TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Piret Naber 183356IABM
Erki Murel 182769IABM

ETTEVÕTTE TURBEHALDUSE TÕHUSUSE MÕÕDIK

Magistritöö

Juhendaja: Ahto Buldas

Tallinn 2021

Autorite deklaratsioon

Kinnitame, et oleme koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autorid: Piret Naber ja Erki Murel

14.05.2021

Annotatsioon

Käesolev magistritöö käsitleb tänapäeval järjest olulisemaks muutunud teemasid küberturbe teadlikkusest isiklikus ja ka ettevõtte kontekstis.

Töö eesmärk on ära kaardistada ettevõtete turbehalduse tõhusus ja riskikohad. Eesmärgi saavutamiseks loovad autorid uue küberturvalisuse teadlikkust mõõtva tööriista, mis on koostatud arusaadavas keeles ja vormis, olgu vastajaks IT juht, reatöötaja või firma juht.

Töö tulemusena on valminud küsimustik ja seda toetav veebipõhine töövahend, millega on vastajal võimalik saada ülevaade oma infoturbealastest teadmistest hinnang ka ettevõtte küberturbe hetkeolukorrale.

Küsitluse valmimise esimeses faasis uurisid autorid asjaosalistelt, kas sedalaadi töövahendi järele on vajadust ja ega midagi samasugust juba olemas ei ole. Seejärel pöörati palju tähelepanu küsimuste sisulisele poolele ja testiti esmaseid versioone erinevate seotud osapoolte peal. Tegeleti ka idee kohandamisega Telia üldise küberturvalisuse teenuste lansseerimise plaaniga. Küsitluse tehniline osa valmis väliste arendajate kaasamisega.

Tänaseks asub test Telia küberturvalisuse maandumislehel ja kasutajad, kes sellele lehele jõuavad saavad enda teadlikkust testida ja vastuseks tulemustele vastavad kommentaarid ja soovitused.

Lisaks eeltoodule seavad autorid hüpoteesi, millega soovivad valideerida, et nende disainitud uus tööriist aitab kaasa küberturbe teadlikkuse tõusule ja motiveerib küsitlusele vastajaid oma olemasolevat olukorda jälgima ja puudustega tegelema.

Autorid usuvad, et kui järjepidevalt paluda ettevõtte töötajatel küsimustele vastata on tulemused igal aastal järjest paremad, kuna teadlikkus küberhügieeni ja küberturvalisuse baastaseme saavutamiseks on saadud. Ollakse ka teadlikud, millal ja millised on võimalused taseme tõstmiseks ja kelle poole peab pöörduma kui küberturbeintsident aset leiab.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 60 leheküljel, 5 peatükki, 6 joonist, 2 tabelit.

Abstract
The indicator of enterprise cybersecurity efficiency

This master's thesis deals with the increasingly important topic of cybersecurity awareness in the personal and also in the business context.

The aim of work is to survey the efficiency and risk areas of corporate security management. Authors are using through the process a security tool that is understood by everyone: an labourer, an IT manager or a company manager. The result should provide a baseline overview of the current situation and highlight the most critical issues that need to be addressed.

The authors would like to do this by creating a new cybersecurity awareness tool, written in an understandable language and format, whether the respondent is an IT manager, a line worker or a company manager.

As a result of the work, authors have developed a tool with which the user can get an overview of his / her information about security knowledge and it will also assess the current situation of his / her company.

In the first phases of the survey, the authors asked the parties whether there was a need for such a tool and whether something similar did not already existed. Much attention was then paid to the substance of the issues. The initial versions were tested on different parties. The idea was also adapted to Telia's overall cyber security service launch plan.

The technical part of the survey was completed with the involvement of external developers.

Today, the test is on Telia's cybersecurity landing page, and users who reach this page can test their awareness and respond with comments and suggestions in response to the results.

In addition to the above, the authors hypothesize to prove that the new tool they designed will help raise awareness of cybersecurity and motivate respondents to monitor their current situation and address shortcomings.

The authors believe that by consistently asking company employees to answer questions, the results are getting better every year, as awareness has been gained to achieve a basic level of cyber hygiene and cyber security. They are also aware of when and what the options are for raising the level and who to turn to if a cyber security incident occurs.

The thesis is written in Estonian and contains 60 pages of text, 5 chapters, 6 figures, 2 tables.

