsitletakse vastajate muret võrguturbe eri aspektide pärast, sealhulgas muret internetipangas toimetamise või veebis ostlemise pärast. Samuti vaadeldakse, milliseid muudatusi on vastajad tingituna muredest turvalisuse ja privaatsuse pärast teinud oma küberkäitumises, näiteks kas on muudetud paroole, kas kasutatakse igal kontol erinevaid paroole. Edasi keskendutakse vastajate informeerituse tasemele küberkuritegevuse riskidest: kui palju küberturvalisusega seotud probleeme nad teavad ja kas nad tunnevad muret küberkuritegevuse ohvriks langemise pärast. Seejärel liigub arutelu vastajate isikliku kogemuse käsitlemisele, samuti uuritakse nende teadlikkust teistest seda kogenud inimestest. Räägitakse ka küberkuritegevuse ohvritest. Esitatud on üksikasjalikud meetmed, mida on vastajad kasutusele võtnud, et kaitsta lapsi veebiahistamise eest. Aruande lõpus uuritakse vastajate teadlikkust selle kohta, kuhu nad saavad küberkuriteost või ebaseaduslikust veebikäitumisest teatada, samuti nendest kuritegudest teatamise sagedusest. Samuti käsitletakse seda, mida vastajad teeksid, kui nad langeksid eri liiki küberkuritegude ohvriks.

Nagu näeme jooniselt 1, on igapäevaseid internetikasutajaid pidevalt lisandunud nii Euroopa Liidus tervikuna kui ka Eestis.



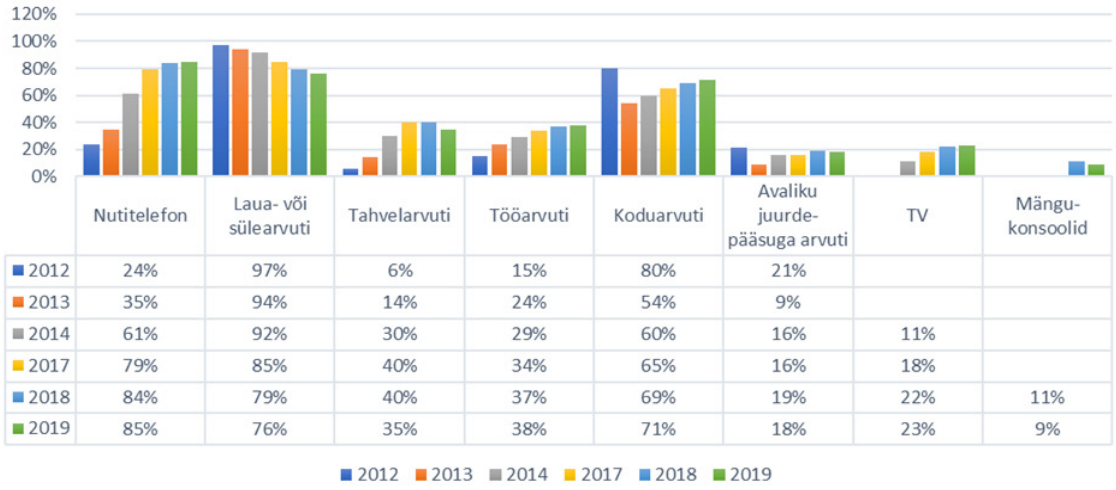
JOONIS 1. IGAPÄEVASED INTERNETIKASUTAJAD EESTIS JA EUROOPAS[1]

Eestlased on võrreldes teiste eurooplastega siiski veidi usinamad igapäevased internetikasutajad: kui EL-i keskmine kasutajate hulk ületas alles 2018. aastal 70% piiri, siis Eestis ületati see piir juba 2014. aastal. Võib arvata, et seoses pandeemiaga suurenes igapäevaste

[1] Kõik selles töös autori koostatud joonised ja tabelid põhinevad järgmistel allikatel:
Cyber Security Report. Special Eurobarometer 390 (2012). https://europa.eu/eurobarometer/surveys/detail/1058
Cyber Security Report. Special Eurobarometer 404 (2013). https://europa.eu/eurobarometer/surveys/detail/1073
Cyber Security Report. Special Eurobarometer 423 (2015). https://europa.eu/eurobarometer/surveys/detail/2019
Europeans' attitudes towards cyber security - Publication Reports. Special Eurobarometer 464a (2017). https://europa.eu/eurobarometer/surveys/detail/2171
Europeans' attitudes towards cyber security (cybercrime) - Publication Reports. Special Eurobarometer 499. (2020). https://europa.eu/eurobarometer/surveys/detail/2249

internetikasutajate arv veel ning võrgustuma olid sunnitud ka need inimesed, kellel oli õnnestunud seda kuni 2020. aasta märtsini vältida.

Interneti igapäevane kasutamine on kasvanud kogu EL-is jätkuvalt, olenemata juurdepääsu viisidest, kuid nende inimeste osakaal, kes kasutavad internetti oma nutitelefonis, on järsult kasvanud: 24%-lt 2012. aastal 85%-ni 2019. aastal. See nihe nutitelefonide poole on kogu EL-is suhteliselt ühtlane. Tahvelarvutist interneti kasutamine oli polpulaarseim 2017. ja 2018. aastal, nüüd on populaarsus taas kahanema hakanud.

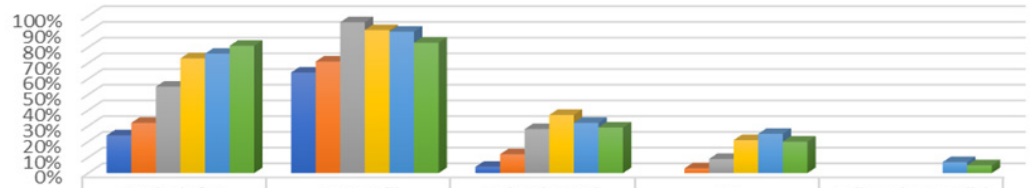


	Nutitelefon	Laua- või sülearvuti	Tahvelarvuti	Tööarvuti	Koduarvuti	Avaliku juurde-pääsuga arvuti	TV	Mängu-konsoolid
2012	24%	97%	6%	15%	80%	21%		
2013	35%	94%	14%	24%	54%	9%		
2014	61%	92%	30%	29%	60%	16%	11%	
2017	79%	85%	40%	34%	65%	16%	18%	
2018	84%	79%	40%	37%	69%	19%	22%	11%
2019	85%	76%	35%	38%	71%	18%	23%	9%

JOONIS 2. EUROOPLASTE ENIM LEVINUD SEADMED INTERNETI KASUTAMISEKS

Kui Euroopas tervikuna kasvab nutitelefonist ja kahaneb süle- või lauaarvutist interneti kasutajate arv, siis Eestis on pikalt olnud esikohal laua- või sülearvuti ja alles viimasest uuringust 2019. aastal on näha, et kasutus on jõudnud peaaegu võrdsele tasemele. Tahvelarvuti kasutamine ei ole Eestis kunagi saavutanud sellist taset kui Euroopas keskmiselt. Televiisorist interneti kasutamine oli populaarseim 2018. aastal, et siis aasta hiljem taas väheneda. Mängukonsoole kasutatakse väga vähe.

Nutitelefoniga kaasnevad samasugused turvariskid kui arvutiga. Riigi Infosüsteemide Amet soovitab kasutada näo- ja sõrmejäljetuvastuse asemel pigem traditsioonilist PIN-koodi ja parooli ning ekraani automaatset lukustussüsteemi (19 soovitust, kuidas muuta …).



	Nutitelefon	Laua- või sülearvuti	Tahvelarvuti	TV	Mängukonsoolid
2012	24%	64%	4%		
2013	32%	71%	12%	3%	
2014	55%	96%	28%	9%	
2017	73%	91%	37%	21%	
2018	76%	90%	32%	25%	7%
2019	81%	83%	29%	20%	5%

JOONIS 3. EESTLASTE ENIM LEVINUD SEADMED INTERNETI KASUTAMISEKS

Tabelist 1 ja 2 näeme, et valdav osa EL-i ja Eesti internetikasutajatest teevad seda e-posti haldamiseks, kuid loevad ka uudiseid, tegutsevad suhtlusvõrgustikes, ostavad veebist kaupu või teenuseid ja müüvad neid või tegelevad internetipangandusega, kuid eestlased teevad kõiki neid tegevusi internetis Euroopa keskmisest märksa sagedamini. Kõige vähem levinud veebitegevuseks 2018. ja 2019. aastal oli Euroopas e-õpe (16%), Eestis oli e-õpe juba enne pandeemiat suhteliselt populaarne (vt tabel 2). Kuid praegu veel puuduvad pandeemiaaegsed ja -järgsed uuringutulemused, mis võivad seada e-õppe keskkondade kasutamine esmaseks internetti sisenemise põhjuseks.

