TARTU ÜLIKOOL

Arvutiteaduse instituut

Informaatika õppekava

Tauno Tamm

Küberhügieeni kursuse „Tagasi kontorisse” loomine DeLRAP platvormile

Bakalaureusetöö (9 EAP)

Juhendajad: Alo Peets, MSc

Lauri Almann, MA

Tartu 2022

Küberhügieeni kursuse „Tagasi kontorisse” loomine DeLRAP platvormile

Lühikokkuvõte:

Küberuum meie ümber on pidevalt arenev. Digitehnoloogiate laialdasem kasutuselevõtt suurendab vajadust paremate küberteadmiste järele. Interaktiivses digiühiskonnas on tõusnud ka kodanike ootused õppematerjalidele ning on vajadus inimeste küberteadlikkust pidevalt tõsta läbi praktiliste näidete. Käesoleva bakalaureusetöö raames loodi ettevõtte Cybexer Academy OÜ platvormile DeLRAP küberhügieeni moodul „Tagasi kontorisse“, mis koosneb 14st eeltesti küsimusest, 25st kaasusest koos selgitavate õppematerjalidega ning 12st lõpptesti küsimusest. Moodul keskendub kasutajate küberteadlikkuse tõstmisele ning nende riskide välja selgitamisele nii tavakontori kui ka kodukontori perspektiivist. Uue mooduli sisu loodi analüüsides hiljutisi küberintsidente, tuginedes Eesti infoturbestandardi 2021. aasta versioonile ning klientide vajaduste kaardistamiseks läbiviidud küsitluse analüüsile. Töö kirjalikus osas antakse ülevaade, milliseid referentsmaterjale analüüsiti ning tutvustatakse uute testküsimuste ja õppematerjalide loomise põhimõtteid.

Võtmesõnad: Küberhügieen, turvalisus, õppematerjal, E-ITS, EITS

CERCS: P175 Informaatika, süsteemiteooria

Creation of the “Back to the Office” Cyber Hygiene Course for the DeLRAP Platform

Abstract:

Cyberspace around us is in continuous evolution. The widespread use of digital technologies has created a growing necessity for improved cyber awareness. Furthermore, the expectations of residents in this interactive digital society are increasing in regards to graspable learning materials, putting emphasis on education through practical examples and cases. The goal of the thesis at hand was to create a cyber hygiene module for CybExer Academy's DeLRAP platform, themed "Back To The Office", which consists of 14 quiz questions, 25 practical cases with explanatory study material and 12 exam questions. The module focuses on raising the trainee's cyber awareness as well as assessing their risks in the context of both regular office and home office environments. The content of the new module was created by analysing recent cyber incidents, using the Estonian Information Security Standard version 2021 as a guideline and mapping out client needs through an thorough survey. The written part of the thesis covers analyzed reference sources and the methodologies used to create new quiz questions and study material cases.

Keywords: Cyber hygiene, security, study material, E-ITS, EITS

CERCS: P175 Informatics, systems theory

Sisukord

Sissejuhatus

Küberruum on väga dünaamiline ja pidevalt arenev keskkond. Küberründajad kasutavad ära nii süsteemide nõrkuseid kui ka inimeste teadmatust, et oma rünnakuid planeerida ja teostada. Eelnevast tulenevalt peavad küberruumi kasutajad olema pidevalt informeeritud olulistest trendidest, päevakohastest probleemidest ja parimatest küberhügieeni tavadest. Täiendavalt toovad Subrata Acharya jt.[1] oma teadusartiklis välja, et inimeste küberturvalisuse teadmised on nõrgad, sest internetis leiduvatest küberturbe juhistest enamus ei ole kirjutatud tavakasutaja jaoks arusaadavas keeles.

Töö lähtepunktiks on CybExer Academy OÜ poolt 2021 aastal loodud Kodust töötamise küberhügieeni õppemoodul (inglise keeles *Work From Home*), mis keskendus inimeste küberteadlikkuse tõstmisele lähtudes kodukontori perspektiivist. Tegemist on *online* keskkonas sooritatava õppemooduliga, mis koosneb kolmest osas: eelküsimustik, olukordi kirjeldavate kaasustega õppematerjali osa ning järeltest. Keskmiselt kulub õppijal 90 minutit kõigi kolme osa läbimiseks. Praeguseks hetkeks on pea aasta tagused trendid ja tavad küberruumis muutunud, mistõttu ei ole tegemist enam nii teemakohase ja klientide vajadusi rahuldava mooduliga. Järjest enam inimesi naaseb tagasi kontoritööle, millega seoses on tarvis meelde tuletada küberhügieeni käitumisnorme kontorikeskkonnas.

Lõputöö eesmärgiks on luua uus küberhügieeni mooduli sisu, mille läbiv mõte on „Tagasi kontorisse“ (inglise keeles *Back to the office*). Hübriidmooduli sisu luuakse nii kodust töötamise kui ka kontori perspektiivist, võttes aluseks kliendiküsitluse analüüsi, hetke küberohtude hinnangud ning Eesti infoturbestandardi 2021. aasta versiooni. Sisu luuakse selliselt, et kaasustes kirjeldatavad sündmused ja tegelased kõnetaksid võimalikult palju mooduli läbijaid. Loodud materjal peab olema võimalikult lihtsasti hoomatav ka isikule, kellel puuduvad eelteadmised küberturbe valdkonnas.

Käesolev bakalaureusetöö koosneb kolmest peamisest sisupeatükist. Esimeses osas selgitatakse, millised on hetke küberturvalisuse ohu trendid ning mida küberturbe standardid nõuavad. Teises osas kirjeldatakse DeLRAP platvormi olemust ja metoodikat ning analüüsitakse CybExer Academy OÜ klientide seas läbi viidud küsitluse tulemusi. Kolmandas osas antakse ülevaade loodud õppematerjalist teemade kaupa. Töö lõppeb kokkuvõtte, kasutatud kirjanduse ja lisadega.

1. Küberturve ja -hügieen

Käesolevas peatükis selgitatakse küberhügieeni olulisust ning tuuakse välja bakalaureusetöö kirjutamise ajal aktuaalsed küberohud. Lisaks kirjeldatakse küberhügieeni regulatiivset keskkonda - miks on oluline tõsta inimeste küberteadlikkust ning kuidas regulatsioonid ja standardid seda nõuavad.

1.1. Küberhügieen

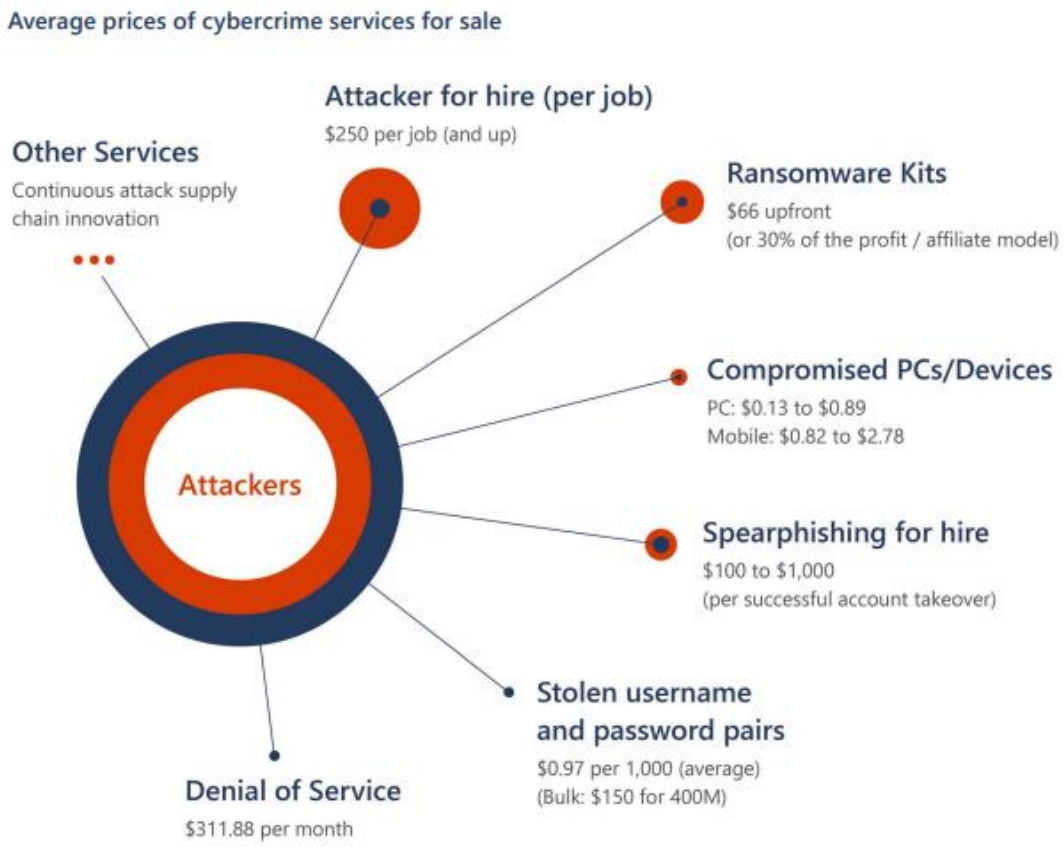
Küberhügieen on kasutaja igapäevane käitumine ning teadmiste kogum küberturvalisuse vallas. Küberhügieen ehk küberturvalisuse elementaarteadmised ja nende rakendamine on olulised inimesel enda andmete, seadmete ja töökoha kaitseks. Iga päev ühendatakse internetivõrku palju uusi seadmeid, luuakse lugematul arvul uusi kasutajakontosid erinevatesse keskkondadesse, sooritatakse palju interneti oste jne. Internet on justkui paralleelmaailm, kus on esindatud kõik füüsiline maailm, millest on osa saamas üha suurem hulk maailma rahvastikust. Sarnaselt igapäevaeluga eksisteerib internetis palju ohte. Rünnakuid viiakse läbi erinevatel viisidel ning rünnakutel on erinevad eesmärgid. Peamiselt tahetakse küberrünnakutega koguda tundlikke andmeid või varastada kasutaja paroole, et hilisemas etapis läbi viia küberkuritegevusi või rikastuda.

Iga internetikasutaja peab olema küberteadlik, et vähendada riski sattuda küberrünnaku ohvriks. Isikul tuleb pidevalt olla kursis levivate ohtudega ning parandada pidevalt enda küberhügieeni teadmisi läbi eluliste näidete. Riigi Infosüsteemi Amet (RIA) on oma nõuannete lehel [2] välja toonud mitmeid ohuallikaid ning meetmeid, mida mõistes ja järgides saab kasutaja tõsta enda küberteadlikkust ning vähendada riske sattuda rünnaku ohvriks. RIA ajaveeb räägib nutiseadmete turvalisusest, õngitsuslehtedest ja -kirjadest, paroolide loomisest, pahavarast jne.

1.2. Hetkel aktuaalsed küberohud

Microsoft toob oma digitaalse kaitse raportis [3] välja, et küberrünnakute odav hind ning tarkvaralised valmislahendused võimaldavad ründeid tellida ning läbi viia ka vähem kogenud

ründajatel. Joonisel 1 tuuakse välja erinevate küberrünnakute teenuste keskmised hinnad, mis annab ülevaate, et ka tavainimesele on taskukohane tellida küberründeid.



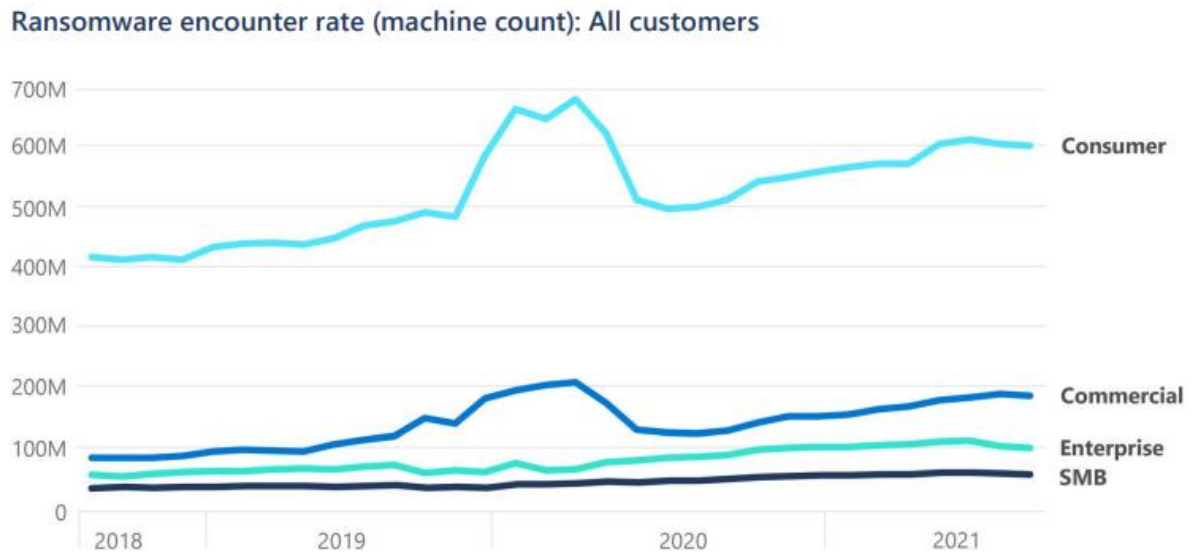
Joonis 1. Küberrünnaku teenuse müümise keskmine hind aastal 2021 [3].

Microsofti sõnul [3] on viimase 12 kuu jooksul küberrünnete teenuseid pakkuvate veebisaitide arv märgatavalt kasvanud, mis viitab sellele, et üha enam kasutatakse rünnakute läbiviimiseks valmis tarkvaralahendusi või tellitakse rünnakud. Järgnevas peatükis tuuakse välja hetkel aktuaalsed ning kiires trendis kasvavad küberrünnakute liigid, mis RIA aastaraamatu [4] hinnangul toob endaga kaasa 2022. aasta küberruumis.