Jooniste loetelu

Tabelite loetelu

Lühendite ja mõistete sõnastik

Backend	Taustsüsteem
B2B	*Business to Business* (äriüksus)
CES	*Cyber Essentials Scheme* (küberjulgeoleku tagamise raamistik)
CPS	*Cyber Physical System* (küber-füüsiline süsteem)
CPTED	*Crime Prevention Through Environmental Design* (riski hindamise kontseptsioon)
CTA	*Call to action* (aktiivne nupp veebilehel, mis kutsub tegutsema)
DP	*Decision Points* (otsustuspunktid)
FAIR	*Factor Analysis of Information Risk* (riskiteguri mõõtmise mudel)
Frontend	Liides UI ja taustsüsteemi vahel
IT	Infotehnoloogia
Modal	*Modal window* (modaalne aken graafiline juhtelement, mis allub rakenduse peaaknale)
MVP	*Minimum Viable Product* (minimaalne töötav toode)
PostqreSQL	*Database management system* (andmebaaside haldussüsteem)
SSO	*Single Sign-on* (ühekordne sisselogimine lahendus kasutaja
TAM	*Technical Account Manager* (tehniline haldur)
UI	*User Interface* (kasutajaliides)
UX	*User experience* (kasutajakogemus)

Sisukord

Sissejuhatus

Autorid õpivad Tallinna Tehnikaülikoolis töökohapõhise õppe raames ja sellest tulenevalt tekkis mõte saavutada õpiväljundina midagi sellist, mis haakuks ka aktuaalsete teemadega tööandja juures ja millest võiks saada tulevikus reaalset kasu igapäevatöös.

2019 aasta alguses otsustas Telia jõulisemalt siseneda IT turvateenuste ärisse. Otsus oli eelkõige tingitud sellest, et igapäevaselt ka ajakirjandusse jõudnud uudised rääkisid järjest rohkem DDOS ja lunaraha rünnetest, mille tagajärjel ettevõtete töö oli häiritud või seiskus sootuks.

Enamus väiksematest juhtumitest aga ei jõuagi kontoriruumidest väljapoole ning see võib tähendada, et avalikkuse tähelepanu alla jõudnud intsidendid on vaid jäämäe veepealne osa. Seda just Eesti kontekstis, kuhu arvatakse, et kõik need ründed ei jõua, kuna Eesti on väike ja tähtsusetu muu maailma mõistes. Kahjuks Eesti ettevõtted alati ei mõista oma andmete väärtust ja levinud on veendumus, et neid pole ju mõtet rünnata.

Lisaks kui vaadata maailma trende (Tabel 1) ja ennustusi, on näha, et IT turvateenuste äri rahaline maht on kasvanud ja kasvab ka lähiaastatel väga suurte hüpetega. [15][19]

Näiteks Gartneri prognoosis 2019 aastal *IT security* valdkonna rahaline mahu kasvuks ligi 9% ja 2020 a lisaks 2,4% . Hüpe toimub eeskätt teenuste arvelt, mis võimaldab kasutada turvalisi lahendusi ka nendel ettevõtetel, kes täna selle jaoks investeeringuid teha ei saa. [15] [19]

Tabel 1. Ülemaailmsed julgeoleku kulutused segmentide kaupa, 2017–2020 (miljonites USA dollarites)

Worldwide Security Spending by Segemnt, 2018-2020 (Millions of U.S.Dollars)				
Market Segment	**2017**	**2018**	**2019**	**2020**
Application Security	2,434	2,742	3,095	3,287
Cloud Securiy	185	304	585	585
Data Security	2,563	3,063	2662	2,852
Identity Access Management	8,823	9,768	9,837	10, 409
Infrastructure Protection	12,583	14,106	16,52	17, 483
Integrated Risk Management	3,949	4,347	4,555	4,731
Network Security Equipment	10,911	12,427	13,387	11, 694
Other Information Security Software	1,832	2,079	2,206	2, 273
Security Services	52, 315	58, 920	61,979	64,27
Consumer Security Software	5,948	6,395	6,254	6,235
Total	**101, 544**	**114, 152**	**120, 934**	**123, 818**
Source: Gartner (June 2020) ja Gartner (August 2018)				

Kõik need maailmatrendid on ka Eestis aktuaalsed. 2020 aasta alguses kinnitas AS Telia Eesti juhatus plaani ning otsustati panustada viide erinevasse kliendi lahenduste kategooriasse:

- **Lõppkasutajate töövahendite kaitse**. Nt viirusetõrje, mobiilide turvalisus, O365 pilveandmete turvalahendus jne.
- **Asutuse perimeetria kaitse**. Nt tulemüüri lahendused.