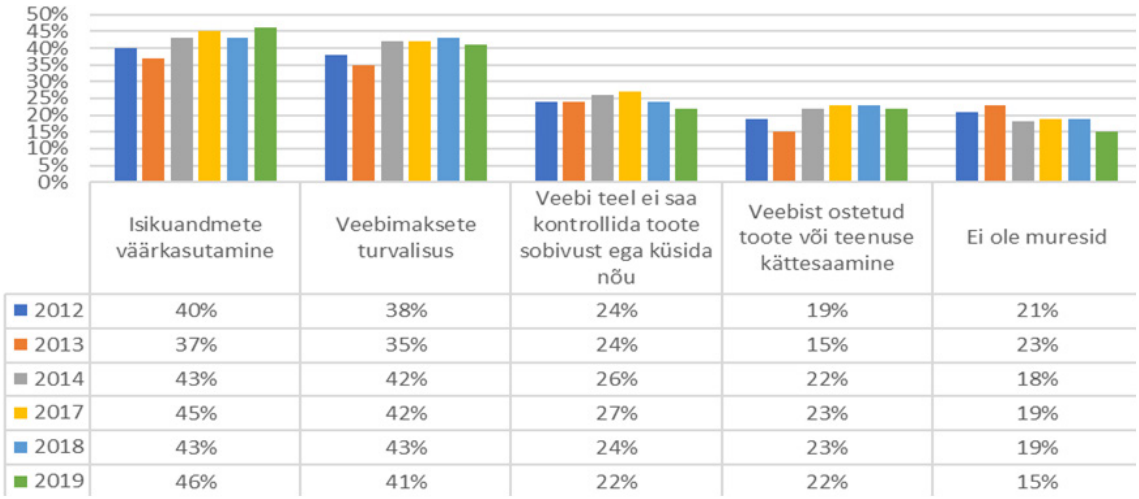
TABEL 1. EUROOPLASTE ENIM LEVINUD TEGEVUSED INTERNETIS

	2012	2013	2014	2017	2018	2019
E-postkasti kasutamiseks	85%	84%	86%	83%	80%	80%
Uudiste, blogide, foorumite lugemiseks	64%	60%	63%	70%	69%	62%
Sotsiaalmeedia sirvimiseks	52%	53%	60%	67%	62%	62%
Internetipanga kasutamiseks	52%	48%	54%	58%	59%	61%
Teenuste ja toodete ostmiseks	48%	50%	57%	60%	57%	55%
Kiireks sõnumivahetuseks						51%
Veebipõhiste video- ja audiokõnede tegemiseks						41%
Meelelahutuseks (mängud, TV)	27%	46%	52%	64%	59%	40%
Avalike teenuste kasutamiseks						36%
Kaupade või teenuste müümiseks	20%	18%	23%	24%	24%	22%
E-õppeks		16%	16%		16%	16%

TABEL 2. ENIM LEVINUD TEGEVUSED EESTI INTERNETIKASUTAJATE HULGAS

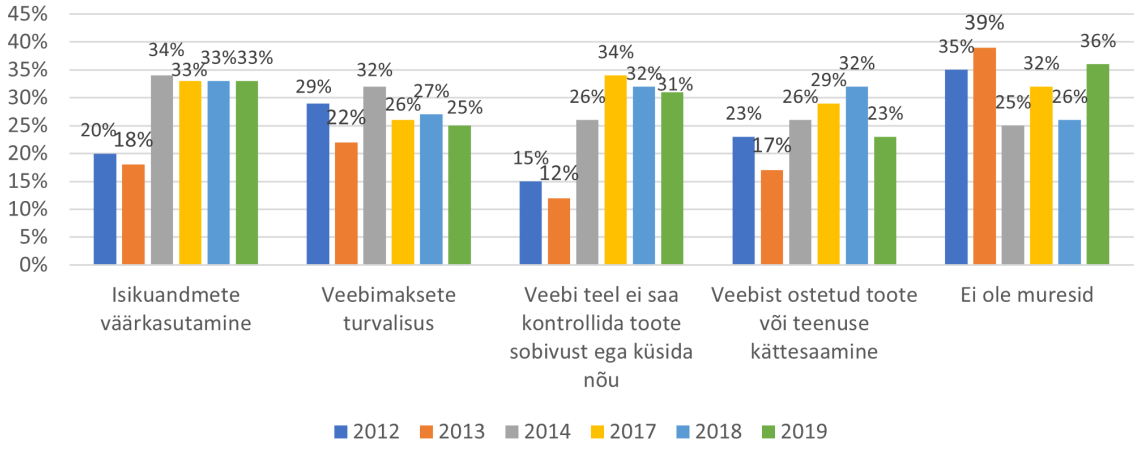
	2012	2013	2014	2017	2018	2019
E-postkasti kasutamiseks	89%	89%	92%	90%	88%	84%
Uudiste, blogide, foorumite lugemiseks	87%	85%	90%	93%	85%	79%
Sotsiaalmeedia sirvimiseks	56%	62%	63%	73%	64%	70%
Internetipanga kasutamiseks	85%	85%	89%	86%	83%	84%
Teenuste ja toodete ostmiseks	46%	41%	56%	60%	59%	59%
Kiireks sõnumivahetuseks						46%
Veebipõhiste video- ja audiokõnede tegemiseks						45%
Meelelahutuseks (mängud, TV)	29%	57%	59%	77%	61%	38%
Avalike teenuste kasutamiseks					67%	65%
Kaupade või teenuste müümiseks	19%	16%	17%	21%	24%	20%
E-õppeks					32%	21%

Enamik EL-i internetikasutajaid tunneb muret identiteedivarguse ja veebimaksete turvalisuse pärast, samas kui eestlasi paneb lisaks isikuandmete väärkasutamisele muretsema just veebiostlemine. Teisalt on eestlased võrdlemisi muretud: 2019. aastal oli lausa 39% neid, keda ükski neist probleemidest ei puudutanud, samas kui EL-i keskmine oli 15% (vt joonis 4 ja 5).



	Isikuandmete väärkasutamine	Veebimaksete turvalisus	Veebi teel ei saa kontrollida toote sobivust ega küsida nõu	Veebist ostetud toote või teenuse kättesaamine	Ei ole muresid
2012	40%	38%	24%	19%	21%
2013	37%	35%	24%	15%	23%
2014	43%	42%	26%	22%	18%
2017	45%	42%	27%	23%	19%
2018	43%	43%	24%	23%	19%
2019	46%	41%	22%	22%	15%

JOONIS 4. EUROOPLASI ENIM MURETSEMA PANEVAD ASJAOLUD INTERNETI KASUTAMISEL



JOONIS 5. EESTLASI ENIM MURETSEMA PANEVAD ASJAOLUD INTERNETI KASUTAMISEL

Internetikasutajad on muutunud iga uuringuga ohtudest järjest teadlikumaks ja vastavalt sellele muutnud oma küberkäitumist mitmel viisil. Näiteks välditakse oma isikuandmete avaldamist internetis, ei avata kunagi e-kirju tundmatutelt inimestelt, on installitud viirusetõrjetarkvara, külastatakse ainult tuntud ja usaldusväärseid veebisaite ning kasutatakse ainult oma arvutit. Siiski tekitab muret, et internetikasutajad nii EL-is kui ka Eestis ei vaheta piisava regulaarsusega oma võrguparoole ning vaid umbes 1/3 kasutab erinevaid paroole eri kontode jaoks. Ka privaatsussätete muutmise vajadus juurdub vaevaliselt.