1.2.1. Lunavararünnak

Lunavararünnakuks (inglise keeles *ransomware attack*) nimetatakse küberrünnakut, mis viiakse läbi kasutades pahavara, mis krüpteerib ohvri andmed ja failid nii, et ohver ei pääse nendele enam ligi. Seejärel saadetakse ohvrile lunarahanõue krüptovaluutas, mille täitmisel failid dekrüpteeritakse. Ettevõtte F-secure blogi [5] andmetel nõuavad lunavararünnakute

läbiviijad tavakasutajalt 300-500$ väärtuses krüptovaluutat dekrüpteerimisvõtme saatmiseks. Microsoft toob oma küberturvalisuse raportis [3] välja, et enne failide krüpteerimist sorteeritakse eelnevalt välja tundlikud andmed ja failid. Microsofti sõnul ei saa sellisel juhul ohvrid lunarahanõuet maksmata jätta, isegi kui neil on andmed varundatud, sest ründajad lubavad tundliku info avaldada. Lunavararünnakute juhtumid on tõusnud alates 2018. aastast kuni 2020. aasta II kvartalini, mil rünnakute arv langes. Juhtumite arv hakkas taas tõusma 2020. aasta III kvartalis. Kokkuvõttes on 2021. aasta lunavararünnakute juhtumite arv tõusnud võrreldes 2018. aasta juhtumite arvuga (Joonis 2). Microsofti sõnul on peamisteks põhjusteks küberrünnakute teenuste odavus ning välja arendatud lunavararünnakute pahavarakomplektid ehk RaaS (*ransomware-as-a-service*), mis võimaldavad keerulisi rünnakuid läbi viia ka vähem kogenud ründajatel. Sellisel juhul jaguneb lunavararünnakutest saadud kasum läbiviija kui ka pahavara arendaja vahel.



Joonis 2. Kasutajate kokkupuude lunavaraga 4 aasta lõikes [3].

RIA aastaraamatus [4] selgitatakse, et Eesti ei ole väga suure mõjuga lunavararünnakute alla sattunud. RIA sõnul on see vaid aja küsimus, sest kogu riigi toimimine sõltub digitaalsetest teenustest. RIA toob välja, et lunavararünnakute vastu aitab pidev küberhügieeni teadlikkuse tõstmine. Seda kinnitab ka Microsoft oma raportis [3] ning lisab, et lunavararünnaku vältimiseks tuleks kasutusele võtta viirusetõrje ning pidevalt värskendada oma operatsioonisüsteemi. Microsofti sõnul tuleks oma andmed ka eelnevalt krüpteerida. Nii saab

kasutaja vältida olukorda, kus lunavararünnaku ohvriks langemisel ähvardab ründaja tema tundlikud andmed paljastada.

1.2.2. Õngitsemine

Õngitsemine (inglise keeles *phishing*) on küberrünnaku tüüp, mille puhul ründaja kehastab usaldatavat allikat, eesmärgiga koguda ohvri tundlikku informatsiooni, näiteks kasutajaandmeid ja paroole, või paigaldades ohvri arvutisse pahavara. Õngitsust esineb mitut liiki - õngitsuskiri, õngitsuskõne, õngitsusveebileht jne. Kõikide liikide puhul on läbiv mõte ja eesmärk sama, kuid rünnaku läbi viimiseks kasutatakse erinevaid vahendeid.

RIA koostatud aastaraamatus [4] on välja toodud, et õngitsuslehed jagunevad peamiselt kaheks: kontoandmete õngitsused ja pangakonto õngitsused, kus õngitsuslehed on originaallehtedele väga sarnased, kuid veebilehe aadressi vaadeldes on aru saada, et tegemist on õngitsuslehega. RIA aastaraamatu [4] andmetel nõudsid CERT-EE spetsialistid 2020. aastal 711 õngitsuslehe mahavõtmist ning 2021. aastal 755 õngitsuslehe mahavõtmist. Microsofti raporti [3] andmetel võtsid nad 2021. aastal maha 168 000 õngitsusveebilehte. Samuti on olunud pidevas tõusutrendis õngitsuskirjade levik (Joonis 3). Ettevõtte Barracuda toob oma artiklis [6] välja, et 2021. aasta jooksul saatsid küberründajad välja 3 miljonit võlts e-kirja, mis saadeti kokku 13 000 kompromiteeritud e-posti kontolt. Ettevõte barracuda väidab, et õngitsuslehtede ja e-kirjade loomisel ründajate poolt enim kehastatud kaubamärk oli Microsoft.

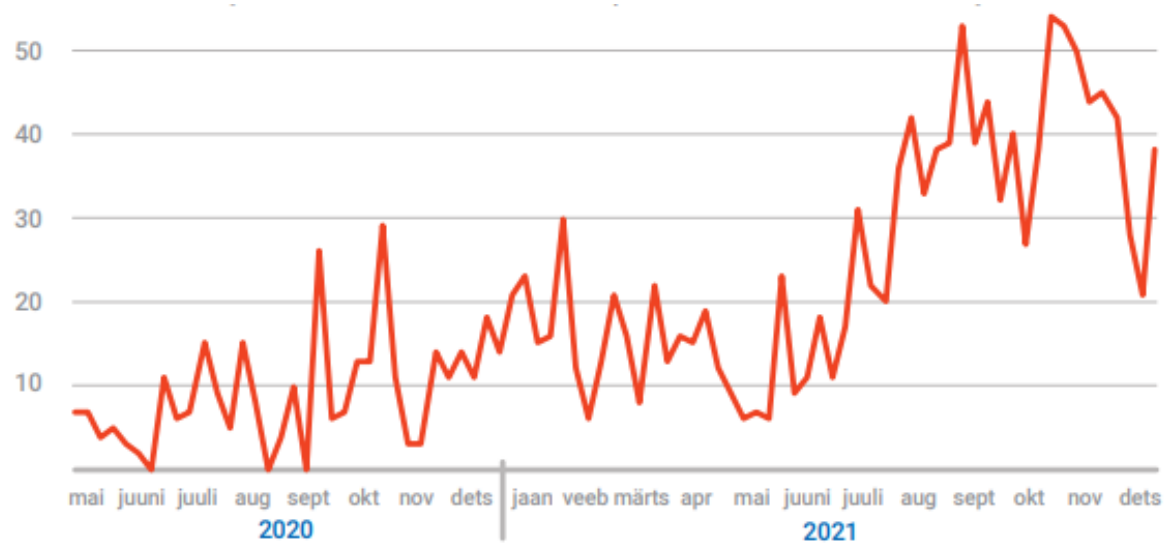
Joonis 3. Avastatud õngitsuskirjad ajavahemikul juuni 2020 kuni juuni 2021 [3].

Microsofti raportis [3] kui ka RIA aastaraamatus [4] soovitatakse oma kontodel kasutada mitmeastmelist autentimist. Nii ei saa ründajad kasutaja kontodele ligi, kui kasutaja andmed on lekkinud, sest kasutajal on tarvis enda isik tuvastada ka teise seadme või autentimisrakenduse abil, millele ründajal ligipääs puudub. Microsoft lisab, et õngitsuskirjade tuvastamiseks tuleks kasutajaid koolitada ning neile selgitada, kuidas ära tunda õngitsuskirju. Õngitsuskirjade ära tundmiseks soovitab Microsoft kuvada kasutajatele päriselulisi näiteid, kus kasutaja peab raporteerima, kas tegemist on õngitsuskirjaga või mitte ning talle antakse koheselt tagasisidet koos selgitustega.

1.2.3. Teenusetõkestusrünnakud

Teenusetõkestusrünnak ehk DDoS rünnak (inglise keeles *Distributed Denial-of-Service*) on küberrünnaku tüüp, mille puhul tehakse ohvri veebilehele palju päringuid, mis halvab veebilehe. Ründaja loob robotvõrgu (inglise keeles *botnet*), olles eelnevalt nakatunud pahavaraga kasutajate arvuteid. Päringuid veebilehtedele tehakse pahavaraga nakatunud arvutitega, kus kasutajad sageli ei tea, et nende arvutit kasutatakse teenusetõkestusrünnete tegemiseks.

RIA aastaraamatus [4] tuuakse välja, et võrreldes 2020. aasta rünnakute arvu 2021. aasta rünnakute arvuga, on suure mõjuga teenusetõkestusrünnakute arv tõusnud 32-lt 47-le. RIA aastaraamatus [4] kuvatud joonisel (Joonis 4) on näha, et teenusetõkestusrünnakute automaatteavituste arv kõigub suure amplituudiga, kuid üldine trend on kasvav.



Joonis 4. Teenusetõkestusrünnakute automaatteavituste arv 2020. aasta maist kuni 2021. aasta detsembrini [4].

RIA sõnul aitab kasutaja arvuti tarkvara ja operatsioonisüsteemi pidev uuendamine ning viirusetõrje programmide kasutamine vältida inimese arvuti nakatumist pahavaraga ning liitmist ründaja robotvõrku. Meetmete kasutusele võtmine aitab vältida olukorda, kus kasutaja arvutit kasutatakse pahatahtlikult ära teiste vastu suunatud küberrünnete läbiviimiseks.

1.3. Regulatiivne keskkond

2022. aastal jõustub uus Eesti Infoturbestandardi (E-ITS) määrus [7]. E-ITS kirjeldab, kuidas ettevõtte infoturbe halduse süsteemi käivitada, rakendada, käigus hoida ja täiustada. Eesti infoturbestandard[1] on kooskõlas standardiga ISO 27001 ning baseerub Saksa päritolu BSI IT-Grundschutz etalonturbe meetodil [9]. Ettevõtte Advisera Expert Solutions Ltd sõnul [10] on ISO 27001 rahvusvaheline standard, mis aitab süsteemselt ja kuluefektiivselt kaitsta igas suuruses organisatsioonide ja ettevõtete informatsiooni.

Standardis ISO 27001 klauslis 7.2 on välja toodud, et organisatsiooni töötajaid tuleb regulaarselt koolitada küberteadlikkuse tõstmise eesmärgil [11]. Standardis loetletakse erinevaid võimalikke viise küberturbe koolituste läbiviimiseks ning üheks sobivaks koolituse formaadiks on pakutud veebipõhine koolitus.

Eesti infoturbestandardi [12] punktis ORP.3.M4 tuuakse välja, et koolitused peavad olema ajakohased ning nende ajakohasust kontrollitakse regulaarselt. Vajaduselt materjale

[1] https://eits.ria.ee/

kohandatakse või tehakse täiendusi. Standardi [12] punktis ORP.3.M7 mainitakse, et infoturbe koolitused peavad sisaldama elulisi näited ja praktilisi harjutusi.

Praktikas on aga väike kuni keskmise suurusega ettevõtetel ja asutustel rahvusvahelise ISO 27001 standardi rakendamine liialt aja- ning ressursimahukas. Täiendavalt on E-ITS ka eestikeelne ning Eesti õigusruumile vastav, mis teeb selle rakendamise mugavamaks.

Kokkuvõtteks eksisteerivad lisaks reaalsetele hetke ohtudele ja intsidentidele ka turvastandardid, mis nõuavad organisatsiooni töötajate regulaarset koolitamist. Standarditest tuleb välja, et koolituste materjalid peavad olema ajakohased ning sisaldama praktilisi harjutusi ja elulisi näiteid.

2. Mooduli loomise protsess

Mooduli loomise protsessi peatükis antakse ülevaade DeLRAP platvormi mooduli loomise protsessist. Mooduli loomist alustati materjali kogumisest ning trendide ja klientide tagasiside analüüsist.

2.1. DeLRAP'i olemus ja metoodika

DeLRAP ehk dünaamiline e-õppe ja riskihindamise platvorm (inglise keeles *dynamic e-learning risk assessment platform*) on ettevõtte CybExer Technologies OÜ loodud platvorm, mis keskendub e-õppele ja riskikäitumise hindamisele. Ettevõtte esindaja sõnul põhineb platvormi kontseptsioon arusaamal, et inimeste riskikäitumise juhtimine on pidev protsess, mille jooksul nii koolitatavad kui ka juhendajad õpivad ja arenevad. DeLRAP platvorm ja sellega kaasnevad kursused on interaktiivsed, elulised ning praktilised. Kursused on suunatud kolmele erinevale töötajate grupile - tavakasutajad, juhid ja spetsialistid. DeLRAP platvormi moodul on võimalik luua selliselt, et iga töötajate grupp (tavakasutaja, juht ja spetsialist) saab vastavalt enda profiilile loodud sisu.

CybExer Academy OÜ tuleb iga aasta välja värske küberhügieeni mooduliga, mis hõlmab endas hetke kõige olulisemaid trende ja tavasid. Moodul on suunatud töötajatele nii era- kui ka avaliku sektori ettevõtetes. Mooduli käigus veendakse kasutajat, et moodulis välja toodud ohud on reaalsed. Seejärel selgitatakse, milliseid tagajärgi käsitletav küberoht võib endaga kaasa tuua ja õpetatakse mooduli läbijat, mida teha välja toodud situatsioonide korral või kuidas neid vältida.

Moodulis olevad küsimused on valikvastustega ning kursuse käigus ei anta mooduli läbijale hinnet, vaid määratakse ära valdkonnad, mille puhul on isiku käitumine riskantne. Mooduli läbijale kuvatakse peale lõpptesti osa tema vastuste põhjal kujunenud riskimaatriks, mis näitab kasutaja riske erinevate riskivektorite põhiselt. Samuti on võimalik platvormi analüütikul vaadata terve organisatsiooni, meeskondade kui ka üksikisiku üldist riskipilti. Tulemuste põhjal saab välja filtreerida riskantsed kasutajad, määrata ohutaseme ning rakendada vajalikud täiendavad tegevused küberhügieeni parandamise osas. Oma olemuselt on tegemist infoturbejuhtidele vajaliku tarkvaraga, millega saab kaardistada organistatsiooni töötajate küberriskid mooduli teemade lõikes. DeLRAP platvorm ja muud töö tehnoloogilised piirangud olid ette antud ettevõtte CybExer Academy OÜ poolt, kus autor kirjutamise ajal töötas.