- **Info ja tegevuste haldamine ning ohtude ennetamine.** Siia kuuluvad muuhulgas logide haldamine, andmete turvalisus, iseõppivad (tehisintellekt) lahendused jne.
- **Kliendipõhised IT turvalisuse lahendused.** Nt ettevõtete poolt endale soetatavatel seadmetel baseeruvad lahendused – eeskätt suurematele ettevõtetele ja riigiasutustele.
- **Konsultatsioon.** Klientide nõustamine, turvalahenduste kaardistamine jne.

2021 aasta alguses uuendati kogu AS Telia Eesti strateegiat ning lepiti kokku, uuesti peamised strateegilised fookused, millest üks, millele keskendutakse on jätkuvalt ka IT ja Küberturbe teenused. Eesmärk on äriline kasv läbi lojaalsete klientide ning ka suurepärase teenuse kvaliteedi kaudu.

Oma tööga soovivad autorid panustada AS Telia Eesti eesmärkide täitmisesse ja anda oluline panus eelpool mainitud tegevustest eelkõige ohtude ennetamisele ning klientide teadlikkuse suurendamisele. Ühtlasi aidata kaasa kogu Eesti ettevõtluse turvalisemale ja efektiivsemale toimimisele.

1 Probleemi sõnastus ja põhjendus

Autorid töötavad Eesti telekommunikatsiooni ettevõttes AS Telia Eesti ja tegelevad igapäevaselt suurklientidega ning nende poolt kasutatavate infotehnoloogiliste lahendustega, seega puutuvad pidevalt kokku ka infoturbe küsimustega. Teadlikkus selles vallas on turul väga erinev aga tänapäeval ei ole praktiliselt ühtegi ettevõtet, kes ei puutuks kokku IT-ga ja see muudab nad seeläbi kohe ka potentsiaalseks ründeobjektiks küberkurjategijatele.

Kahjuks ei kasva inimeste teadlikkus nendes teemades nii kiiresti kui lisandub maailmas uusi keerulisemaid probleeme, mis seotud IT valdkonnaga.

Probleemiks on see, et Telial ja ka üldiselt Eesti turul ei ole kliendi jaoks head vahendit, millega nende olukorda IT turvalisuse osas hinnata ja puudustele viidata ja teadlikkust tõsta.

Tööriistad, mida maailmas pakutakse, on keerulised ja eeldavad tehnilist IT teadmust. Lisaks tundide viisi tööd süvenemaks kasutusjuhenditesse ja üldiselt keskendutakse ainult ühele kindlale osale nt. Cybexer, kelle välja töötatud küsitluse täitmiseks on vaja põhjalikku tehnilist teadmist IT osas. Valdavalt pole olemasolevatel lahendustel ka Eesti keele tuge.

Probleemi lahendamiseks käisid autorid läbi erinevaid ideid, kuidas seda paremini ellu viia. Näiteks oli mõte teha nn. animeeritud infoturbe teemaline koolitus ettevõtte töötajatele. Lähemalt teemat uurides leidsid autorid, et selline on juba olemas ja uue sarnase leiutamine tundus mõttetu.

Seejärel otsustasid autorid läbi viia vajaduse täpsustamiseks küsitluse esialgu Telia töötajate hulgas, kes igapäevaselt tegutsevad IT juhtimises ja on tihedalt seotud IT alaste küsimustega. Telias on sellisteks töötajateks tehnilised haldurid (TAM) suuremate klientide juures. Osalusprotsent oli 60%, st 10-st 6 vastas küsitlusele.

Küsimused esitati neile peamiselt efektiivsuse mõttes koos valikvastustega ja olid järgmised:

1. Millised valdkonna teemad on ettevõtte /IT juhil kõige tihedamalt laual ?
2. Millist infot ootavad nad Telia käest oma turvariskide osas?
3. Kui tihti kliendid ise alustavad IT turvalisuse teemadel juttu? Ja kui avatud on nad nendel teemadel suhtlema ja infot avaldama?
4. Kui teadlikud on ettevõtte/IT juht enda ettevõtte IT turvalisusega seotud võimalikest riskidest?
5. Kas olete kokku puutunud turul olevate nn. turvahügieeni küsimustikega? (nt. https://cybexer.com/#hygiene). Kui oled, siis millised (nimeta)?
6. Kas kliendid ka kasutavad neid?
7. Kui oled ise kasutanud või nendega tutvunud, siis kas sinu arvates, annaks selliste küsimuste laialdasem kasutamine väärtust juurde?