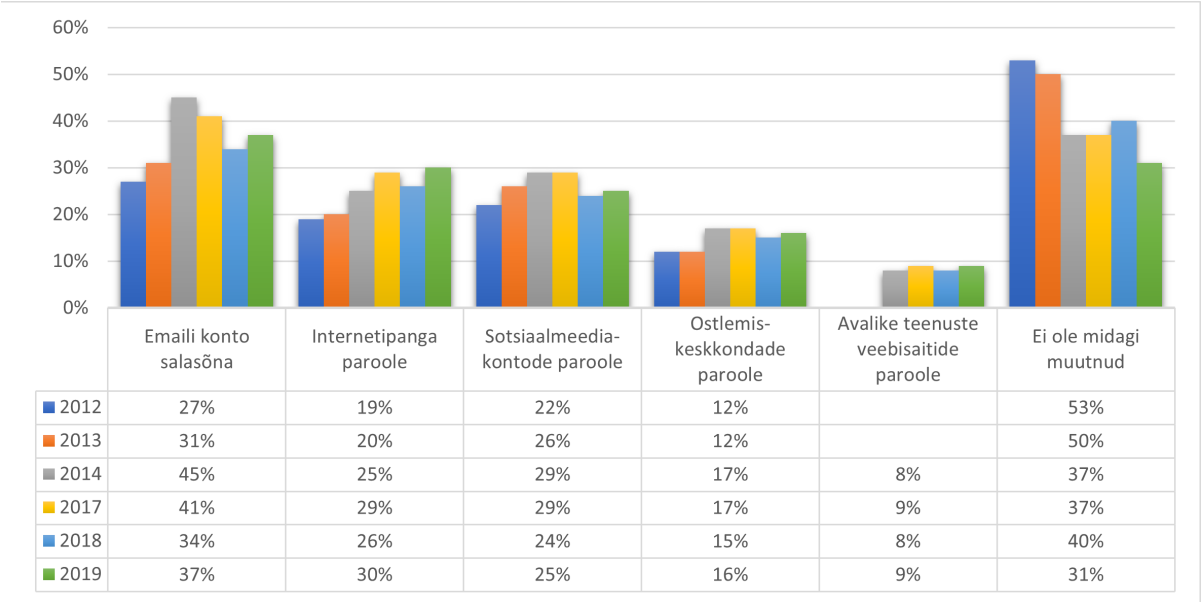
TABEL 3. KÜBERKÄITUMISE MUUTUMISE TRENDID EL-IS TERVIKUNA

	2012	2013	2014	2017	2018	2019
Ei ava tundmatute isikute e-kirju	51%	40%	49%	35%	45%	42%
Viirustõrjeprogrammi installeerimine	34%	46%	61%	45%	47%	42%
Ainult usaldusväärsete veebikeskkondade kasutamine	34%	32%	36%	27%	32%	32%
Ainult isikliku arvuti kasutamine	29%	26%	38%	36%	34%	32%
Pigem ei sisesta veebisaitidele oma isikuandmeid		34%	38%	39%	37%	30%
Kasutab erinevaid paroole eri kontode jaoks	25%	24%	31%	28%	29%	29%
Kasutab varasemast keerulisemaid paroole					27%	26%
Ei ühenda oma seadet internetti läbi turvamata kuumkoha						23%
Vahetab regulaarselt paroole	45%	16%	27%	25%	21%	21%
On muutnud oma privaatsussätteid	16%	16%	18%	20%	17%	13%
Pigem ei kasuta internetipanka	15%	15%	12%	10%	9%	8%
Pigem ei osta tooteid ja teenuseid internetist	18%	17%	13%	11%	11%	10%
On tühistanud pettuskahtluse korral veebipõhise ostu sooritamise		6%	7%	11%	10%	9%
Kasutab paroolihaldurit						7%

TABEL 4. KÜBERKÄITUMISE MUUTUMISE TRENDID EESTIS

	2012	2013	2014	2017	2018	2019
Ei ava tundmatute isikute e-kirju	57%	55%	64%	42%	57%	64%
Viirustõrjeprogrammi installeerimine	57%	59%	67%	41%	53%	50%
Ainult usaldusväärsete veebikeskkondade kasutamine	40%	34%	42%	29%	39%	41%
Ainult isikliku arvuti kasutamine	35%	28%	45%	39%	36%	43%
Pigem ei sisesta veebisaitidele oma isikuandmeid	30%	24%	33%	31%	33%	33%
Kasutab varasemast keerulisemaid paroole					26%	27%
Kasutab erinevaid paroole eri kontode jaoks	30%	26%	37%	27%	34%	32%
Ei ühenda oma seadet internetti läbi turvamata kuumkoha						23%
Vahetab regulaarselt paroole			34%	22%	24%	17%
On muutnud oma privaatsussätteid	3%	15%	16%	19%	16%	16%
Pigem ei kasuta internetipanka	11%	4%	5%	3%	1%	3%
Pigem ei osta tooteid ja teenuseid internetist	14%	10%	11%	8%	7%	6%
On tühistanud pettuskahtluse korral veebipõhise ostu sooritamise		8%	11%	10%	14%	12%
Kasutab paroolihaldurit						6%

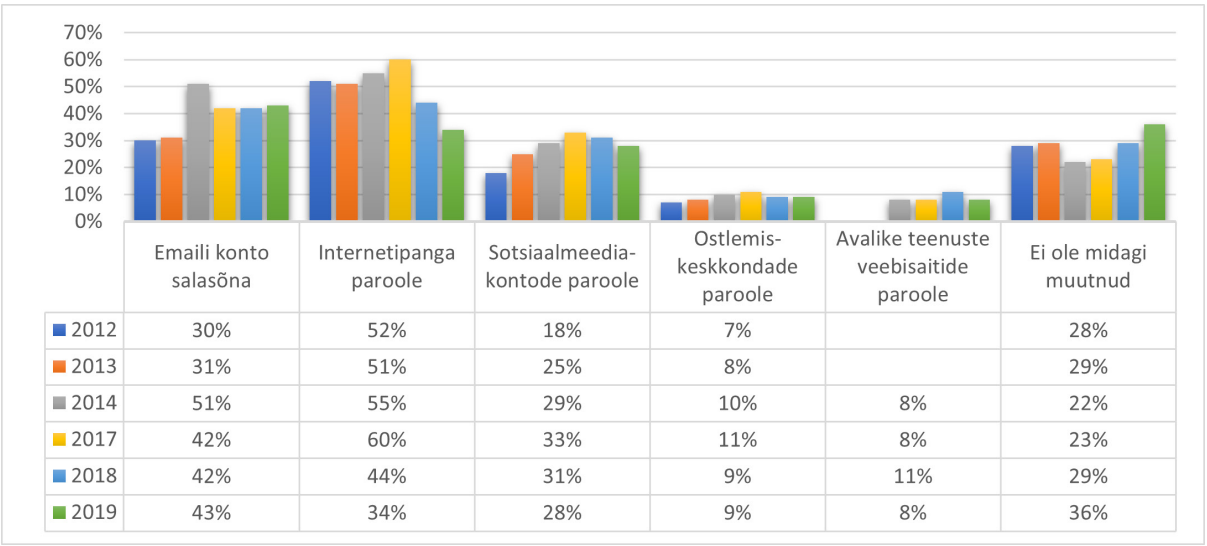
Paroolihaldus on võtmesõna oma isikliku ja tööarvuti ning kontodele sissehäkkimise takistamisel. Enamik internetti kasutavatest vastajatest on muutnud oma parooli vähemalt ühe kasutatava teenuse jaoks viimase 12 kuu jooksul. Jooniselt 6 ja 7 näeme, et kõige sagedamini muudeti meilikonto paroole, järgnesid internetipanganduse ja veebipõhise suhtlusvõrgustiku paroolid. Ostuveebisaitide ja avalike teenuste paroole ei olda nii varmad vahetama. Küllap on põhjus selles, et avalike teenuste veebisaite usaldatakse ning ostlemisest on saanud igapäevane tegevus ja kasutatakse juba usalduse võitnud ostukeskkondi.



	Emaili konto salasõna	Internetipanga paroole	Sotsiaalmeedia-kontode paroole	Ostlemis-keskkondade paroole	Avalike teenuste veebisaitide paroole	Ei ole midagi muutnud
2012	27%	19%	22%	12%		53%
2013	31%	20%	26%	12%		50%
2014	45%	25%	29%	17%	8%	37%
2017	41%	29%	29%	17%	9%	37%
2018	34%	26%	24%	15%	8%	40%
2019	37%	30%	25%	16%	9%	31%

JOONIS 6. KÜSITLUSELE EELNENUD VIIMASE 12 KUU JOOKSUL TOIMUNUD PAROOLIMUUDATUSED EL-IS

Pikemas perspektiivis on näha, et keskmiselt väheneb nende inimest osakaal EL-is, kes oma paroolide haldusega ei tegele, Eestis aga pärast mõneaastast langust 2014. ja 2017. aastal on selliste internetikasutajate arv taas kasvanud.