2.2. Mooduli ülesehitus

DeLRAP platvorm ei ole mõeldud ainult küberturvalisuse teemasid puudutavate moodulite läbimiseks, vaid platvormi on võimalik luua vabalt valitud temaatikal põhinevat moodulit - määrata riskimaatriksi peamised kategooriad ning osade riskivektorid ning kirjutada soovitud temaatikale vastav sisu. Terviklik platvormi moodul koosneb kolmest elemendist - eelküsimustik, õppematerjal ja järeltest.

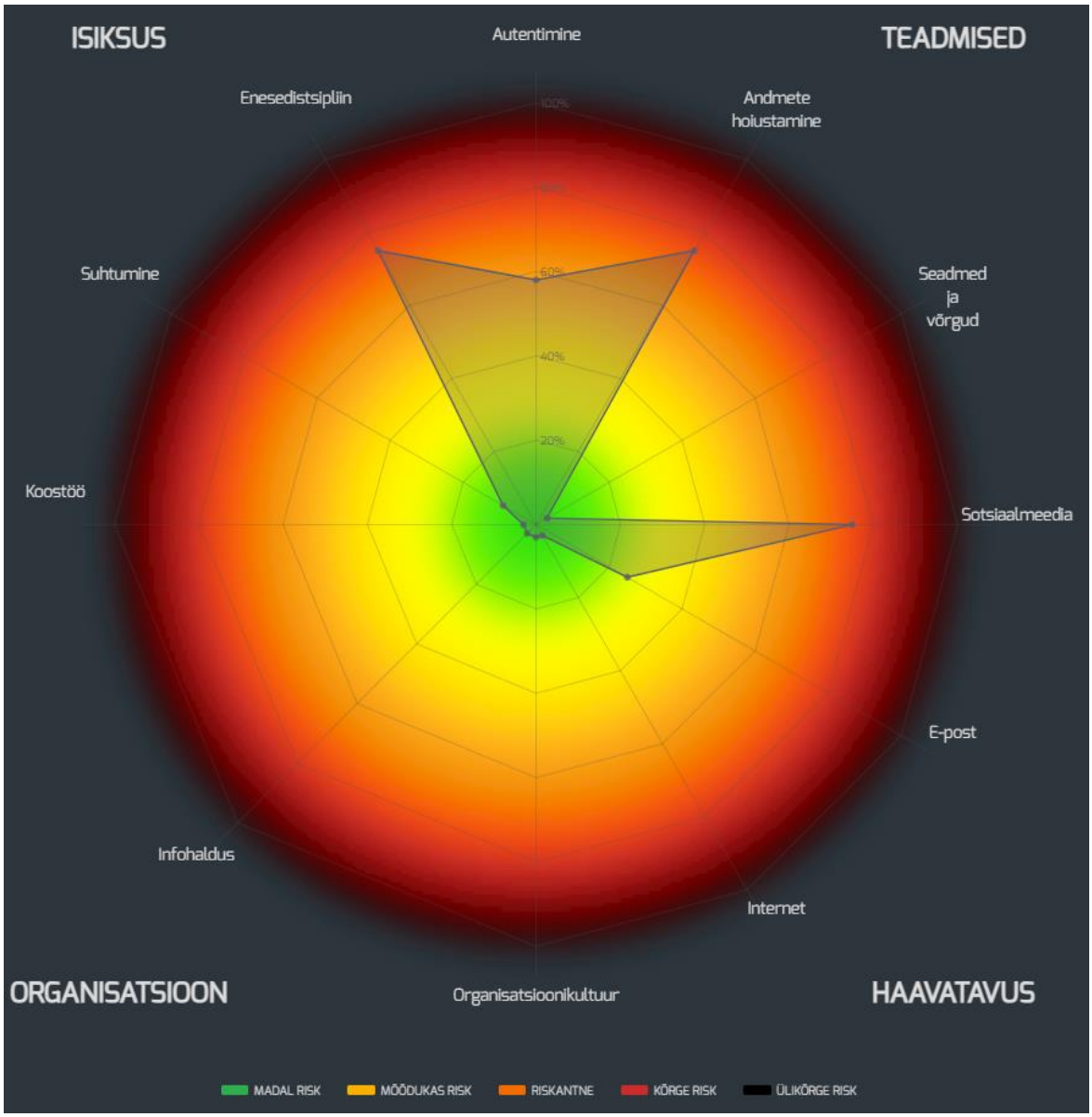
Eelküsimustiku osas küsitakse mooduli läbijalt teemat puudutavaid küsimusi ning kaardistatakse tema algsed teadmised. Seejärel hakkab kasutaja läbima õppematerjali osa. Õppematerjali osas on välja toodud piltidega illustreeritud kaasused mingi konkreetse juhtumi kohta ning kasutajalt soovitakse teada, kuidas tema sellises situatsioonis käituks. Kasutajale antakse ette valikvastused, mille hulgast peab ta valima endale meelepärase vastuse. Siinpuhul on oluline, et kasutaja ei valiks õiget vastust, vaid selle vastuse, kuidas tema sellises situatsioonis käituks. Seda selgitatakse kasutajale mooduli alguses koheselt. Nii annab riskimaatriks kasutajale ja analüütikutele väga täpse ülevaate kasutajate riskikäitumisest. Kui kasutaja valib „õige“ vastuse, mitte enda igapäevast käitumist küberruumis kirjeldava vastusevariandi, ei ole genereeritud riskimaatriks täpne.

Kui kasutaja on valinud enda küberkäitumist kõige paremini peegeldava vastuse ning on selle ära esitanud, kuvab platvorm kõikide vastuste riskitaseme. Riskitasemed on välja toodud värvidena, kus roheline tähistab madalat riski, kollane mõõdukat riski, oranž riskantset käitumist, punane suurt riski ning must ülisuurt riski. Samuti ilmub kasutajale nähtavale selgitav tekst, mis selgitab mooduli läbijale, millest antud kaasus räägib, miks mingi vastus on riskantne, mida peaks antud olukorras tähele panema ja meelde jätma ning kuidas oleks õige antud situatsioonis käituda. Järeltesti osas hinnatakse kasutaja teadmisi õppematerjalis õpetatu põhjal. Iga vastatud vastus mõjutab riskiprofiilil kaasusega seotud vektoreid - nii kujuneb moodulit läbides vastaja riskiprofiil. Tegemist on mooduli loomise metoodikaga, mida rakendatakse kõigi DeLRAP moodulite loomisel samasuguselt.

Keskmiselt koosneb küsimustik kümnest küsimusest, õppematerjal kahekümnest kaasusest ja küsimusest ning testi osa viieteistkümnest küsimusest. Kokku võtab mooduli läbimine aega umbes 90 minutit sõltuvalt kasutaja varasematest teadmistest, kokkupuudetest mooduli valdkonnaga ning tema soovist keskenduda mooduli sisu läbi lugemisele ning selle mõistmisele.

2.3. Riskihindamise maatriks

DeLRAP platvorm[2] hõlmab endas süsteemset üksikasjalikku riskimaatriksit (Joonis 5). Riskimaatriks genereeritakse mooduli läbijale pärast kursuse lõpetamist, võttes arvesse kasutaja riskid läbitud mooduli suhtes. Riskimaatriksi kujunemisel võetakse arvesse kasutaja vastuseid eelküsimustiku, õppematerjali ja järeltesti osas. Peale mooduli läbimist on võimalik vaadelda kasutaja üldriskimaatriksit, kui ka iga mooduli osa riskimaatriksit eraldi. Riskimaatriks koosneb neljast peamisest kategooriast: teadmised, haavatavus, organisatsioon ja isiksus. Kategooriad jagunevad omakorda vektoriteks.



Joonis 5. DeLRAP platvormi „Tagasi kontorisse“ mooduli riskihindamise maatriks.

[2] https://login.mycyberhygiene.com/#login

Riskimaatriksi keskele saab tõmmata mõttelise horisontaaljoone, mis jagab riskimaatriksi kaheks osaks. Horisontaaljoonest ülespoole jäävad vektorid näitavad mooduli läbija enda panust küberhügieeni. Need on valdkonnad, milles saab mooduli läbija ennast parandada. Ta saab muuta enda suhtumist küberhügieeni vastu, olla rohkem distsiplineeritud järgima reegleid ja raamistikku enda ja asutuse turvalisuse huvides ning olla rohkem koostööaltim. Samuti saab mooduli läbija suurendada enda teadmisi autentimise, andmete hoiustamise ning interneti ja seadmete vallas.

Horistonaaljoonest allapoole jäävad vektorid on teemad, mis ei sõltu otseselt mooduli läbijast endast. Nendeks teemadeks on organisatsioonikultuur, infohaldus ja erandite lubatavus, mis annavad ülevaate organisatsioonis toimuvast - kas, kuidas ning millised reeglid ja tavad on rakendatud, et tagada töötajate jaoks parem küberturvalisus. Samuti kategooriad sotsiaalmeedia, e-post ja internet on ohuvektorid, mille kaudu on võimalik viia läbi ründeid. Ründe läbiviimine jällegi ei sõltu otseselt mooduli läbijast endast, pigem keskendutakse sellele, kuidas antud situatsioonide korral riskivabalt käituda või mida teha, et mitte anda võimalust selliste situatsioonide ja rünnakute tekkeks.

Riskimaatriksi keskele saab tõmmata ka mõttelise vertikaaljoone, mis jagab riskimaatriksi kaheks osaks. Vertikaaljoonest vasakule jääb mittetehniline osa, mis keskendub isikuomaduste kui ka tema kuuluvuse hindamisele. Vertikaaljoonest paremale jääb tehniline osa, mis katab kasutaja teadmisi küberrünnakute ennetamise kui ka äratundmise osas.

2.3.1. Teadmised

Kategooria „Teadmised" hindab objektiivselt kasutaja teadmisi kolmes valdkonnas – „Autentimine", „Andmete hoiustamine", „Seadmed ja võrgud". Teadmiste vektori raames käsitletavas materjalis on tegemist juhtumite ja selgitustega, kus küberrünnaku või võimaliku riski tekkimise ärahoidmine sõltub mooduli läbija teadmistest. Mooduli loomisel käsitletakse hetke trendidest tulenevate teadmiste kontrolli ja arendamist. CybExer Academy OÜ poolt 2021. aastal ilmunud Kodust töötamise moodulis oli kategooria „Teadmised" jagatud kolmeks vektoriks: Autentimine, WiFi seadmed ja Kaasaskantavad seadmed. Autori arvates ei katnud 2021. aasta Kodust töötamise mooduli vektorid ära kõiki teemasid, näiteks puudus andmete varundamisele keskenduv teemavektor, mistõttu loodi vektor „Andmete hoiustamine".

Vektorid „WiFi seadmed“ ja „Kaasaskantavad seadmed“ oli liiga kitsahaardelised, mistõttu otsustas autor need ühendada üheks „Seadmed ja võrgud“ vektoriks.

Autentimise vektor puudutab turvalist autentimist ning sellega seonduvate riskide kaardistamist ja õpetamist. Autentimise peamisteks teemadeks on tugevad paroolid ja nende loomine, paroolide haldus ning mitmefaktoriline autentimine. Näiteks on kasutajale lõpptesti osas valikvastused erinevate paroolidega, mille hulgast tuleb tal valida tema arvates hea parool.

Andmete hoiustamise vektor kaardistab mooduli läbija võimalikke teemaga seonduvaid riske ning selgitab ja õpetab, kuidas turvalisi andmeid hoiustada. Andmete hoiustamise teema puhul räägitakse andmete varundamise olulisusest, andmete varundamise võimalustest ning kuidas varundatud andmeid turvaliselt kaitsta. Näiteks küsitakse kasutajalt eelküsimustiku osas, kas ja kui tihti teeb ta oma olulistest andmetest varukoopiaid, et kaardistada kasutaja harjumused enne õppematerjali osa läbimist.

Vektor „Seadmed ja võrgud“ käsitleb riistvara suunitlusega teemat, kus kaardistatakse mooduli läbija riskid ning teadmised seadmeid ja võrke puudutavatel teemadel. Antud mooduli raames käsitletakse olukorda, kuidas veenduda oma internetiruuteri turvalisuses ning kuidas kaitsta värkvõrgu seadmeid ning nutitelefoni. Näiteks kuvatakse kasutajale kaasus, mille õppematerjali osas tuuakse välja võtted, mida rakendades on kasutaja ruuter turvalisem.

2.3.2. Haavatavus

Kategooria „Haavatavus” kaardistab kasutaja riske sattuda oma küberkäitumisega võimalike küberrünnakute alla. Tegemist on üldteemaga, milles käsitlevaid teemad ei olene otseselt kasutajast, vaid keskenduvad võimalikele küberrünnakutele ning selle, kuidas tekkinud olukorras käituda ja riske maandada. Kategooria „Haavatavus” hindab kasutaja haavatavust kolme peamise ründevektori kaudu, milleks on „Sotsiaalmeedia”, „E-post” ja „Internet”.

Sotsiaalmeedia vektor käsitleb sotsiaalmeediaga seonduvaid ohte. Sotsiaalmeedia kasutajate arv kasvab iga-aastaselt. Kasvuga kaasneb ka küberrünnakute arv sotsiaalmeedias - ründajad lekitavad pahaloomulise sisuga linke, koguvad andmeid ebamääraste rakenduste kui ka hapuunimise (inglise keeles *harpooning*) ehk sihitud ründe näol. Loodud moodulis veendakse, selgitatakse ja õpetatakse mooduli läbijat, kuidas sotsiaalmeedias võimalikke riske maandada. Näiteks kuvatakse kasutajale kaasus, kus kaasuse peategelane on saanud sotsiaalmeedia platvormil sõnumi oma sõbralt, mis sisaldab kahtlast linki. Kasutajalt soovitakse teada, kuidas ta selles olukorras käituks.