Küsimustikule vastanute vastustest võis välja lugeda, et AS Telia Eesti suunas oodatakse ülevaadet võimalikest riskidest ja ohtudest ning ka meetodeid kuidas nendega hakkama saada ja kuidas neid ennetada.

Sellest tulenevalt leidsid autorid, et liiguvad õiges suunas ja otsustati see ka enda ühise magistritöö sisuks valida. Kaaluti ka laiendada vastanute arvu levitades küsitlust IT müügijuhtide hulgas, aga esialgse vajadusest ülevaate saamiseks piisas ka esialgsest väiksemast valimist.

Septembris 2019 viidi Telias koos Kantar Emoriga läbi uuring „Infotehnoloogia kasutamine ja tulevikuplaanid Eesti ettevõtetes“

Uuringus paluti küsimustele vastata isikul, kes on vastutav IT valdkonna eest. Küsitleti kokku 400 ettevõtet, kus oli vähemalt 5+ töötajat. Küsitlus viidi läbi telefoni intervjuu käigus.

Uuring koosnes erinevatest osadest, kus uuringu kuuendas osas uuriti just IT turvalisuse poolt. Vastustest leiti, et IT turvalisus on väga olulisel kohal ja ligi 2/3 vastanutest hindas oma IT süsteemide olekut heaks või isegi väga heaks, samas IT teadlikkuse osas nii

kõrgeid hinnanguid ei antud, pigem hinnati seda väga madala hindega. Vaid 12% vastanutest arvas, et nende IT teadlikkus on väga hea.[11]

Suur osa ettevõtetest on andmelekke kartuses ja on kindlad, et see kahjustaks nende äri oluliselt. Ca 5% ettevõtetest on aga kindlad, et andmelekke korral suudavad oma äriga ikka edasi minna. 6% ettevõtetest juba on vähesel või suurel määral kokku puutunud andmelekkega. [11]

Probleemide korral on ettevõtted enamuses veendunud, et pöörduksid probleemide korral esmajoones oma IT partneri poole, kuna peavad vastutavaks IT teemade puhul just neid. Nii toimivad need ettevõtted, kellel on partner olemas. Need aga kellele IT partner puudub ei oska kohe nimetada ettevõtet, kelle poole muredega pöörduda tuleks.[11]

IT alaste probleemide puhul otsitakse infot internetist, teenusepakkujatelt, koostööpartneritelt ning ka sõpradelt ja tuttavatelt.[11]

Eriolukord riigis 2020 aasta alguses seoses COVID19-ga tõi välja palju turvanõrkusi, mida enne ei oldud teadvustatud või oluliseks peetud. Kõige levinumad olid õngitsusründed, millega püüti kätte saada kasutajanimed ja salasõnad: kasutajad suunati lehekülgedele, mis olid väga sarnased ettevõtte õigete lehtedega. Oli ka teisi võimalusi, nt saadeti manusega kiri, inimene avas manuse, kus oli peidetud ka kahjurvara.[9]

Kriisiolukord andis ka võimaluse selle olukorra ärakasutamiseks pahalaste poolt, näiteks oli hulgaliselt õngitsusrünnakud, mis kasutasid ära COVID19 pandeemiat peibutamaks heausklikke kasutajaid oma andmeid loovutama. [9]

Teiseks viisiks olid lunavara (ransomware) rünnakud. Seal kasutati ära lekkinud kasutajanimesid või paroole ja võeti üle inimeste kontosid, et pääseda seeläbi juurde ettevõtte infosüsteemidele. 2019 aastal oli Eestis mitu tõsisemat lunavara rünnakut, mille tulemusel oli nende ettevõtete töö mitmeid päevi häiritud, kuna igapäevaseid tegevusi ei saanud teha tavapärasel viisil ja kiirusega. [9]