	Emaili konto salasõna	Internetipanga paroole	Sotsiaalmeedia-kontode paroole	Ostlemis-keskkondade paroole	Avalike teenuste veebisaitide paroole	Ei ole midagi muutnud
2012	30%	52%	18%	7%		28%
2013	31%	51%	25%	8%		29%
2014	51%	55%	29%	10%	8%	22%
2017	42%	60%	33%	11%	8%	23%
2018	42%	44%	31%	9%	11%	29%
2019	43%	34%	28%	9%	8%	36%

JOONIS 7. KÜSITLUSELE EELNENUD VIIMASE 12 KUU JOOKSUL TOIMUNUD PAROOLIMUUDATUSED EESTIS

Eurobaromeeter uurib ka, kas EL-i kodanikud on küberkuritegevusest midagi kuulnud ja kui hästi nad end küberkuritegevuse ohtudest informeerituna tunnevad. Vaadeldakse internetikasutajate suhtumist küberturvalisusesse, seda, kas nad on kogenud küberkuritegevust või langenud selle ohvriks, kui palju nad selle pärast muretsevad ja kelle poole nad pöörduksid või kellega võtaksid ühendust, kui kogeksid või langeksid küberkuritegevuse ohvriks või märkaksid midagi, mida võiks pidada küberrünnakuks. Enamikus Euroopa riikides peavad vähem kui pooled vastanutest end hästi informeerituks küberkuritegevuse ohtudest. Üha rohkem vastajaid on mures küberkuritegevuse eri vormide

ohvriks langemise või selle võimaliku kogemise pärast, kuid vähesed on seda ka tegelikult kogenud. Vastajate kõige levinumad toimingud laste kaitsmiseks veebis olid laste internetikasutuse jälgimine ja piiramine või lastega internetiriskidest rääkimine.

Kanadas alustati 2018. aastal regulaarset statistiliste andmete kogumist, mida nimetatakse Kanada küberturvalisuse ja küberkuritegevuse uuringuteks. Selle iga kahe aasta tagant toimuva uuringu eesmärk on koguda andmeid küberkuritegevuse mõju kohta Kanada ettevõtetele ja nende mõju leevendamise kohta. Uuringuga saadakse teavet küberturvalisuse meetmetesse investeerimise, küberturvalisuse koolituse, küberturvaintsidentide mahu, tüüpide ja nendele intsidentidele reageerimisega ning neid ennetavate tegevustega kaasnevate kulude kohta. Andmeid kogutakse vastavalt statistikaseadusele. Küsimustik on elektrooniline, mõeldud eelkõige ettevõtete juhtidele ja/või IT-töötajatele ning näiteks 2022. aasta küsimustik sisaldas 44 küsimust (Canadian Survey of Cyber Security and Cybercrime, 2022).

12. novembrist 2018 kuni 9. jaanuarini 2019 tehti Ühendkuningriigis elanikkonna uuring: 1350 telefoniintervjuud vähemat 16-aastaste inimestega. Selle kvantitatiivse uuringu eesmärk oli mõõta ja mõista elanikkonna teadlikkust ja suhtumist küberturvalisusesse ja sellega seotud käitumisse. Uuring oli osa laiemast uurimisprojektist, mille eesmärk oli anda valitsusele sisend edaspidiseks tegevuseks, et julgustada avalikkust küberohtudest hoidumisel positiivselt käituma. Tulemused näitasid, et vaid 15% inimestest on veendunud, et oskavad end veebis kaitsta. Nooremad ja jõukamad vastajad on teadlikumad ja kasutavad tõenäolisemalt kaitsemeetmeid. Peaaegu pooled nõustusid, et enamik teavet selle kohta, kuidas käituda internetis turvaliselt, tekitab pigem segadust. 80% ütles, et küberjulgeolek on väga oluline, kuid see ei tähenda, et nad rakendaksid kaitsemeetmeid. 21% vastanutest kasutas paroolide salvestamisel paroolihalduri abil ja 75% kasutas seadmete avamiseks parooli/pääsukoodi/PIN-koodi. Kõige levinumad veebiturvalisuse kaalutlused olid oma privaatsuse kaitsmine ja rahavarguse vältimine. 70% respondentidest uskus, et nad langevad järgmise kahe aasta jooksul tõenäoliselt vähemalt üht kindlat tüüpi küberkuritegevuse ohvriks. Veidi enam kui iga kolmas nõustus, et raha või isiklike andmete kaotamine interneti kaudu on tänapäeval vältimatu. Iga kolmas lootis küberturvalisuse osas mingil määral sõprade või pere abile, 65-aastased ja vanemad inimesed on eriti sõltuvad pereliikmetest. (UK Cyber Survey Key findings – General public, 2019)

Alates 2016. aastast tehakse Ühendkuningriigis ettevõtete, heategevusorganisatsioonide ja haridusasutuste küberturvalisuse rikkumiste uuringuid. See aitab organisatsioonidel mõista küberjulgeolekuohtude olemust ja olulisust ning seda, mida teised turvalisuse tagamiseks teevad. Samuti toetab see valitsust küberturvalisuse poliitika kujundamisel. Selle aja jooksul on organisatsioonid seisnud silmitsi oluliste ülesannetega ja muutustega oma töös, seetõttu on toimunud ka muutusi selles, kuidas nad küberturvalisusse suhtuvad ja sellele lähenevad, samuti kohanemis- ja reageerimisviisis üha arenevatele ohtudele. Viimase uuringu tulemused näitasid, et organisatsioonide küberhügieenis on arenguruumi. On selge, et kübervastupidavust mõjutab suuresti juhtkonna käitumine. Kuigi küberturvalisust tähtsustatakse kõrgelt, ei tähenda see suurt asjatundlikkust. Lisaks ei suuda IT-töötajad sageli juhtkonnale põhjendada, miks tuleb küberturvalisusse rohkem panustada, mis mõjutab oluliselt ettevõtete võimet teha tõhusaid küberturvalisusega seotud otsuseid. See tähendab, et sageli ei investeerita olulistesse valdkondadesse, mis suurendaksid organisatsiooni küberturvalisust. See toob kaasa reaktiivse lähenemise küberintsidentidele, mitte aga proaktiivse lähenemis küberriski piiramisel. See on valdkond, mida plaanitakse järgmistel aastatel tähelepanelikumalt jälgida (Cyber Security Breaches Survey 2022).

23.–24. märtsini 2022 uuriti Prantsusmaal elanikkonna suhtumist küberturvalisusesse. Uuringus osales 983 inimest, kes moodustasid esindusliku valimi 18-aastastest ja vanematest Prantsusmaa elanikest. 82% prantslastest ütleb, et nad on mures küberrünnakute ülemaailmsete ohtude pärast. Küberturvalisusega seotud riskid ei ole kaugeltki abstraktsed ohud, vaid puudutavad paljusid prantslasi. Iga kolmas prantslane on juba langenud eduka internetihäkkimise ohvriks, paljud on kogenud riskantseid olukordi. Peaaegu iga teine prantslane (48%) on olnud häkkimiskatse objekt. Peaaegu iga kolmas (31%) on olnud eduka rünnaku ohver. Kuigi üle poole vastanutest tunneb, et nad on halvasti informeeritud, kuidas nende andmeid kasutatakse, näitab uuring erinevat usaldust osaliste vastu, kellele prantslased oma andmed usaldavad. Usaldusväärsemad näivad olevat eelkõige tervishoiutöötajad, pangad, maksuamet ja riiklik ravikindlustussüsteem. Riigivõimudes nähakse kaitset küberrünnakute vastu ja oma isikuandmete kaitses (Mercier, 2022).