E-post on äärmiselt levinud viis, mida küberkurjategijad kasutavad, et saata halbade kavatsustega manuseid (pahavara, võltsarved jms) ja petulinke ohvrile või mõjutada ohvrit psühholoogiliselt, et välja petta tundlikke andmeid, paroole või raha. Alamvektor „E-post" kaardistab, selgitab ja õpetab e-postiga seonduvaid ohte. Hetkel on suurimaks e-posti ründeviisiks õngitsusrünne (inglise keeles *phishing*), millele selle mooduli raames keskendutaksegi. Moodulil läbijale kuvatakse näited õngitsuskirjadest ning kasutaja peab välja tooma, milline element reedab, et tegemist on õngitsuskirjaga. Õppematerjali osas kuvatakse õngitsuskirjade näited, kus õngitsuskirjale viitavad elemendid on ümber märgitud punaste kastidega.

Interneti ohuvektor kaardistab, veenab ja õpetab mooduli läbijale internetiga seonduvaid riske. Antud mooduli puhul keskendutakse turvalise internetiühenduse loomisele kasutades privaatvõrgu lahendust (inglise keeles *virtual private network*) ning selgitatakse mooduli läbijale, kuidas turvaliselt veebis liigelda. Näiteks kuvatakse kasutajale kaasus, kus isik on eiranud turvalise internetikülastuse põhimõtteid ning mooduli läbijalt soovitakse teada, kas ja miks ei olnud kaasuses mainitud isiku käitumine turvaline.

2.3.3. Organisatsioon

Kategooria „Organisatsioon" hindab kasutaja riske tulenevalt organisatsiooni eripäradest. Vektoritena vaadeldakse kolme elementi: „Organisatsioonikultuur", „Erandite lubatavus", „Infohaldus".

Organisatsioonikultuur annab ülevaate organisatsioonist üleüldiselt, kas on kombeks mõelda turvalisusele ning millised on kombed ja kirjutamata reeglid ohu maandamiseks. Näiteks kirjeldatakse kasutajale olukorda, kus peale pandeemia lõppu naasevad inimesed taas kontoritööle, kuid kontoris liigub ringi tundmatu daam, keda peetakse ettevõtte töötajaks. Kasutajalt soovitakse teada, kas tema hinnangul on ka tema organisatsioonis peale pandeemia lõppu sarnased riskid.

Infohaldus kaardistab, kui palju on organisatsiooni loodud reeglitest kasu ning kui hästi on töötajad organisatsiooni kehtestatud reeglitega kursis. Näiteks soovitakse kasutajalt teada, kas tal on piisavalt informatsiooni lunavararünnakutest ning nendega toimetulekuks.

Erandite lubatavus kaardistab, kui tihti on organisatsioonis kombeks kehtestada erandeid ning vaadata mööda kehtestatud turvareeglitest. Õpetatakse ning selgitatakse, mis riskid see võib endaga kaasa tuua. Näiteks kuvatakse mooduli läbijale kaasus, kus ettevõtte juht peab kasutama

sõnumite saatmiseks alternatiivset kanalit ning kasutajalt soovitakse teada, millist rakendust kasutada.

2.3.4. Isiksus

Kategooria „Isiksus" kuvatud profiilis koosneb kolmest vektorist: „Enesedistsipliin", „Suhtumine" ja „Koostöö". „Enesedistipliin" näitab kasutaja valmisolekut järjepidevalt järgida ja turvalisuse meetmeid. „Suhtumine" annab ülevaate mooduli läbija suhtumisest turvareeglite, tavade ja protsesside vastu. „Koostöö" näitab kasutaja valmidust teha koostööd ja kaasa mõelda turvalisusega seotud teemadel nii organisatsioonisiseselt kui ka läbitud kursuse raames.

Enesedistsipliini vektor kaardistab, kui järjepidevalt kasutaja järgib turvaeeskirju ja tavasid. Tagasi kontorisse moodulis keskendutakse peamiselt turvauuendustele, kus selgitatakse mooduli läbijale nende vajalikkust ning uuendamisega kaasnevat riski maandamist. Näiteks soovitakse eelküsimustiku osas kasutajalt teada, kuidas ta suhtub järjekordselt ekraanile ilmuvasse turvauuendusesse.

Suhtumise vektor kaardistab mooduli läbija suhtumist turvareeglistikesse ning tavadele, mis vähendavad tema kui ka organisatsiooni riski.

Suhtumist puudutavale vektorile ei loodud otseselt kaasuseid, kuid suhtumise tulemust mõjutasid teiste kaasuste vastused. Kui mooduli läbija annab oma valikvastustega mõista, et teda antud küsimus ei puuduta või tema tegevus ei mõjuta kuidagi organisatsiooni küberturvalisuse taset, siis hinnatakse kasutaja suhtumist riskantseks. Iga organisatsioon on täpselt nii turvaline, kui turvaline on tema kõige nõrgem töötaja. Seetõttu peab iga liige andma endast maksimumi, et tagada organisatsiooni terviklik turvalisus.

Koostöö vektor hindab mooduli läbija tahet kaasa mõelda turvaküsimustes nii läbitava mooduli raames kui ka organisatsioonisiseselt üldiselt.

2.4. Klientide vajaduste kaardistamine ja analüüs

Klientide tagasiside saamiseks kasutati ettevõtte BHC Laboratory OÜ platvormi STRATEX. STRATEX on kriisiõppuse platvorm, millega korraldatakse erinevaid õppuseid, näiteks kriisiõppuseid, stsenaariumipõhiseid arutelusid, organisatoorsete poliitikate ja protseduuride kontrollõppuseid jne. Õppust juhib moderaator ning kasutajad läbivad õppusel kriisi stsenaariumi, mille käigus pannakse proovile kasutajate otsustusvõime keerulistes

situatsioonides. Iga küsimuse järel kuvatakse ekraanile graafikud kasutajate valikutest ning moderaator analüüsib tulemusi. Platvorm on ideaalne tööriist küsitluse läbiviimiseks, sest STRATEX platvormi kasutajatel on väga intuitiivne liides, mille abil on lihtne küsimustele vastata ning kommentaare jätta. Platvorm koostab iseseisvalt hästi loetavad graafikud ning ettevõte saab olla kindel, et andmed ei leki mõnele kolmandale osapoolele, sest platvormi majutatakse ettevõtte enda serverites.

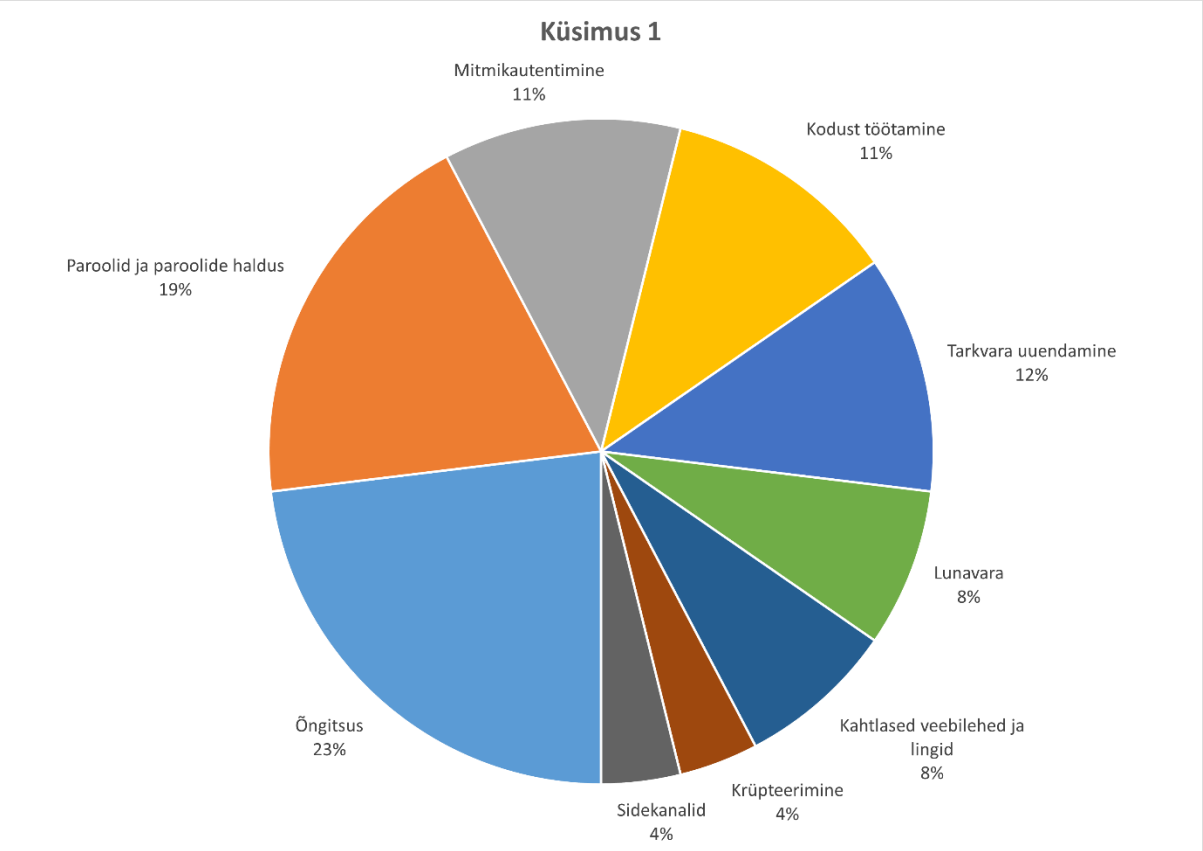
Küsitlus viidi läbi anonüümselt ning küsitluse eesmärgiks oli uurida klientide ootusi uuele moodulile ning selgitada välja, mis on hetkel kõige olulisemad küberturbe teemad, mida tuleks uues moodulis käsitleda. Läbi viidud küsitlus oli suunatud ettevõtete infoturbejuhtidele ning nende meeskondadele. Kaardistati klientide poolt välja toodud hetke küberohud, juhtunud intsidendid ning kliendi ettevõtte jaoks kõige paremini materjali edasi andvad lisandväärtuslikud mooduli elemendid - pildid, videod jms. Küsimustik sisaldas viit küsimust, mis on välja toodud Lisas 1.

Klientide puhul võeti ühendust organisatsiooni infoturbejuhiga või organisatsioonis infoturvet korraldava kontaktisikuga. Organisatsioonide infoturbejuhtidele ja kontaktisikutele teatati küsitluse toimumisest telefonitsi või e-posti teel. Kui organisatsioon nõustus osalema küsitluses, saadeti pikem küsimustikku puudutav informatsioon neile e-posti teel. E-kirjas selgitati küsimustiku toimumise vormi ning saadeti ette ka küsimustiku küsimused, et vastajatel oleks võimalik juba eelnevalt nende küsimuste peale mõelda. Küsimustikku oli nõus täitma 19 kasutajat ning nõustunud kasutajate STRATEX platvormi sisselogimise kredentsiaalid saadeti välja 19 kasutajale krüpteeritult nende e-posti aadressidele. Küsimustikule vastas 19st kasutajast 9 kasutajat.

Tagasisidest tuli välja, et klientide jaoks on hetkel kõige muret tekitavam teema õngitsusmeilid ja - veebilehed (inglise keeles *phishing*) ning tugevad salasõnad ja turvaline autentimine. Toodi välja, et uue mooduli sisu võiks õpetada ning tähelepanu juhtida, kuidas tunda ära õngitsusmeile ja -veebilehti. Täiendavalt ilmnes, et vastanute jaoks on väga oluline teema tugevad salasõnad ja turvaline autentimine. Seoses ülemaailmse pandeemia lõpuga on üha enam inimesed naasemas kontoritööle. Sellega seoses küsiti vastajatelt, et kas on kontorisse tööle naasmisega esile kerkinud mõni spetsiifiline küberoht. Saadud vastuste kohaselt ei ole vastajad tundnud esile kerkinud küberohte.

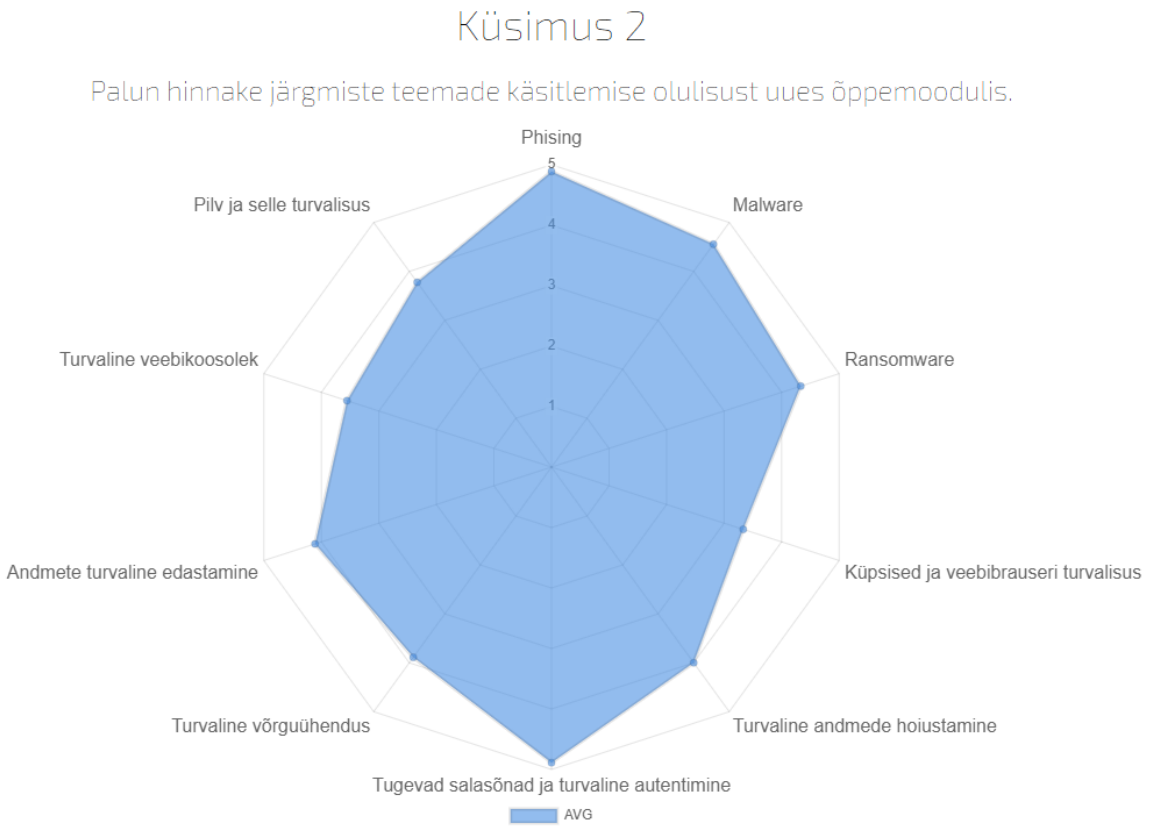
Tagasiside kohaselt teeb mooduli kaasahaaravaks peamiselt selgitava teksti lihtsus ja arusaadavus, elulised kaasused ning teemakohased näited ja illustratsioonid. Läbiviidud küsitluse tulemused kinnitasid autori varasemalt leitud andmeid.