Kuhugi ei kadunud ka nn. DDoS ründed, kus serveritesse suunati väikseid päringuid ja sellega seoses koormati see üle. Tagajärjeks muutus teenus klientide jaoks aeglaseks või

üldse kättesaamatuks. Eelkõige täheldati DDOS rünnete kasvu Hiina suunas, mille peamiseks põhjuseks võis olla maailmas valitsevad hoiakud pandeemia COVID19 päritolust tingituna. [9]

Tsiteerides AS Telia Eesti küberturbe valdkonna juhti Aigar Käis´i: “Kui ettevõtte serverid on halvasti kaitstud võib ettevõte kokku puutuda tõsiste probleemidega. Rahvusvaheline turvalisuse konfiguratsiooni monitooringu Hardenize andmetel on Eestis vaid 41% veebi- ja e-posti serveritest hästi konfigureeritud, ülejäänud 59% ei ole piisavalt turvalised. Üheks põhjuseks võib olla ebapiisav serverite hooldus. Kui server on aastaid tagasi üles pandud, kuid uuendusi ja turvapaikasid ei ole hiljem installeeritud, ei ole need rünnakute eest enam piisavalt kaitstud. Kahjurvara areneb väga kiiresti, seepärast on oluline kaitselahendusi pidevalt uuendada ja parandada” [9]

Kahjurvara areneb väga kiiresti, sellepärast on oluline kaitse lahendusi pidevalt uuendada ja parandada. Selleks, et tagada maksimaalne võimalik kaitse, tuleb mõelda nii võrgu turvalisusele kui ka tegeleda inimeste küberhügieeni ja teadlikkuse tõstmisega. [9]

2019 aastal korraldasid ka Samsung koostöös küberjulgeoleku ettevõtte CybExer Technologies uuringufirmaga Norstat Eesti uuringu inimeste küberturvalisuse teadlikkuse ja vajalikkuse kohta. Sellest selgus kahjuks, et huvi on väga madal, eelkõige seetõttu, et sellest ei saada aru või on liiga keeruline. [12]

Läbiviidud uuringu kohaselt vastas 42 protsenti Eesti inimestest, et on teatud hetkel ise otsinud informatsiooni küberturvalisuse teemadel. Samas kõigest 20 protsenti nentis, et on viimase kuue kuu jooksul mõnda teemakohast artiklit näinud, videot vaadanud või raadiosaadet kuulanud. Kahjuks ligi 50 protsenti vastajatest, ei ole digiturvalisuse teemadega aga üldse kokku puutunud. Oli ka neid, kes üldse ei mäletanud, et oleks viimase kuue kuu jooksul antud teemadega tegelenud. [12]

Põhjused, miks eirati või jäeti kasutusele võtmata olid: ligi 37 protsenti ei mõistnud, mis kasu sellest saadakse ja 34 protsenti ei saanud aru, mida nad täpselt ikkagi tegema peaksid. Mainiti ära ka ajapuudust ja sellega kaasnevaid väljaminekuid. [12]

Küsitluse tulemusel leiti, et vajalik on rohkem panustada teavitustöösse, et mõitsa paremini, miks küberturvalisusi ja küberhügieeni on nii olulisust. Kuna ühiskond liigub järjest rohkem digitaalse elu poole, siis kindlasti ka küberturvalisus pole vähetähtis teema, millega ainult IT-mehed ja tehnikud kokku puutuvad, eriti Eestis, kus virtuaalmaailm on kõigega niivõrd läbi põimitud. [12]

COVID19 pandeemia on jätkunud ka 2020 ja 2021 aastal, inimesed veedavad enamuse tööajast ekraani taga kodukontoris mitte ettevõtte ruumides. Sellega seoses on tekkinud uued mured ja juba eelmisel aastal aktuaalsed küberturbe teemad on veel olulisemaks muutunud. Sellega seoses on tõusnud tähtsus inimeste teadlikuse tõstmises, et kaitstud oleks nii ettevõtte kui ka isiklikud andmed ja varad.