4. POPULAARSEMAD METOODIKAD KÜBERTEADLIKKUSE UURIMISEKS

Kuigi elanikkonna massuuringud on olulised ja näitavad trende küberhügieeni teadlikkuse suurenemise või hoolimatu käitumise sagenemise kohta, siis kõige sagedasemad on küberturvanõuete rikkumised organisatsioonides ja neid seostatakse enamasti pigem inimlike vigadega, mida on võimalik vältida inimeste küberhügieeni regulaarselt hinnates-mõõtes ja neid koolitades. Küberkuritegevus on üsna noor teadusliku uurimise valdkond, mis on pakkunud huvi nii akadeemilisteks uuringuteks kui ka praktiliseks tegevuseks. Juba 2005. aastal märgiti ekspertide puudust ja infoturbe uuringute vähesust inimtegurite ja inimlike vigade kohta. Schultz (2005) on välja toonud, kui oluline on mõista, kuidas töökeskkond ja töökultuur mõjutavad töötajate teadlikkuse arengut, et järgida korralikku turvalisusele orienteeritud käitumist. Võimalused inimloomust suhteliselt lihtsalt ära kasutada on tekitanud olukorra, kus mitmed ründed keskenduvad inimlikele nõrkustele. Vaja on suurendada organisatsioonide ja nende töötajate teadlikkust infoturbest ning edendada nende võimet küberturvalisusega seotud ebaturvalise käitumisega tegeleda (Mäses, 2015). Sellised tegurid nagu sugu ja vanus, aga ka haridustase, võivad mõjutada käitumist küberjulgeoleku valdkonnas (Hadlington, 2017). Selleks et vähendada infoturbe inimfaktoriga seonduvaid riske, on välja töötatud mitmeid usaldusväärseid skaalasid ja metoodikaid, et mõõta riskantseid hoiakuid ja käitumist seoses organisatsiooni teabeturbega. Allpool tutvustatakse neist kõige asjakohasemaid.

Parsonsi jt poolt välja töötatud infoturbe inimaspektide küsimustik HAIS-Q (Parsons *et al.*, 2014) on meetod infoturbeteadlikkuse (*Information Security Awareness*, ISA) hindamiseks organisatsiooni sees. Meetodit on kasutatud väga erinevate elanikkonnarühmade, sealhulgas üliõpilaste, valitsusasutuste ja finantsinstitutsioonide töötajate küberturvalisuse teadlikkuse hindamiseks (Parsons *et al.*, 2017). Meetodit on mitu korda eelretsenseeritud ja seda loetakse kehtivaks. Meetod põhineb kolmel teguril: hoiak, käitumine ja teadmised. Testis hinnatakse, kus töötajatel või õpilastel on vajakajäämisi infoturbe vallas. Kuigi kellelgi võib olla positiivne hoiak kehtivate tõekspidamiste või reeglite järgimisel, ei pruugi samal isikul olla piisavaid teadmisi infoturbe kohta üldiselt. Organisatsioonikultuur võib mõjutada inimese käitumist, aga ka rikkumiste arvu organisatsioonis (McCormac *et al.*, 2017).

Küsitlus koosneb 63 küsimusest, mis on järjestatud skaalal 1–5, kus 1 tähendab „ei nõustu" ja 5 „täiesti nõus". Samas on HAIS-Q uuringut tehtud ka nelja modifitseeritud Likerti skaalaga, kus on välja jäetud nn mugavusskaala „ei oska vastata". Sellega eemaldatakse neutraalsed vastused, et vältida eelarvamusi, subjektiivsust ja erapoolikust (Ranas *et al*., 2020). Parsons jt (Parsons *et al*., 2014) usuvad, et teadmiste, suhtumise ja käitumise suhe on olemas ning seda mõjutavad paljud individuaalsed, sekkumis- ja organisatsioonilised tegurid.

Egelman ja Peer on töötanud välja turvakäitumise kavatsuste skaala (SeBIS). See mõõdab lõppkasutajate suhtumist arvutiturbesse. Vaatamata lõppkasutajatele pakutavatele turvanõuannete ja veebipõhiste koolitusmaterjalide rohkusele pole lõppkasutajate turvalise käitumise jaoks standardset mõõtmisvahendit. Autorid selgitasid esmalt välja kõige levinumad arvutiturbenõuanded, mida eksperdid lõppkasutajatele pakuvad, et koostada Likerti skaala küsimuste kogum, mille abil uurida, millisel määral vastajad väidavad, et järgivad neid nõuandeid. Kuna kavatsused on planeeritud käitumise eeltingimus, on see skaala kasulik kasutajate arvutiturvalisuse käitumise ennustamiseks. Nad jälgisid, et iga küsimus oleks kohaldatav suurele osale elanikkonnast, et vastajate vahel oleks piisav erinevus ja neil oleks suur usaldusväärsus (st soovitavad psühhomeetrilised omadused). Pärast nii uuriva kui ka kinnitava faktoranalüüsi tegemist tuvastati 16-punktiline skaala, mis koosneb neljast alamskaalast, mis mõõdab suhtumist paroolide valimisse, digiseadmete kaitsesse, ennetavasse kaasamisse ja tuvastamisse ning lõpuks tarkvarauuendusse. (Egelman & Peer, 2015)

Ögütçü jt töötasid välja mõõdiku, mille abil seostada küberturvalisusega seotud käitumist erinevate kohusetundlikkuse tasemetega. Kuna organisatsioonide infoturbega seotud varasid haldavad ja juhivad inimesed, on enamasti infoturbe nõrgim lüli vähese küberteadlikkusega inimene (Abawajy, 2014; Arce, 2003). Kuigi infoturbe riske ei saa iial täielikult eemaldada, saab neid riske minimeerida talutava tasemeni, kui arendada küberteadlikkust ja muuta selle tavapäraseks käitumiseks. Mõõdik saadi nelja eri skaala abil: riskantse käitumise skaala (RBS) – sellega mõõdetakse kasutajate käitumist infosüsteemidega ja see näitab, kui kasutatakse arvutit ilma turvameetmeteta ja pannakse sellega ohtu nii iseennast kui ka inimesi, kellega elatakse või töötatakse koos; konservatiivse käitumise skaala (CBS) – selle eesmärk on mõõta kasutaja tegevust infosüsteemi kasutamisel, see määrab konkreetsed toimingud, mida kasutajad oma teabe kaitsmiseks ette võtavad; ekspositsiooni skaala (EOS) – selle eesmärk on mõõta kasutajate kokkupuudet mis tahes küberjulgeolekuohuga, tõstes esile kokkupuute kasutaja käitumisest ja sündmustest tulenevate riskide, ohtude ja mõju suhtes; ja riskitaju skaala (RPS) – see mõõdab riskitaset või ohtu, mis tabab infotehnoloogiakasutajat, ning on seotud usaldusväljaga, mis kasutajal on võimalike küberrünnakute ees (Öğütçü, 2016; Benavides-Astudillo *et al*., 2022). Skaalad ja skaalaküsimused töötati välja olemasoleva kirjanduse ja valdkonna juhtivate spetsialistide eksperdiarvamuste põhjal. Üsna oluline on kindlaks teha teadlikkuse tase, kuna teadlikkus ja käitumine on väga lähedalt seotud. Kuid mõnel juhul võib teadlikkus olla suur, kuid käitumine ei pruugi siiski olla asjakohane.

Lee Hadlingtoni väljatöötatud metoodika hõlmas inimtegurite mõju juhuslikele või oportunistlikele siseringirünnakutele organisatsioonides (Hadlington, 2018). Kõigepealt iseloomustas Hadlington neid inimtegureid, mis võivad viia selleni, et üksikisik võib muutuda ohuks. Lisaks töötas ta välja võtmeraamistikke selliste ohtude leevendamiseks. Edasine teadustöö käsitles küberturvalisuse riskantse käitumise, ärikeskkonna küberturvalisusesse suhtumise, internetisõltuvuse ja impulsiivsuse vahelist seost. Selles uuringus esitas Hadlington järgmised skaalad: lühendatud impulsiivsuse skaala (ABIS), veebipõhise tunnetuse skaala (OCS), riskantse küberturvalisuse käitumise skaala (RScB)

ning skaala suhtumise kohta küberturvalisusesse ja küberkuritegevusesse ettevõtluses (ATCIB) (Hadlington, 2018).

Aivazpour ja Rao (2018) kordasid Hadlingtoni tööd ja jõudsid järeldusele, et tema uurimistöö koos Egelmani ja Peeri uurimistööga (Egelman & Peer, 2015) võiks olla hea lähtepunkt riskantse küberturvalisuse käitumise impulsiivsuse uurimiseks. Aivazpouri järeldustes mainitud vajadus töötada välja RScB ja ATC-IB skaalad ajendasid Hadlingtoni neid täiustama. Ta hakkas uurima, kas ettevõtte suurus, vanus või hoiakud mõjutavad töötajate suhteid riskantse küberjulgeoleku käitumise ja üldise teadlikkusega küberkuritegevusest (Aivazpour & Rao, 2018; Nunes *et al.*, 2021).