Esimene küsimus oli koostatud avatud küsimusena, kus kasutajal tuli jätta oma vastus kommenteerimise lahtrisse. Küsitluses osalenutel paluti nimetada kolm küberturvalisuse teemat, mis on nende arvates hetkel eriti aktuaalsed. Kasutajate arvates olid hetke kõige aktuaalsemateks küberteemadeks (Joonis 6) õngitsus ning paroolid ja paroolide haldus. Küsitlusele vastajate jaoks olid olulisel kohal ka mitmefaktoriline autentimine, kodust töötamine, tarkvara uuendamine ja lunavara.



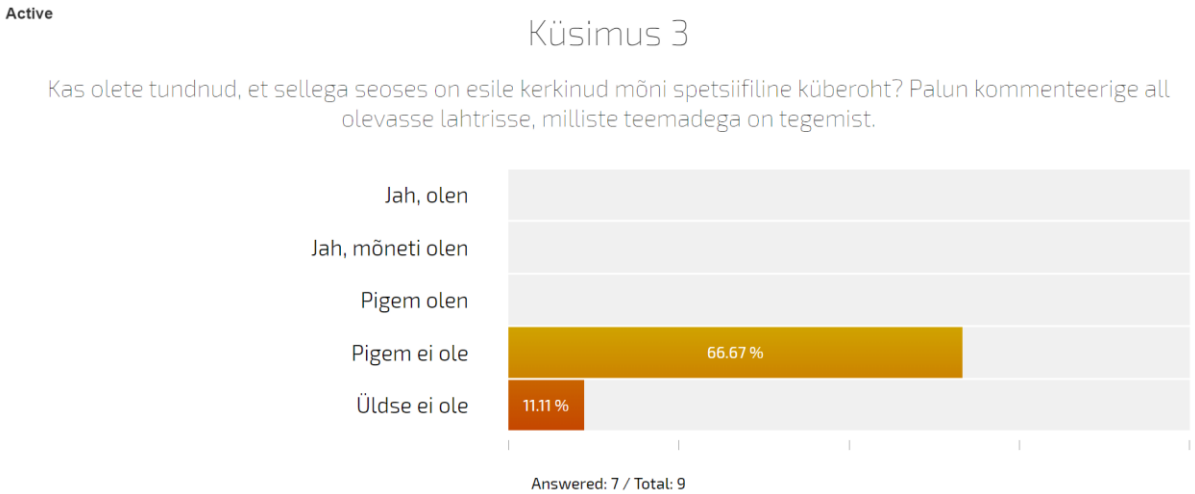
Joonis 6. Küsimustikus klientide poolt välja toodud asjakohased küberturvalisuse teemad.

Teine küsimus viidi läbi raamistikküsimusena (inglise keeles *framework question*), kus kasutajale oli ette antud 10 erinevat küberturbe teemat, mille puhul tuli märkida iga teema olulisus. Küsimuse tulemustest (Joonis 7) selgus, et kasutajate jaoks on etteantud teemadest kõige olulisemateks õngitsus (inglise keeles *phishing*) ning tugevad salasõnad ja turvaline autentimine, mille olulisust hinnati väärtusega 5/5st. Samuti peeti väga oluliseks pahavara (inglise keeles *malware*), lunavara (inglise keeles *ransomware*), turvalist andmete hoiustamist ja andmete turvalist edastamist, mille olulisusust hinnati vastavalt väärtustega 4.6/5st; 4,3/5st; 4/5st ja 4.1/5st.



Joonis 7. Vastanud klientide hinnang teemade käsitlemise olulisusest.

Kolmanda küsimusena sooviti klientidelt teada, kas seoses ülemaailmse pandeemia lõppemisega ning töötajate kontorisse tööle naasmisega on esile kerkinud ka mõni spetsiifiline küberoht. Küsitluse tulemuste (Joonis 8) põhjal selgus, et kliendid ei ole täheldanud küberohtude suurenemist seoses inimeste kontorisse tööle naasmisega.



Joonis 8. Klientide hinnang esile kerkinud küberohtude kohta seoses inimeste kontorisse tööle naasmisega.

Neljas küsimus viidi läbi taaskord raamistikküsimusena, kus klientidel tuli hinnata välja toodud elementide mõju mooduli interaktiivsusele ja kaasahaaravusele. Küsimuse tulemustest (Joonis 9) selgus, et kliendid peavad kõige olulisemaks õppematerjali selgitava teksti lihtsust ja arusaadavust. Samuti on nende jaoks oluline elulised kaasused ehk situatsioonide näited elust enesest.

Joonis 9. Klientide hinnang mooduli elementide mõjust mooduli interaktiivsusele.

Viies küsimus oli konstrueeritud avatud küsimusena, kus sooviti, et küsimustikule vastajad kirjeldaksid oma juhtumeid ja ohte, mida nad sooviksid ka teistega jagada. Kuus kasutajat üheksast jagasid platvormi STRATEX kaudu mitmeid elulisi juhtumeid ja situatsioone, mida kasutati ka mooduli kaasuste loomisel. Ühe situatsioonina toodi välja õngitsuskirja juhtum, kus ohvrile saadeti kiri, mis näiliselt saabub statistika ettevõttest. Kirjas viidi läbi uuring, mille sisuks oli teada saada, millist virtuaalvõrku kasutaja kasutab, mis viirusetõrje arvutis kasutusel on. Ohvrile lubati näilise küsitluse vastamise eest 50 euro suurune kinkekaart.

2.5. Kodust töötamise mooduli analüüs Eesti infoturbestandardi põhjal

Igal aastal tuleb CybExer Academy OÜ välja värske mooduli sisuga, mis hõlmab endast hetke kõige olulisemaid trende ja teadmisi, mida õpetada mooduli läbijatele. Aastal 2021 levis maailmas laialdaselt COVID-19 pandeemia, mistõttu pidid enamus inimesi töötama

kodukontoris. Kuna kodukontoris ja ettevõtte või organisatsiooni kontoris on tingimused ja ohud erinevad, loodi „Kodust töötamise moodul“, mis keskendub kodukontori ohtudele ja trendidele.

2022. aastal jõustub riigiteatajas E-ITSi määrus, mille jõustumisest alates saavad E-ITS kohuslased ennast auditeerida E-ITSi vastu [13]. E-ITSi eesmärk on tagada avalike ülesannete täitmiseks kasutatavate äriprotsesside ja infosüsteemide kõikehõlmav kaitse ning saavutada infoturbe ühtlane tase nende kõigis osades [8]. CybExer Academy OÜ klientide seas on palju avalikke ülesandeid täitvaid asutusi. Kuna selle töö aluseks on eelmise aasta Kodust töötamise moodul, leidis autor et materjalide ettevalmistuse raames oleks mõistlik analüüsida ka tolle materjali teemade vastavust uue standardiga.

Eesti infoturbestandard on eestikeelne ja Eesti õigusruumile vastav infoturbe käsitlemise alusraamistik [8]. E-ITS on kooskõlas rahvusvaheliselt tunnustatud infoturve halduse standardiga ISO/IEC 27001 ning aluseks on Saksa päritolu BSI IT-Grundschutz etalonturbe meetod [8]. Eesti infoturbestandardi eesmärgiks on arendada ja parandada Eesti asutuste infoturvet [7]. Dokument on kohustuslik avalikke ülesandeid täitvatele ettevõtetele ja organisatsioonidele, kuid on ka soovitatav rakendada erasektori ettevõtete puhul [8]. Eelnevalt oli Eestis kasutusel ISKE ehk infosüsteemide kolmeastmeline etalonturbe süsteem, mis aegub 31.12.2023 [8] ning Eesti infoturbestandardi määrus jõustub 2022. aastal [13]. Kahe aasta jooksul tuleb üle minna vanalt standardilt uuele.

Bakalaureusetöö käigus analüüsiti Kodust töötamise mooduli õppematerjali osa ning selle vastavust Eesti infoturbestandardiga. Eesti infoturbestandardi etalonturbe kataloog kirjeldab väga detailselt ära organisatsiooni infoturbe korraldamise, taristu, personali, sidevõrke, süsteeme puudutavad ohud ja meetmed. Välja on toodud konkreetsed ohud ja mured ning milliste meetmetega neid parandada. Analüüsi käigus käidi läbi kõik kaasused ning õppematerjalid ning otsiti üles neile vastavad punktid standardis. Leiti, et kõikidel kaasustel ja õppematerjalidel on tugev seos Eesti infoturbestandardi etalonturbe kataloogiga ning kõik kaasuste õppematerjalid olid kaudselt vastavuses Eesti infoturbestandardi etalonturbe kataloogis välja toodud meetmetega.

Peatükis selgitati platvormi DeLRAP olemust, metoodikat ning ülesehitust. Lisaks analüüsiti klientide vajaduste kaardistamiseks läbi viidud küsitluse tulemusi ning kirjeldati CybExer Academy OÜ poolt loodud varasema Kodust töötamise mooduli vastavust Eesti infoturbestandardi 2021 versiooniga. Järgmises peatükis esitletakse valminud õppematerjali.

3. Valminud õppematerjal moodulile „Tagasi kontorisse“

Peatükis antakse ülevaade valminud õppematerjalist. Selgitatakse valminud õppematerjalide teemade ja kaasuste käsitlust vektorite kaupa ning tuuakse näiteid valminud õppematerjali kaasustest ja testi küsimustest.

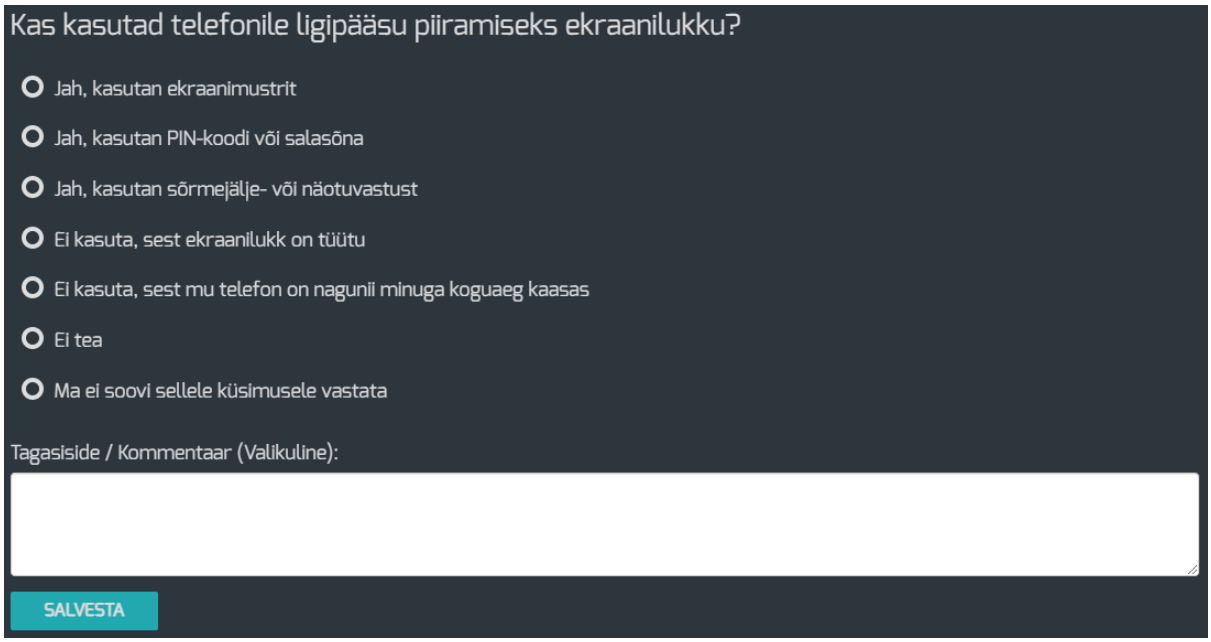
3.1. Kategooria „Teadmised”

Kategooria „Teadmised” sisaldab endas kolme ohuvektorit – „Autentimine“, „Andmete hoiustamine“, „Seadmed ja võrgud“.