2020 aastal oli küberrünnete kasvu trend ca 600% ja see on siiani tõusuteel. Enam ei ole seotud ainult IT inimesed vaid kogu ettevõtte juhtkond. Kõik püüavad leida lahendusi, kuidas kaitsta kodus töötavaid töötajaid, nende seadmeid võimalike ohtude eest kübermaailmas. [16]

Piirid, mis enne eristasid töö ja eraelu jäävad järjest nõrgemaks, kuna nüüd kasutatakse ka kaugtöö tegemiseks oma isiklikke internetiühendusi. Üldiselt ei ole eraisikud oma ruutereid turvauuendustega paiganud, paroole kasutatakse korduvalt ja autentimine ei ole muudetud ka kaheastmeliseks. [16]

Need kõik tingivad ettevõtete jaoks uued nõuded ja tingimused. Vajalik on määrata küberturvalisuse baastase. Valdkonniti on see erinev, aga üldiselt sisaldavad järgmiseid tegevusi: töötajate koolitamine, töötavad ja arusaadavad reeglid kodukontoris töö tegemisel, turvalised töövahendid, kontroll ettevõtte andmete üle, tarkvara regulaarsed uuendused ja ka oma ala ekspertide kaasamine igapäevatöö turvalisemaks muutmisel. [16]

1.1 Töö eesmärgi sõnastus ja põhjendus

Magistritöö eesmärk on ära kaardistada ettevõtete turbehalduse tõhusus ja riskikohad. Väljundiks loome küberturvalisuse tööriista, mis on kõigile arusaadavas sõnastuses, olgu vastaja IT juht, reatöötaja või firma juht. Tulemuseks soovivad autorid saada ülevaate ka hetkeolukorrast ja tuua välja kriitilisemad teemad, millega peaks jätkuvalt tegelema.

Plaanis järgnevad tegevused:

- Oluliste teemade järjestus, küsimuste välja valimine

Telial on varasemast välja töötatud küsimustik, mida on kasutatud põhjalike turvakaardistuse intervjuude läbiviimisel. Küsimusi selles on umbes 100, need on väga pikad ja mitte igaühele lihtsasti arusaadavas keeles. Autorid tutvusid nende küsimustega, et kaardistada olulisemad teemavaldkonnad. Kuna antud küsimustik on pikk ja keeruline, kasutav pigem abivahendina siis autorite eesmärk oli filtreerida sealt välja olulisim, teha valitud osa lihtsamaks ja arusaadavamaks.

- Töötada välja kõigile arusaadav küsimustik

Autorid pidasid oluliseks luua sobilikud ja mõistetavad küsimused. Küsimused jagatakse 5 alamkategooriasse, mis annavad vastused erinevat tüüpi riskide osas .

- Veebipõhise tööriista loomine

Tehnilise poole pealt panustasid autorid esialgselt võimalusele kasutada Tallinna Tehnikaülikooli bakalaureuseõppe tudengite tehnilisi teadmisi. 2020 õppeaasta alguses ei õnnestunud koolist sellest huvitatud tudengeid kahjuks leida. 2020 novembris leidsid autorid endile abilise koodi kirjutamiseks Telia praktikandi programmi raames. Autorid palusid lahendad prooviülesande ja valisid välja ühe praktikandi.

- Kogutud materjali kasutamine Telia eesmärkide täitmisel ja klientidele parema turvataseme loomisel.

Valminud tööriist ja selle abil kogutud info saab olema oluline abivahend Telia siseste eesmärkide täitmisel klienditeeninduslikele üksustele ning sisendiks olemasolevate teenuste/toodete analüüsimisel aga ka uute teenuste arendamisel.

Autorid püstitavad magistritöö raames hüpoteesi, et nende poolt loodud küsimustiku küsimustele vastaja saab ülevaate teda ohustavatest võimalikest küberturbe riskidest ja hakkab teadlikumalt tegelema vastustest välja tulnud puudustega ning pakutud soovitustega, et saavutada vajalik küberturbe baastase.
Baastasemeks loetakse AS Telia Eestis üheksa valdkonnaga teadlikku tegelemist ja võimalike ohtude teadvustamist (Joonis 1) [20]. Sellega aitavad autorid ka kaasa kogu Eesti ettevõtluse turvalisemaks ja efektiivsemaks toimimiseks.