5. EESTIS TEHTUD KÜBERTURVALISUSE TEADLIKKUSE UURINGUD

Eestis on elanikkonna eri gruppide küberteadmisi ja küberhügieeni uuritud juba aastaid. 2015. aastal kaitses Tallinna Tehnikaülikoolis küberkriminalistika ja küberjulgeoleku keskuses magistritöö „Infoturbe inimfaktori hindamismeetod" Sten Mäses (2015), kes katsetas Eestis esimest korda Parsonsi jt (2014) teadmise-suhtumise-käitumise (*knowledge-attitude-behaviour* (KAB)) mudelit, et määrata töötajate küberteadlikkust. Tema töö eesmärk oli esitleda meetodit, mis võimaldab töötajatel hinnata oma infoturbega seonduvaid teadmisi, suhtumist ja käitumist eri valdkondade kaupa. Magistritöö tarbeks arendas ta spetsiaalselt välja interaktiivse veebipõhise testi (https://testing.planet.ee/), mis annab sooritajale kohese tagasiside ning loetleb üles tema hinnangulised tugevused ja nõrkused. Lisaks kuvatakse testi läbinud töötajale soovitused turvateadliku käitumise parandamiseks. Paraku on test vaid ingliskeelne, mis seab keeleoskuse piirangu selle kasutamisel inimeste küberteadlikkuse hindamiseks (Mäses, 2015, lk 5).

Alex Bindevaldi Tallinna Tehnikaülikoolis 2021. aastal kaitstud magistritöö „Küberturvalisus koolides – väljakutsed, võimalused ja vajadused CTFlahenduse järele" eesmärk oli välja selgitada, mida ja kuidas õpetatakse küberkaitsest üldhariduskoolides ning milliseid õppekavaväliseid tegevusi saavad õpilased küberkaitse õppimiseks kasutada. Uuringu tulemused näitasid, et praegu on küberturvalisuse õpetamiseks olemas õppekava põhikoolis ja gümnaasiumis, aga kuna koolidel on endil võimalus valida, mida õpetada, siis õpetatakse küberhügieeni vähestes koolides. Lisaks saab õpilane küberturvalisusega seotud oskusi omandada suvelaagritest, treeningkeskkondadest ja küberturvalisuse võistlustelt. (Bindevald, 2021, lk 4)

Tiia Sõmer kaitses 2022. aastal doktoritöö teemal „Finantsiliselt motiveeritud küberkuritegevuse modelleerimine". Väitekirjas kasutas ta küberkuritegevuse mõistmiseks interdistsiplinaarset lähenemist ja arvutiteadustes traditsiooniliselt mittekasutatavaid sotsiaalteaduslikke meetodeid. Selline lähenemine annab teistsuguse vaate küberkuritegevuse kohta, mis omakorda pakub lisavõimalusi kuritegude uurimiseks ja ennetamiseks, vastumeetmete väljatöötamiseks või teadlikkuse suurendamiseks. (Sõmer, 2022)

Alates 2017. aastast on korraldatud kooliõpilaste iga-aastast uuringut KüberPähkel. KüberPähkel on koodnimi Kaitseministeeriumi ellu kutsutud ja Tallinna Tehnikaülikooli küberkriminalistika ja küberjulgeoleku keskuse läbiviidavale uuringule, mille käigus testitakse põhikooli-, gümnaasiumi- ja kutsekoolide õpilasi. Keskendutakse digitaalse ohutuse ja küberkaitse teadmistele, näiteks privaatsus ja turvalisus (millised andmed on

mõistlik internetti jagada, millised mitte, kus oman kontot ja milline on hea parool), tehniline taip (mida teha enne kui oma arvuti müüki panna, kuidas lukustada nutiseadme ekraan turvaliselt), küberkaitsealane probleemilahendusoskus (kuidas tuvastad, mis on toimunud ja leiad lahendusi), käitumine internetis (kuidas olen ise targem ja saan teisi aidata, kui mure on vaja lahendada, kuidas tuvastan pahade eesmärkidega inimesed), probleemilahendusoskus (mida teha, kui asjad pole nii nagu need olema peaksid, kas oskad märgata valesti olevaid asju ja neile lahendus pakkuda).

2021. aastal toimus esimest korda KüberNööpnõel, mis on 1.–6. klassile mõeldud minitestimine/võistlus digitaalse ohutuse, küberturbe ja nuputamise valdkonnas.

Siseturvalisuse avaliku arvamuse uuringuid on tehtud alates 2016. aastast kaheaastase intervalli järel ning igas uuringus on küberturvalisuse osa muutunud järjest olulisemaks. Praeguseks on ilmunud kokku neli uuringuaruannet. Kogu riiki puudutavatest ohuolukordadest nägi 44% Eesti elanikest 2016. aastal küberkuritegevust kõige tõenäolisema ohuna, 2018. aastal ainult 27%, 2020. aastal 57% ja 2022. aastal juba 69% vastanutest. 2020. ja 2022. aasta uuringus on küberturvalisus aruandes juba eraldi peatükina ja hõlmab väga detailseid küsimusi. Näiteks küsiti, kui tõenäoliseks peetakse küberkuritegevuse eri liikide ja petuskeemide ohvriks langemist ning kas vastaja isiklikult on viimase 12 kuu jooksul sattunud küberkuritegevusega seotud olukordade ohvriks. Samuti uuriti, mida on vastaja viimase 12 kuu jooksul oma küberturvalisuse suurendamiseks teinud. Oma teadlikkust küberkuritegevusega seotud riskidest pidasid 2020. aastal väga heaks või heaks 58% vastanutest ja 2022. aastal 59% vastanutest. Võrreldes 2020. ja 2022. aasta uuringuid peeti 2022. aastal kõiki küberturvalisusega seotud ohte endisest tõenäolisemaks. Eriti paistavad selles osas silma järgmised küberkuritegevuse liigid: sotsiaalmeedia, panga- või muudele isiklikele andmetele ligipääs võõraste poolt, identiteedivargus ja oma salasõnade sisestamine võltsitud veebilehtedele. Vastajaid, kes ei ole midagi teinud oma küberturvalisuse tagamiseks, oli 2020. aastal 15% ja 2022. aastal 8%. Õnneks on vähe ka neid, kes on reaalselt küberkuritegevusega kokku puutunud. Samas nendest vähestest, kes siiski sattusid mõne küberkuriteo ohvriks viimase 12 kuu jooksul, ei teatanud 71% sellest politseisse või mujale ametiasutusse (Siseturvalisuse avaliku arvamuse uuring, 2016; Siseturvalisuse avaliku arvamuse uuring, 2018; Siseturvalisuse avaliku arvamuse uuring, 2020; Siseturvalisuse avaliku arvamuse uuring, 2022).

Ajavahemikul 8. jaanuarist kuni 21. jaanuarini 2021 korraldas uuringufirma Saar Poll OÜ Sisekaitseakadeemia sisejulgeoleku instituudi uuringu käigus Eesti elanikkonna küsitluse, mille valim oli 1000 inimest. Küsitluse eesmärk oli muu hulgas välja selgitada isikuandmete turvalisuse olulisus Eesti elanikele ja mida peetakse tundlikeks isikuandmeteks; kuidas hindavad Eesti elanikud ohtu oma (digitaalsetele) isikuandmetele; missugused on Eesti elanike harjumused julgeolekualase informatsiooni tarbimisel jm. Tundlikeks isikuandmeteks peavad vastajad kõiki eriilmelisi isikuandmeid, mis tekivad kas riigi või eraettevõtte teenuse vahendusel ja mida ei tohiks ilma loata kasutada. Kõige tundlikemaks peetakse finantsandmeid, suhtlusandmeid (sh telefonivestlusi, e-kirju), terviseandmeid, perekonnaseisu, kodust aadressi ja telefoninumbrit. Kõige vähem tundlikeks aga nime, isikukoodi ja sünniaega. Küsitlusest selgus, et kõige suuremaks ohuks hinnatakse isikuandmete kuritarvitamist küberkujategijate poolt, samuti isikuandmete avalikuks saamist kellegi hooletuse või eksimuse tõttu. Kõige sagedamini peeti julgeolekuohuks küberrünnakuid ja -kuritegevust. Ka välisriikide infosõda ja/või valeinformatsiooni levitamist peeti suureks ohuks (Puusalu ja Marnot, 2021, lk 5–6).

Selle uuringu tulemusena nenditi, et elanikkonna teadlikkust küberohtudest, sh küberrünnakutest ja küberkuritegevusest, ning isikuandmetel lasuvate ohtude maandamisest/ennetamisest on vaja suurendada. Hinnang teadlikkusele näitab, et elanikkonna teadmi-

sed andmete kasutusest ja nende üle kontrolli omamisest on vähene. Teadlikkuse suurendamine ning heade kasutusharjumuste tutvustamine ja hoidmine riskide maandamiseks eeldab täiendavat ja pidevat teavitus- ja koolitustegevust (Elanikkonna küsitluse raport, 2021, lk 95).