Autentimise vektori raames veendakse kasutajat autentimise olulisuses. Kasutajale selgitatakse, milline peab olema tugev parool. Sealhulgas selgitatakse parooli loomise mnemoonilised võtteid, mis aitavad tugevat parooli meeles hoida. Salasõnade kattuvuse vältimiseks ning mitte kattuvate salasõnade meelespidamiseks soovitatakse kasutada paroolihaldurit. Mooduli läbijat veendakse kasutama oma kontode turvalisemaks muutmiseks mitmefaktorilist autentimist. Mooduli testi osas küsitakse küsimusi, mida õpetati õppematerjali osas. Näiteks antakse testi osas mooduli läbijale neli erinevat parooli, millest hulgast tuleb tal valida turvaline ning meeldejääv parool.

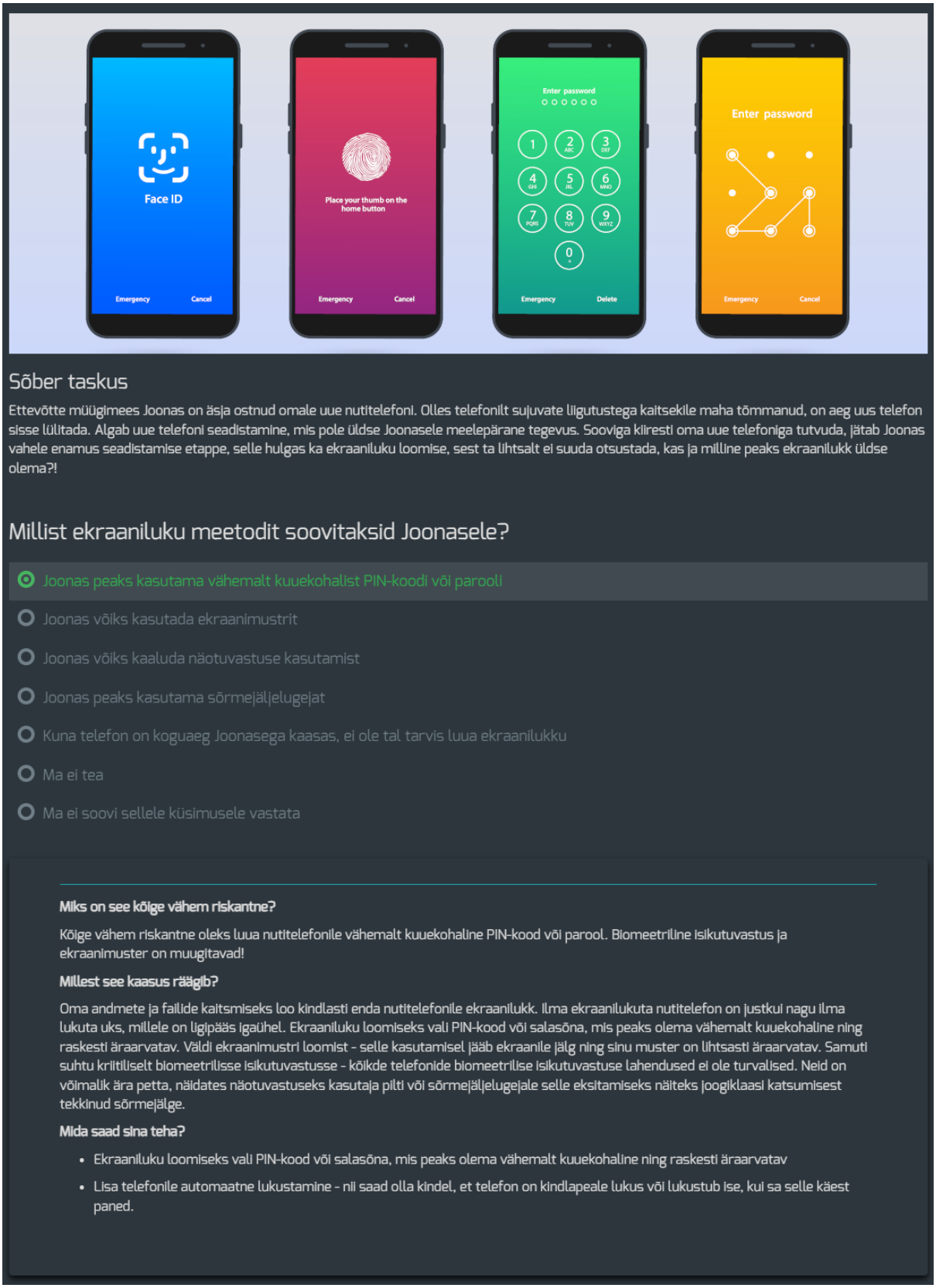
Seadmed ja võrgud vektor selgitab kasutajale, kuidas muuta koduinterneti ruuter turvalisemaks, millised on nutika kodu ohud ning kuidas luua oma telefonile turvaline ekraanilukk. Näiteks selgitatakse kasutajale, et oma nutitelefoni kaitsmiseks tuleb kindlasti kasutada ekraanilukku. Parim viis selleks on vähemalt kuuekohalise PIN-koodi või salasõna kasutamine. Mooduli eelküsimustiku osas soovitakse kasutajalt teada, kas ja millist ekraaniluku tüüpi ta kasutab oma telefonile ligipääsu piiramiseks (Joonis 10). Kõige vähem riskantsemaks on märgitud vastus „Jah, kasutan PIN-koodi või salasõna“. Üldjuhul on turvaline ka kasutada sõrmejälje- või näotuvastust, kuid vanemate nutitelefonide puhul ei pruugi sõrmejälje- ja näotuvastuse lahendused olla nii turvalised ning neid on võimalik ära petta. Seetõttu märgiti sõrmejälje- ja näotuvastuse kasutamise vastus kollase riskivärviga. Seda kinnitab ka RIA ajaveeb [2]. Vastuse „Jah, kasutan ekraanimustrit“ värviks märgiti oranž, kuna peale ekraanimustri sisestamist võib ekraanile jääda ekraanimustri jälg. Nii on ründajal lihtne ära arvata ohvri ekraanimustrit. Vastused „Ei kasuta, sest ekraanilukk on tüütu“ ja „Ei kasuta,

sest mu telefon on nagunii minuga koguaeg kaasa“ on märgitud väga riskantseteks ning samuti mõjutavad need vastused negatiivselt ka kasutaja suhtumist turvaküsimustesse.



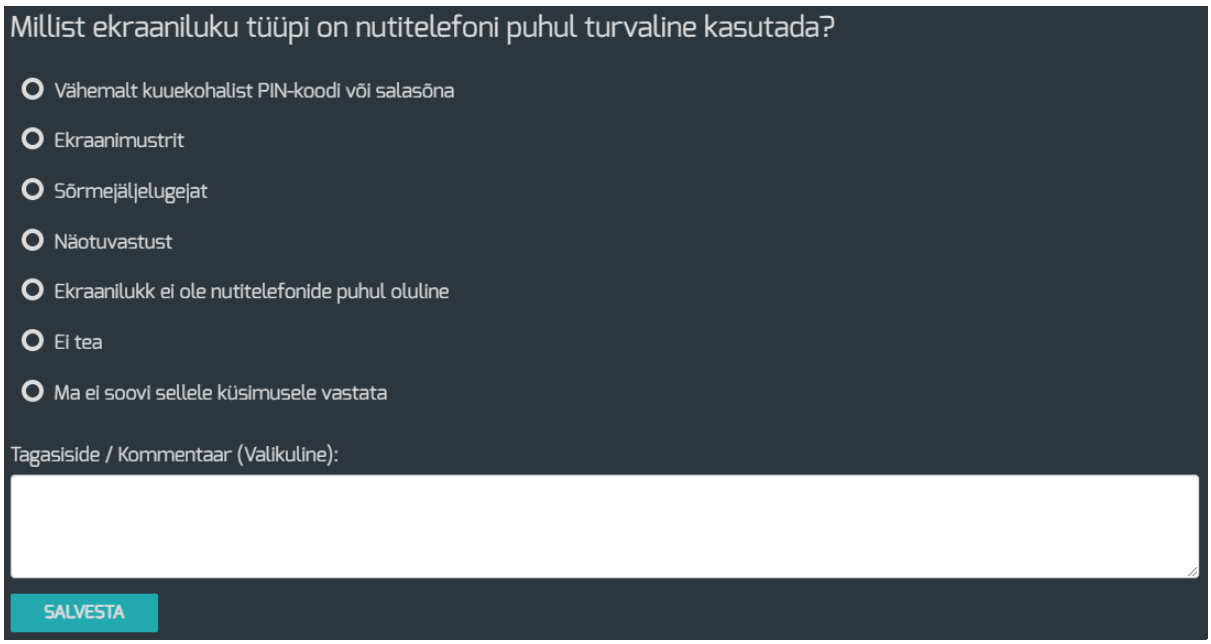
Joonis 10. Vektori "Seadmed ja võrgud" nutitelefoni ekraanilukku puuduva teema eelküsimustiku küsimus.

Õppematerjali osas kirjeldatakse kasutajale olukorda ning soovitakse teada, millist ekraaniluku meetodit ta soovitaks olukorras välja toodud isikule (Joonis 11). Seejärel selgitatakse mooduli läbijale teiste ekraanilukkude puudused ja ohud ning soovitatakse nutitelefonil aktiveerida automaatne ekraani lukustus. Nii saab nutitelefoni kasutaja olla kindel, et nutitelefonis olev teave on kaitstud isegi siis, kui kasutaja unustab oma nutitelefoni lukustada.



Joonis 11. Vektori "Seadmed ja võrgud" nutitelefoni ekraanilukku puuduva teema õppematerjali osa kaasus ja õppematerjal.

Mooduli järeltesti osas hinnatakse kasutaja omandatud teadmisi, küsides kasutajalt, millist ekraaniluku tüüpi on nutitelefonide puhul turvaline kasutada (Joonis 12).



Joonis 12. Vektori "Seadmed ja võrgud" nutitelefoni ekraanilukku puuduva teema järeltesti küsimus.

Andmete hoiustamise vektori raames veendakse kasutajat süsteemselt andmeid varundama. Selgitatakse, mis on lunavararünnak ning kuidas varundamine selle vastu aitab. Andmete varundamiseks tuuakse välja erinevad lahendused, sealhulgas keskendutakse rohkem pilveteenustele, mis tagab kasutaja andmete automaatse ja mugava varundamise. Üheks loodud kaasuseks on olukord, kus ettevõtte raamatupidaja on väga hoolikas arvutikasutaja ning mooduli läbijalt soovitakse teada, kas raamatupidajal on vaja karta lunavararünnakut. Õppematerjalides selgitatakse, mis on lunavararünnak, kes on selle sihtmärgid ning kuidas vältida lunavararünnakust tulenevaid tagajärgi ning kuidas käituda lunavararünnaku korral.

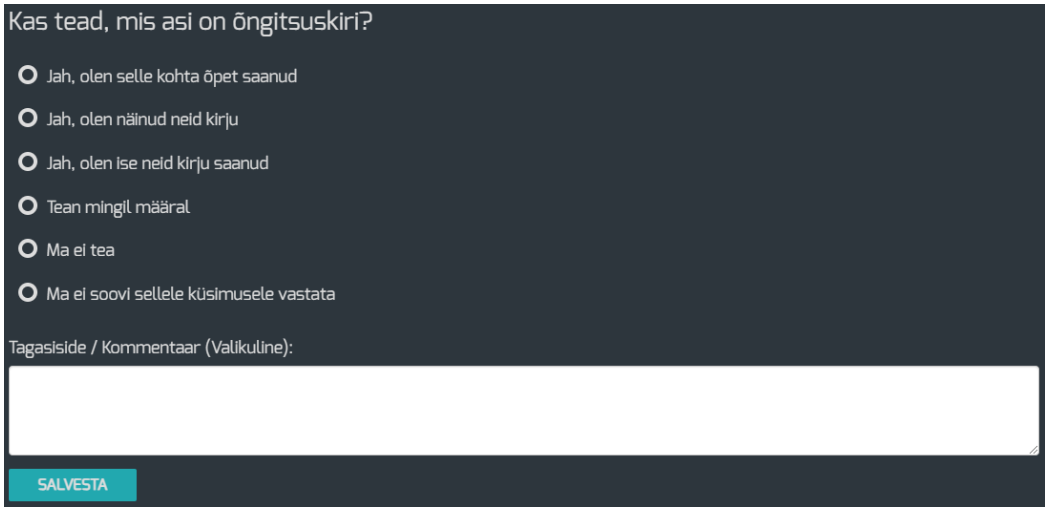
3.2. Kategooria „Haavatavus”

Kategooria „Haavatavus” kaardistab kasutaja riske sattuda oma küberkäitumisega võimalike küberrünnakute alla. Tegemist on üldteemaga, milles käsitlevaid teemad ei olene otseselt kasutajast, vaid keskenduvad võimalikele küberrünnakutele ning selle, kuidas tekkinud olukorras käituda ja riske maandada. Kategooria „Haavatavus” koosneb kolmest vektorist - Sotsiaalmeedia, E-post, Internet.

Sotsiaalmeedia vektori puhul keskendub uus sisu sotsiaalmeedia platvormil Facebook levivatele ohtudele. Õppematerjal selgitab kasutajale, mida tähendab laikide farmimine (inglise keeles *like-pharming*). RIA on oma ajaveebis [14] selgitanud laikide farmimist järgnevalt: „pahategevus, mille eesmärk on FB's püstipandud kurilehele suuremat külastatavust toota ja selle kaudu oma eesmärki reklaamida". Kasutajale selgitatakse, kuidas üks süütuna näiv sotsiaalmeedia postituse jagamine või meeldivaks märkimine võib kaasa aidata tulevikus läbiviidavatele küberrünnetele. Mooduli läbijale selgitatakse sotsiaalmeedias levivat andmepüüki ning libakontosid, mille abil üritatakse varastada tundlikku informatsiooni. Üheks loodud sotsiaalmeedia kaasuseks on olukord, kus sotsiaalmeedia platvormi kasutajale saadab sõnumi tema sõber. Sõber väidab, et nägi kaasuse peategelast ühes videos ning sõnumis on välja toodud ka kahtlane link, mis justkui viitaks mainitud videole. Mooduli läbijalt küsitakse, kuidas sellises situatsioonis käituda ning selgitatakse, et tegemist võib olla ründega. Sellises olukorras ei tohiks mitte kunagi lingile vajutada. Võimalusel tuleks ühendust võtta sõbraga mõne teise kanali kaudu, et välja selgitada, kas tegemist võis olla ründega. Lingile klõpsates on oht, et laetakse ohvri arvutisse pahavara, varastatakse tema andmed või kaaperdatakse tema sotsiaalmeedia konto.