KOKKUVÕTE

Elanikkonna küberkuritegevuse teadlikkuse uuringuid on Euroopas ja Eestis tehtud enam kui kümmekond aastat. Kuigi ekspertide sõnul ei ole küberkuritegevust kunagi võimalik täielikult likvideerida ja küberrünnakuid 100% vältida, on elanikkonna eri gruppide ja organisatsioonide töötajate koolitamine ja nende küberteadlikkuse pidev hindamine järjest olulisem. Küberkuritegevus kui üks kuritegevuse liike tungib järjest enam inimeste igapäevaellu ja ohustab sellega meie turvatunnet: kogu riiki puudutavatest ohuolukordadest nägi 2020. aastal 57% uuringule vastanutest küberkuritegevust kõige suurema ohuna ja 2022. aastal juba 69%. Nii Eurobaromeetri uuringute tulemused, siseturvalisuse avalike uuringute tulemused kui ka Riigi Infosüsteemide Ameti andmed näitavad, et Euroopa Liidu ja ka Eesti inimeste küberhügieeni harjumused paranevad jõudsalt. Kõige enam on paranenud paroolide tugevuse küsimus kõikides vanuserühmades.

Kuid küberpettuste laviin ei näita vaibumise märke. Küberkuritegevuses on alati kaks aspekti: tehniline ja sotsiaalne. Üle 95% küberrünnakutest toimub inimeste vastu, seega kasutatakse ära inimlikke nõrkusi: kurjategijad mängivad inimeste ahnuse, tunnete, õnnega jms. Kuidas vähendada ohvreid tavakodanike hulgas ning kuidas kaitsta olulisi avalikke ja eraorganisatsioone oma töötajate riskantsest küberkäitumisest tingitud tagajärgede eest? Murelikuks teevad Eurobaromeetri uuringute tulemused, kus paroolihaldusega ei tegele üldse peaaegu 1/3 Eesti internetikasutajatest. Viimased siseturvalisuse avalikud uuringud on siiski näidanud, et nende vastajate arv, kes ei tee enda küberohutuse tagamiseks midagi, väheneb jõudsalt: kui 2020. aastal oli selliseid vastajaid 15%, siis 2022. aasta uuringus vaid 8%. Infoturbe olulisuse teadlikkust tuleb pidevalt suurendada, sest infoturve on ühest küljest küll tehniline probleem, kuid seda mõjutab ja selle muudab haavatavaks just inimeste hoolimatus või teadmatus.

Kuigi elanikkonda hõlmavad uuringud on küberhügieeni trendide väljaselgitamiseks väga olulised ning tänu just Eurobaromeetri uuringutele ja nüüd ka üha tõsisemalt ja detailsemalt küberturvalisust käsitlevatele Eesti siseturvalisuse avalikele uuringutele on olnud võimalik neid trende juba paar aastakümmet jälgida, on edaspidi vaja keskenduda elanikkonna eri gruppide ning organisatsioonide töötajate infoturbe- ja küberturvalisusalastele teadmistele, hoiakutele, oskustele ja tegelikule käitumisele. On selge, et juhtkonnal on määrav roll kübervastupidavuse suurendamisel ja ohtude ennetamisel – sageli ei mõisteta, et küberturvalisusse tuleks rohkem panustada, ka töötajate küberkäitumist mõõtes, tulemusi hinnates ja selle põhjal otsustada koolitusvajadus.

Eestis on juba tehtud küberturvalisuse teadusuuringuid, maailmas on välja töötatud mitmeid häid ja läbiproovitud metoodikaid, millega süsteemselt mõõta näiteks tervishoiutöötajate, ülikoolide ja kõrgkoolide tudengite ja töötajate, mäluasutuste töötajate jt küberturvalisuse teadmisi ja hoiakuid. Nende uuringute põhjal saab otsustada, milliseid

koolitusi konkreetne sihtgrupp või organisatsioon vajab. See on valdkond, millele tuleks lähitulevikus üha rohkem keskenduda.

Kuigi elukestva õppe strateegia 2014–2020 raames sooviti tagada, et digioskusi puudutavad kompetentsid sisaldavad ka küberturvalisust ning õppekavadesse integreeritakse lisaks digitehnoloogiale ka küberturvalisusega seonduvaid elementaarseid teadmisi, näitas Alex Bindevaldi 2021. aastal kaitstud magistritöö, et kuigi küberturvalisuse õpetamiseks on olemas valikaine õppekava põhikoolis ja gümnaasiumis, siis tegelikult õpetatakse küberhügieeni vähestes koolides. Küberturvalisus tuleks lõimida gümnaasiumide õppekavasse, luues nii eeldused küberteadlike kodanike järelkasvuks formaalharidussüsteemi kaudu.

KASUTATUD KIRJANDUS

Aaviksoo, J., 2010. Cyberattacks Against Estonia Raised Awareness of Cyberthreats. Defence Against Terrorism Review, 3(2), pp. 13–22. https://www.coedat.nato.int/publication/datr/volumes/datr6.pdf#page=18

Abawajy, J., 2014. User preference of cyber security awareness delivery methods, Behaviour & Information Technology, 33(3), pp. 237–248. https://doi.org/10.1080/0144929X.2012.708787

Aivazpour, Z. & Rao, V., 2018. Impulsivity and Risky Cybersecurity Behaviors: A Replication. AMCIS 2018 Proceedings. 2. https://www.researchgate.net/profile/Zahra-Aivazpour/publication/334726198_Impulsivity_and_Risky_Cybersecurity_Behaviors_A_Replication/links/60fb55722bf3553b29096e73/Impulsivity-and-Risky-Cybersecurity-Behaviors-A-Replication.pdf

Arce, I., 2003. The Weakest Link Revisited. IEEE Security ja Privacy, 1, pp. 72-76. https://informationsecurity.report/Resources/Whitepapers/7f28ebd7-7068-4c34-9655-2e182f86c463_TheWeakestLinkRevisited.pdf

Benavides-Astudillo, E., Silva-Ordonez, L., Rocohano-Ramos, R., Fuertes, W., Fernandez-Pena, F., Sanchez-Gordon, S. & Bastidas-Chalan, R., 2022. Analysis of Vulnerabilities Associated with Social Engineering Attacks Based on User Behavior. In M. Botto-Tobar, S. Montes León, P. Torres-Carrión, V. M. Zambrano & B. Durakovic, (Eds.), Applied Technologies. ICAT 2021. Communications in Computer and Information Science, 1535, pp. pp 351–364. Springer. https://doi.org/10.1007/978-3-031-03884-6_26

Bindevald, A., 2021. Küberturvalisus koolides - väljakutsed, võimalused ja vajadused CTF-lahenduse järele. Cyber Security at Schools - Challenges, Opportunities and Needs for CTF-Solution. Tallinna Tehnikaülikool. https://digikogu.taltech.ee/et/Item/49f9674f-34c7-4db6-a938-25738dd2d61f

Canadian Survey of Cyber Security and Cybercrime (CSCSC), 2022. https://www23.statcan.gc.ca/imdb/p2SV.pl?Function=getSurvey&SDDS=5244

Cyber Security Breaches Survey 2022. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022#further-information

Cyber Security Report. Special Eurobarometer 390, 2012. https://europa.eu/eurobarometer/surveys/detail/1058

Cyber Security Report. Special Eurobarometer 404, 2013. https://europa.eu/eurobarometer/surveys/detail/1073

Cyber Security Report. Special Eurobarometer 423, 2015. https://europa.eu/eurobarometer/surveys/detail/2019

Dhillon G., 2007. Principles of information systems security. John Wiley & Sons.

Egelman S., & Peer, E., 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, pp. 2873–2882. https://doi.org/10.1145/2702123.2702249

Europeans' attitudes towards Internet. Special Eurobarometer 480, 2007. https://europa.eu/eurobarometer/surveys/detail/2207

Europeans' attitudes towards cyber security - Publication Reports. Special Eurobarometer 464a, 2017. https://europa.eu/eurobarometer/surveys/detail/2171

Europeans' attitudes towards cyber security (cybercrime) - Publication Reports. Special Eurobarometer 499, 2020. https://europa.eu/eurobarometer/surveys/detail/2249

Hadlington L., 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7). https://doi.org/10.1016/j.heliyon.2017.e00346

Hadlington, L., 2018. The Human Factor in Cybersecurity. In J. McAlaney, J. Frumkin, L. A. Benson, V. (Eds.), Psychological and Behavioral Examinations in Cybersecurity (pp. 46–63). https://doi.org/10.4018/978-1-5225-4053-3.ch003

ISO/IEC. ISO/IEC TR 13335-1:2004 Information Technology Security Techniques Management of Information and Communications Technology Security Part 1: Concepts and Models for Information and Communications Technology Security Management. ISO/IEC, JTC 1, SC27, WG 1.

Lungescu, O., 2004. Tiny Estonia Leads Internet Revolution. BBC News, 7 Apr. http://news.bbc.co.uk/2/hi/europe/3603943.stm

Majandus- ja kommunikatsiooniministeerium. Digiühiskonna arengukava 2030. https://www.mkm.ee/media/6791/download

Majandus- ja Kommunikatsiooniministeerium. Küberjulgeoleku strateegia 2008-2013, 2008. https://www.valitsus.ee/sites/default/files/contenteditors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf

Majandus- ja Kommunikatsiooniministeerium. Küberturvalisuse strateegia 2019–2022, 2019. https://www.mkm.ee/media/700/download

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M., 2017. Individual differences and Information Security Awareness. Computers in Human Behavior, 69, pp. 151–156. https://doi.org/10.1016/j.chb.2016.11.065

Mercier, E., 2022. 82% of French People Say They are Worried About the Global Risks of Cyber-Attacks. https://www.ipsos.com/en/82-french-people-say-they-are-worried-about-global-risks-cyber-attacks

Mitnick, K. D. & Simon, W. L., 2002. The Art of Deception. Controlling the Human Element of Security. https://repo.zenk-security.com/Magazine%20E-book/Kevin_Mitnick_-_The_Art_of_Deception.pdf

Mäses, S., 2015. Infoturbe inimfaktori hindamismeetod. Evaluation Method for Human Aspects in Information Security. Tallinna Tehnikaülikool. https://digikogu.taltech.ee/et/Item/1c19ddce-e325-440c-838f-9a349e087ca6

Nunes, P., Antunes, M. & Silva, C., 2021. Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions. Procedia Computer Science, 181, pp. 173–181. https://doi.org/10.1016/j.procs.2021.01.118

Öğütçü, G., Testik, Ö. M. & Oumout, C., 2016. Analysis of Personal Information Security Behavior and Awareness. Computers & Security, 56, pp. 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. & Zwaans, T., 2017. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further Validation Studies. Computers & Security, 66, pp. 40–51. http://dx.doi.org/10.1016/j.cose.2017.01.004

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M & Jerram, C., 2014. Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, pp. 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Puusalu, J. ja Marnot, D., 2021. Elanikkonnaküsitlus „Eesti elanike suhtumine isiklike andmete privaatsusesse ja turvalisusesse". https://digiriiul.sisekaitse.ee/handle/123456789/2846

Ranas, T., Fariz, A., Dirgantara, B., Muhamad, A. & Ruldeviyani, Y., 2020. Measuring Information Security Awareness of Client's Information Security: Case Study at PT XYZ. International Journal of Advances in Electronics and Computer Science, 7(7), pp. 1–6. https://www.iraj.in/journal/journal_file/journal_pdf/12-669-15992140201-6.pdf

Randel, T., 2008. CERT Eesti tegevuse aastakokkuvõte 2007. https://www.ria.ee/sites/default/files/content-editors/CERT/cert_2007_aastakokkuv6te.pdf

Riigi Infosüsteemi Amet. 19 soovitust, kuidas muuta nutitelefoni kasutamine turvalisemaks. https://www.ria.ee/et/kuberturvalisus/nouanded/nutiseadmete-turvalisus.html

Safer internet, 2006. Special Eurobarometer 250 "Safer Internet" Report. https://europa.eu/eurobarometer/surveys/detail/490

Schmidt, A., 2013. The Estonian Cyberattacks. In The fierce domain – conflicts in cyberspace 1986–2012, edited by Jason Healey, Washington, D.C.: Atlantic Council.

Schultz, E., 2005. The human factor in security. Computers & Security, 24, 425–426. https://doi.org/10.1016/j.cose.2005.07.002

Siseturvalisuse avaliku arvamuse uuring, 2016: aruanne, 2016. Siseministeerium. https://digiriiul.sisekaitse.ee/handle/123456789/2627

Siseturvalisuse avaliku arvamuse uuring, 2018: aruanne, 2018. Siseministeerium. https://digiriiul.sisekaitse.ee/handle/123456789/2623

Siseturvalisuse avaliku arvamuse uuring, 2020 : aruanne, 2020. Siseministeerium. https://digiriiul.sisekaitse.ee123456789/2604

Siseturvalisuse avaliku arvamuse uuring, 2022: aruanne, 2022. Siseministeerium. https://digiriiul.sisekaitse.ee/handle/123456789/2604

Siseministeerium. Siseturvalisuse arengukava 2020–2030. https://www.siseministeerium.ee/media/748/download

Solms von, R. & Niekerk van, J., 2013. From information security to cyber security. Computers & Security, 38, pp. 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Sõmer, T., 2022. Modelling Financially Motivated Cybercrime. Doktoritöö. Tallinn: Tallinna Tehnikaülikool Press. https://doi.org/10.23658/taltech.10/2022

Tõiste, T., 2021. Eesti Raamatukoguhoidjate Ühingu tegevus 2020. aastal. https://eru.lib.ee/images/stories/dokumendid/ERY_2020_aruanne.pdf

UK Cyber Survey Key findings – General public. 2019. file:///C:/Users/Kate-Riin/OneDrive%20%20House%20Haldus%20O%C3%9C/Latitude5410/Downloads/UK%20Cyber%20Survey%20-%20analysis.pdf

Vaks, T., 2013. Riigi Infosüsteemi Ameti kokkuvõte küberturvalisuse tagamisest 2012. RIA-kuberturvalisuse-teenistuse-kokkuvote-2012.pdf

Whitman, M., & Mattord, H., 2010. Management of Information Security. Cengage/Course Technology.

Woodward, C., 2003. Estonia, where being wired is a human right. Christian Science Monitor July 1. http://www.csmonitor.com/2003/0701/p07s01-woeu.html

Yeng, P. K., Fauszi, M. A. & Yang. B., 2021. Assessing the effect of human factors in healthcare cyber security practice: An empirical study. 25th Pan-Hellenic Conference on Informatics. November 2021 (pp. 472–476). https://doi.org/10.1145/3503823.3503909

SIINNE MÕTTEPABER KAARDISTAB TEEMAD, MIS ON ESILE KERKINUD SEOSES ÜHA SUURENEVATE KÜBEROHTUDEGA ETTEVÕTETE JA ÜKSIKISIKU TASANDIL.

Siseturvalisuse avaliku arvamuse 2022. aasta uuring näitas, et kogu riiki puudutavatest ohuolukordadest peavad Eesti elanikud lähima kolme aasta jooksul kõige tõenäolisemaks küberrünnakut. Kui vaadata Eurobaromeetri uuringute trende aastatel 2012–2019, tekitab muret, et Eesti internetikasutajad ei vaheta piisava regulaarsusega oma võrguparoole ning vaid umbes 1/3 kasutab erinevaid paroole eri kontode jaoks. Kõige sagedasemad küberturvanõuete rikkumised on seotud inimlike vigadega, mida on võimalik vältida küberteadlikkust eri sihtgruppides regulaarselt hinnates-mõõtes ja selle põhjal erineva tasemega koolitusi korraldades. Eesti riik on korraldanud mitmeid küberteadlikkuse suurendamise kampaaniaid ning välja töötanud strateegiaid, kus vähemal või rohkemal määral on paika pandud eesmärgid kasvatada nii elanike kui ka organisatsioonide teadlikkust küberkuritegevusega seotud ohtudest ja nendest hoidumise võimalustest. Kokkuvõttes rõhutatakse olulisust keskenduda elanikkonna eri gruppide ning organisatsioonide töötajate infoturbe- ja küberturvalisusealaste teadmiste, hoiakute, oskuste ja tegeliku käitumise uurimisele ning vajadusele küberturvalisuse lõimimiseks gümnaasiumide õppekavasse, et tagada küberteadlike kodanike järelkasv.

sisekaitse.ee