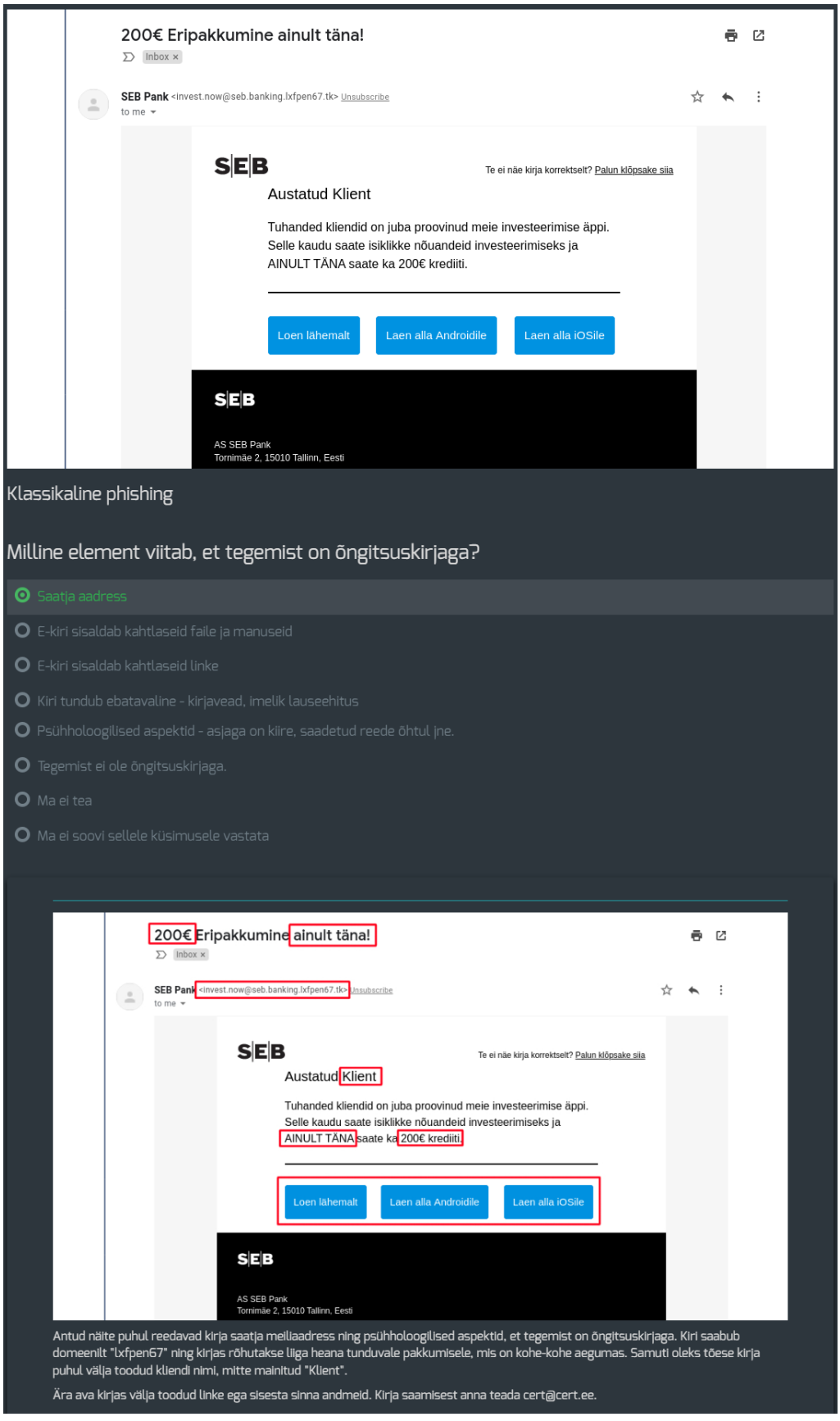
E-posti vektor keskendub õngitsuskirjade tuvastamisele. Kasutajale selgitatakse, millised on need elemendid, mille järgi tuvastada õngitsuskirja. Esmalt selgitatakse mooduli läbijale, mis on õngitsuskiri ning kuidas seda ära tunda. Seejärel kuvatakse õngitsuskirjade näited, mille puhul mooduli läbija peab tuvastama need elemendid, mis viitavad, et tegemist on õngitsuskirjaga. Eesti- ja inglisekeelsete õngitsuskirjade näidised koostasid bakalaureusetöö autor ning ettevõtte CybExer Academy OÜ töötaja Richard Jõgi. Õngitsuskirjad kehastavad suuri ettevõtteid, kes pöörduvad kliendi poole, suunates klienti avama kirjas toodud linki, laadima alla ja avama manuseid või saatma tagasi tundlikku informatsiooni.

Eelküsimustiku osas soovitakse kasutajalt teada, kas ta teab, mis asi on õngitsuskiri (Joonis 13). Nii kaardistatakse mooduli läbija varasem kokkupuude õngitsuskirjadega.



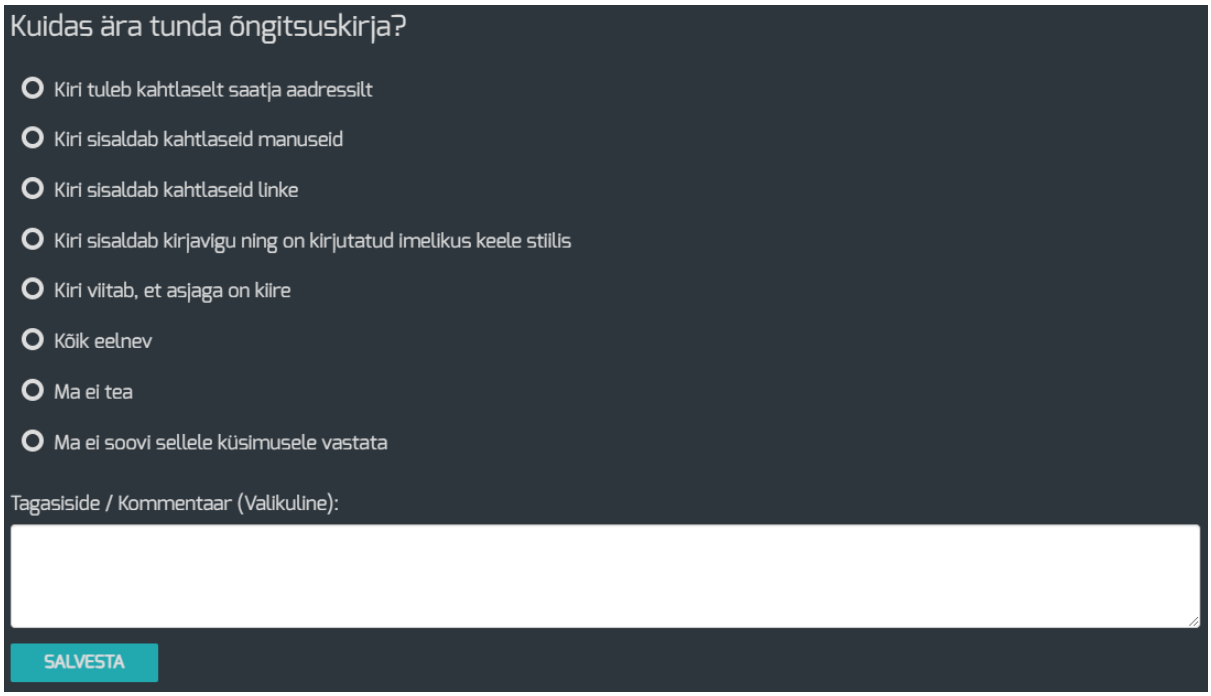
Joonis 13. Vektori "E-post" õngitsuskirju puuduva teema eelküsimustiku küsimus.

Õppematerjali osas kuvatakse kasutajale õngituskirja näide (Joonis 14). Mooduli läbijal palutakse valida valikvastuste hulgast element, mille põhjal kasutaja arvab, et tegemist on õngitsuskirjaga. Selgitavas osas tuuakse pildinäitega välja kõik elemendid, mis vihjavad, et tegemist on õngitsuskirjaga.



Joonis 14. Vektori "E-post" õngitsuskirju puuduva teema õppematerjali kaasus ja õppematerjal.

Järeltesti osas küsitakse mooduli läbijalt, millise elemendi põhjal on võimalik ära tunda õngitsuskirja (Joonis 15). Antud küsimuse eesmärgiks on tuua kasutajale silme ette kõik eelnevalt selgitatud õngitsuskirja elemendid, et kinnistada õpitut. Kasutajale on valikvastusteks välja toodud kõik eelnevalt õppematerjalis käsitletu. Valede vastustega kasutajat siinkohal ei eksitata. Vastused „Kiri tuleb kahtlaselt saatja aadressilt“, „Kiri sisaldab kahtlaseid manuseid“, „Kiri sisaldab kahtlaseid linke“, „Kiri sisaldab kirjavigu ning on kirjutatud imelikus keele stiilis“ ning „Kiri viitab, et asjaga on kiire“ on kõik märgitud kollase riskitasemega. Vastused on küll õiged, kuid õngitsuskirja ära tunda ainult ühe elemendi põhjal on raske. Seetõttu on rohelisega märgitud vastuseks „Kõik eelnev“, et kasutaja oleks teadlik kõigist õppematerjalis käistletud õngitsuskirja elementidest.



Joonis 15. Vektori "E-post" õngitsuskirju puuduva teema järeltesti küsimus.

Interneti vektor käsitleb teemasid nagu virtuaalne privaatvõrk (VPN) ja õngitsuslehed. Moodulis selgitatakse kasutajale, kuidas luua turvaline võrguühendus ning kuidas turvaliselt internetis ringi liikuda. Virtuaalse privaatvõrgu puhul tuuakse välja ohud, mis võivad kaasneda virtuaalset privaatvõrku kasutades. Näiteks, kui kasutaja laeb alla ning kasutab tasuta virtuaalse privaatvõrgu lahendust, on oht, et tema võrguliiklust kuulatakse pealt või kogutakse ja varastatakse tema andmeid.

3.3. Kategooria „Organisatsioon”

Kategooria „Organisatsioon” kaardistab organisatsiooni riske sattuda oma küberkäitumisega võimalike küberrünnakute alla. Tegemist on üldteemaga, milles käsitlevaid teemad ei olene otseselt kasutajast, vaid vaatlevad organisatsiooni tervikuna. Kategooria „Organisatsioon” koosneb kolmest vektorist - Organisatsioonikultuur, Erandite lubatavus, Infohaldus.

Organisatsioonikultuuri vektori juures kaardistatakse organisatsiooni IT-toe abivalmidust ning organisatsiooni üldist küberturvalisust mooduli läbija vaates. Õppematerjalis tuuakse välja kaasus, mis peale COVID-19 pandeemia lõppu on väga aktuaalne. Inimesed tulevad üha enam tagasi kontoritööle, kuid peale aastat kodukontoris töötades ei tunne nad oma uusi kolleege. Sel juhul on tegemist potentsiaalse ohuga, kus ründaja võib kontoris vabalt ringi liikuda, sest tegemist on nende arvates kolleegiga, keda nad lihtsalt ei tunne.

Erandite lubatavuse vektor keskendub olukorrale, kus vaatama regulatsioonidele on erandite rakendamine vajalik. Antud moodulis selgitatakse kasutajale turvalisi alternatiivseid sõnumirakendusi, mille kasutamine ei sea organisatsiooni ohtu, kui tekib vajadus kasutada organisatsioonivälise andmevahetuse kanaleid. Kaasuses kirjeldatakse juhtumit, kus ettevõtte juhil on käimas kohtumine, kuid tiheda graafiku tõttu tuleb tal samal ajal tundlikku infot vahetada sõnumitena. Kasutajalt küsitakse, millist järgnevatest sõnumirakendustest tema sellises situatsioonis kasutaks. Valikuvariantides on välja toodud Facebook Messenger, Yandex Messenger, WeChat, telefoni tekstisõnum ja Signal. Mooduli läbijale selgitatakse, et Venemaa ja Hiina rakendused nagu Yandex Messenger ja WeChat jälgivad vestluseid ning koguvad andmeid. Facebook Messengeri sõnumid on küll krüpteeritud, kuid Facebookil on siiski ligipääs sõnumite sisule. Kasutajal soovitatakse kasutada Signalit, mis on Ameerika Ühendriikides loodud sõnumirakendus, mis kasutab otspunktkrüpteeringut.

Infohalduse vektor kaardistab, kas organisatsiooni infohaldust. Moodul mõõdab ning annab ülevaate, kas organisatsiooni töötajatel on piisav ligipääs organisatsiooni turvareeglitele ning kas nad on nendest teadlikud. Näiteks küsitakse valminud mooduli testi osas mooduli läbijatelt, kas nad on kursis, kust leida enda organisatsiooni küberturvalisuse eeskirju.

3.4. Kategooria „Isiksus”

Kategooria „Isiksus” kaardistab mooduli läbija individuaalset lähenemist turvalisuse küsimustele. Kategooria jaguneb kolmeks vektoriks - enesedistipliin, suhtumine, koostöö.

Enesedistsipliin käsitles temaatiliselt peamiselt uuendusi puudutavat teemat. Kaardistatakse mooduli läbija suhtumine turvauuendustesse. Seejärel selgitatakse ja veendakse mooduli läbijat, miks turvauuendused on olulised. Näiteks on loodud enesedistsipliini vektorile järgnev kaasus: Tõenäoliselt saad tihti operatsioonisüsteemilt ja rakendustelt märguandeid, mis annavad märku, et sa neid uuendaksid. Millegipärast saabuvad need alati siis, kui sul on kiire! Nii juhtus ka Taavil. Taavi luges parasjagu üht olulist dokumenti, kui ilmus tema arvutiekraanile märguanne järjekordsest turvauuendusest.
Mooduli läbijalt küsitakse, kuidas ta käituks sellises situatsioonis. Kasutajale antakse järgmised valikuvariandid:

- Uuendan arvuti koheselt
- Lükkan uuendamise edasi
- Planeerin uuendamiseks lähima sobiva aja ning märgin selle ka endale kalendrisse
- Ignoreerin märguannet
- Ma ei tea
- Ma ei soovi sellele vastata

Kõige vähem riskantsemaks on märgitud vastused „Uuendan arvuti koheselt" ning „Planeerin uuendamiseks lähima sobiva aja ning märgin selle ka endale kalendrisse". Seejärel selgitatakse mooduli läbijale miks on see kõige vähem riskantsem vastus, millest see kaasus räägib ning mida saab kasutaja teha, et oma küberriski antud valdkonnas vähendada.

Miks on see kõige vähem riskantsem vastus?

Kõige vähem riskantsem oleks teha uuendus koheselt või ajapuuduse tõttu ka planeerida endale lähim võimalik aeg uuenduste tegemiseks. Nii parandatakse tekkinud turvaaugud esimesel võimalusel, mis vähendab riski potentsiaalseks ründeks, mis kasutab ära olnud turvaauke.

Millest see kaasus räägib?

Uuendused ei ole pelgalt opratsioonisüsteemi viis sind närvi ajada. Turvaaukude avaldamisel kasutavad ründajad neid ära koheselt. Kiirus loeb - mida kiiremini teed uuenduse ära, seda väikem on risk langeda rünnaku ohvriks. Uuenduse välja tulemisel on info avalik esinevate turvanõrkuste kohta, mida kasutatakse ära koheselt!

Mida saad sina teha?

- Uuenda tarkvara koheselt, kui arvuti annab uuendusest teada
- Aja puudusel planeeri aeg, mil enda tarkvara uuendada
- Ära lükka uuendamist edasi - nii suurendad riski sattuda küberrünnaku ohvriks
- Võimaluse korral lülita sisse automaatne uuendamine

Suhtumise vektor kaardistab mooduli läbija suhtumise turvaküsimustesse ning koostöö vektor kaardistab mooduli läbija koostöövalmiduse mõelda kaasa turvaküsimustes. Tegemist ei ole eraldi küberhügieeni teemadega, kuid annavad põhjaliku ülevaate mooduli läbija isiksusest. Näiteks, kui mooduli läbija valib küsimuse vastuseks, et antud teema ei ole oluline, annab see mõista, et kasutaja hoiak küberturvalisuse probleemidele on vale.

Koostöö vektor kaardistab mooduli läbija valmidust teha koostööd turvaküsimustes. Kui kasutaja valib valikvastuseks, et ta ei soovi sellele küsimusele vastata, siis määratakse tema koostöö vastava küsimuse puhul punase riskiastmega. Samuti, kui kasutaja valib valikvastuseks „Ma ei tea", siis märgitakse tema koostöö vastava küsimuse puhul oranži riskiastmega, sest kasutaja ei anna maksimaalset panust leida probleemile lahendus turvaküsimustes.

Töö käigus valmis 14 eeltesti küsimust, 25 kaasust koos selgitava õppematerjaliga ning 12 lõpptesti küsimust. Õppematerjali küsimustele lisati olukorda illustreerivad pildid ning tulem vormindati platvormile sobivasse formaati ning imporditi ettevõtte testplatvormi. Edasise sammuna kinnitatakse mooduli sisu ettevõtte poolt ja saadetakse valminud õppematerjal keeletoimetusse, et moodul „Tagasi kontorisse" oleks keeleliselt korrektne ja üheselt mõistetav. Pärast täiendavaid kontrolle tehakse küberhügieeni õppemoodul kättesaadavaks ettevõtte klientidele. Töö lisades ei avaldata loodud õppematerjali, sest see läheb vastuollu ettevõtte ärihuvidega. DeLRAP platvormis olev moodul „Tagasi kontorisse" tehakse kättesaadavaks töö retsensendile ning kaitsmiskomisjonile.

Kokkuvõte

Küberuum meie ümber on pidevalt arenev. Pidevalt parandatakse küberturvalisust, kuid need teadmised ja õppematerjalid ei ole sageli tavainimesele atraktiivsed ning intuitiivselt mõistetavad, mistõttu on vaja inimeste küberteadlikkus pidevalt tõsta läbi praktiliste näidete. Käesoleva bakalaureusetöö eesmärgiks oli luua CybExer Academy OÜ platvormile DeLRAP uus küberhügieeni moodul, mis keskendub kasutajate küberteadlikkuse tõstmisele ning nende riskide välja selgitamisele.

Kuna üha enam inimesi naaseb tagasi kontoritööle, on loodud mooduli nimeks „Tagasi kontorisse". Tegemist on hübriidmooduliga, mis keskendub küberohtudele nii tavakontori kui ka kodukontori perspektiivist. Varasemalt on ettevõte iga aasta välja tulnud uue küberhügieeni õppemooduliga, mis keskendub viimase aasta kõige levinumatele küberohtudele. Selle aasta uue mooduli sisu loodi tuginedes hetke küberohtudele, Eesti infoturbestandardi 2021. aasta versioonile ning klientide vajaduste kaardistamiseks läbiviidud küsitluse analüüsile. Loodud moodul koosnes eelküsimustikust, õppematerjali osast ning järeltestist. Töö tehnoloogilised piirangud olid ette antud ettevõtte CybExer Academy OÜ poolt, kus autor kirjutamise ajal töötas.

Uue küberhügieeni mooduli „Tagasi kontorisse" eesmärgiks on õpetada kasutajale, millised on hetkel levinumad ohud ning kuidas sellistes olukordades enda riski vähendada. Mooduli läbija parandab oma küberhügieeni teadmisi ning oskab õpitu põhjal vältida igapäevaseid küberriske. Kasutajale genereeritakse vastatud vastuste põhjal riskimaatriks, mis näitab isikule ära tema nõrgad kohad määratud valdkondades. Riskimaatriks on infoturbejuhile nähtav ka gruppide ning kogu organisatsiooni põhiselt. Nii saab organisatsioon ülevaate oma töötajate küberhügieeni teadmistest ja võimalikest riskidest.

Töö käigus valmis 14 eelküsimustiku küsimust, 25 kaasust koos selgitava õppematerjaliga ning 12 lõpptesti küsimust. Õppematerjal vormistati sobivasse formaati ning laeti üles ettevõtte testplatvormile. Edasise sammuna kinnitatakse mooduli sisu ettevõtte poolt ning valminud mooduli vaatab üle keeletoimetus, et mooduli õppematerjalid oleksid keeleliselt korrektsed ning üheselt mõistetavad. Pärast täiendavaid kontrolle tehakse küberhügieeni õppemoodul kättesaadavaks ettevõtte klientidele.

Viidatud kirjandus

[1] Neigel A., Claypoole V., Waldfogle G., Acharya, S., Hancock G. Holistic cyber hygiene education: Accounting for the human factors. *Computers & Security*, Vol 92, 2020, https://www-sciencedirect-com.ezproxy.utlib.ut.ee/science/article/pii/S0167404820300183?via%3Dihub (29.03.2022)

[2] Riigi Infosüsteemi Amet. Riigi Infosüsteemi Ameti nõuanded. https://www.ria.ee/et/kuberturvalisus/nouanded/nutiseadmete-turvalisus.html (29.03.2022)

[3] Microsoft. Microsoft Digital Defense Report, 2021. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi?id=101738 (25.04.2022)

[4] Riigi Infosüsteemi Amet. Küberturvalisuse aastaraamat 2022. https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria_kyberturvalisuse_aastaraamat_2022_est_veeb.pdf (29.03.2022)

[5] F-Secure. What is a ransomware attack?. https://www.f-secure.com/en/home/articles/what-is-a-ransomware-attack (25.04.2022)

[6] Barracuda. Key findings on the latest social engineering tactics and the growing complexity of attacks, *Spear Phishing: Top Threats and Trends*, vol 7, 2022. https://assets.barracuda.com/assets/docs/dms/Spear-phishing-vol7.pdf (29.03.2022)

[7] Riigi Infosüsteemi Amet. KKK. https://eits.ria.ee/et/avalehe-menueue/kkk/ueldine/#kuesimus1millaljoustubeits1 (19.03.2022)

[8] Riigi Infosüsteemi Amet. Eesti infoturbestandard. https://www.ria.ee/et/kuberturvalisus/eesti-infoturbestandard.html (19.03.2022)

[9] Riigi Infosüsteemi Amet. ISMS. Nõuded. https://eits.ria.ee/et/versioon/2021/juhendid/isms-noouded/#4eitsolemus8 (19.03.2022)

[10] Advisera. What is ISO 27001? Quick and easy explanation. https://advisera.com/27001academy/what-is-iso-27001/ (06.05.2022)

[11] Panhalkar T. ISO 27001 Annex : A.7.2 During Employment. https://info-savvy.com/iso-27001-annex-a-7-2-during-employment/ (25.04.2022)

[12] Riigi Infosüsteemi Amet. Eesti infoturbestandard. https://eits.ria.ee/et/versioon/2021/etalonturbe-kataloog/orp-organisatsioon-ja-personal/orp3-infoturbe-teadlikkuse-toostmine-ja-koolitus/ (19.03.2022)

[13] Riigi Infosüsteemi Amet. Eesti infoturbestandard. https://eits.ria.ee/et/versioon/2020vers1/juhendid/luehijuhend/ (19.03.2022)

[14] Veri R. Laikide farmimine: ohud ja ennetus. 2016. https://blog.ria.ee/laikide-farmimine-ohud-ja-ennetus/ (09.05.2022)

Lisad

I. Klientide vajaduste kaardistamise küsitluse küsimused

0

Tere tulemast!

Tegemist on uue mooduli Back to Work tagasiside küsimustikuga, kus Teie vastused on anonüümsed.

Head vastamist!

1

Küsimus 1

Nimetage 3 küberturvalisuse teemat, mis on Teie arust hetkel eriti aktuaalsed.

2

Küsimus 2

Palun hinnake järgmiste teemade käsitlemise olulisust uues õppemoodulis.

Phising (õngitsusmeilid ja -veebilehed)

Täiesti ebaoluline	Pigem ebaoluline	Keskmise tähtsusega	Oluline	Ülioluline

Malware (pahavara)

Täiesti ebaoluline	Pigem ebaoluline	Keskmise tähtsusega	Oluline	Ülioluline

Ransomware (lunavara)

Täiesti ebaoluline	Pigem ebaoluline	Keskmise tähtsusega	Oluline	Ülioluline

Küpsised ja veebibrauseri turvalisus

Täiesti ebaoluline	Pigem ebaoluline	Keskmise tähtsusega	Oluline	Ülioluline

Turvaline andmede hoiustamine

Täiesti ebaoluline	Pigem ebaoluline	Keskmise tähtsusega	Oluline	Ülioluline

Tugevad salasõnad ja turvaline autentimine

Täiesti ebaoluline	Pigem ebaoluline	Keskmise tähtsusega	Oluline	Ülioluline

Turvaline võrguühendus

Täiesti ebaoluline	Pigem ebaoluline	Keskmise tähtsusega	Oluline	Ülioluline

Andmete turvaline edastamine

Täiesti ebaoluline	Pigem ebaoluline	Keskmise tähtsusega	Oluline	Ülioluline

Turvaline veebikoosolek

Täiesti ebaoluline	Pigem ebaoluline	Keskmise tähtsusega	Oluline	Ülioluline

Pilv ja selle turvalisus

Täiesti ebaoluline	Pigem ebaoluline	Keskmise tähtsusega	Oluline	Ülioluline

3

Küsimus 3

Ülemaailmne pandeemia on lõppemas ning üha enam suunduvad inimesed tagasi kontoritööle.

Kas olete tundnud, et sellega seoses on esile kerkinud mõni spetsiifiline küberoht? Palun kommenteerige all olevasse lahtrisse, milliste teemadega on tegemist.

- Jah, olen
- Jah, mõneti olen
- Pigem olen
- Pigem ei ole
- Üldse ei ole

4

Küsimus 4

Palun hinnake järgmiste elementide mõju mooduli interaktiivsusele ja kaasahaaravusele. Võite kommentaarides välja tuua, mis veel muudab Teie arvates mooduli kaasahaaravaks.

Elulised kaasused

Väga väike	Pigem väike	Keskmine	Pigem suur	Väga suur

Olukorda illustreerivad pildid

Väga väike	Pigem väike	Keskmine	Pigem suur	Väga suur

Õppevideod ja animatsioonid

Väga väike	Pigem väike	Keskmine	Pigem suur	Väga suur

Õppematerjali selgitava teksti lihtsus ja arusaadavus

Väga väike	Pigem väike	Keskmine	Pigem suur	Väga suur

5

Küsimus 5

Oleksime tänulikud, kui kirjeldate anonüümselt oma juhtumeid ning ohte, mida saaksime jagada küberturvalisuse kogukonnaga.

7

Täname!

Suur aitäh, et olite nõus vastama meie küsimustikule!

II. Litsents

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, **Tauno Tamm**,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose
   Küberhügieeni kursuse „Tagasi kontorisse" loomine DeLRAP platvormile,

   mille juhendajad on Alo Peets ja Lauri Almann,

   reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 4.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Tauno Tamm
09.05.2022