Joonis 1. AS Telia Eesti küberturvalisuse baastaseme visuaal

1.2 Metoodika

Autorid on antud töö metoodikaks valinud disainiteaduse (*Design Science*). Seda saab kasutada siis kui teema on seotud uute IT tehiste (programm, metoodika, mustrite keel jne) loomisega. See metoodika on keskendunud eelkõige probleemidele lahenduste leidmiseks. [17]

Käesoleva magistritöö eesmärk on ka luua uus tööriist, millega saab määrata küberhügieeni taset ettevõtetes ja selle läbi aidata kaasa küberturbe teadlikkuse tõstmisele ning võimalike ohtude vältimisele. Autorid leiavad, et antud töö juures on ka teine metoodika kasutusel, milleks on tegevusuuringu sümbioos disainiteadusega *(Action Design Research)* (Joonis 2), seda just seetõttu, kuna antud rakendust lisaks disainimisele soovitakse kohe ka rakendada ellu AS Telia Eesti´s küberturbe teemadega seoses uuel kodulehel ja lisarakendusena ka iseteeninduses IT portaalis. Ühtlasi näitab see ka seda, et antud rakendus on rakendatav ja praktiline. [18]

Disainiteadus metoodika puhul püstitatakse kõigepealt esialgne uurimisküsimus. Autorite töös on selleks, kuidas tõsta ettevõtetes teadlikkust infotehnoloogiliste lahenduste kasutamisega kaasnevate võimalike ohtude osas.[17]

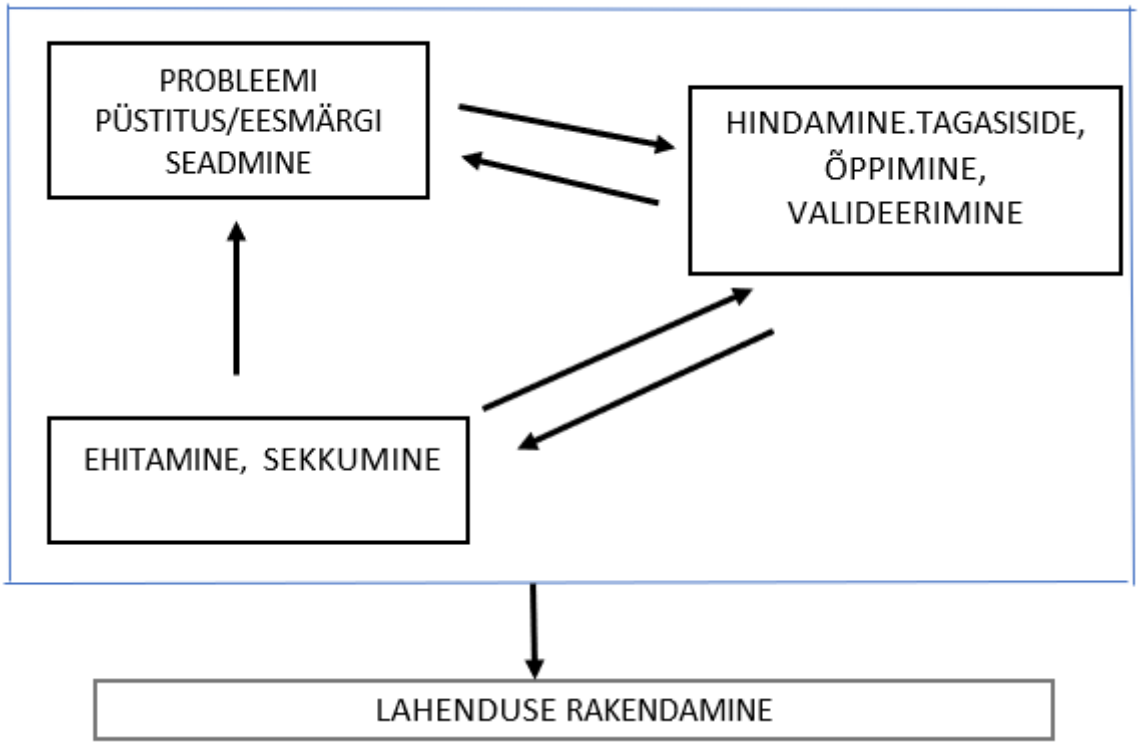
Järgmisena uuritakse olemasolevat olukorda nii hetkeseisus olemasolevate rakenduste näol kui ka teaduskirjandust veendumaks, et sellist tööriista, mida soovitakse luua, tõepoolest ei ole, kuid selle loomiseks on vajadus olemas. [17]

Töö alguses viisid autorid läbi küsitluse isikute hulgas, kes Telias igapäevaselt puutuvad kokku nende teemadega. Valiti küsitluse saajateks Telia suurklientide lahendusi toetavad tehnilised haldurid (TAM). Samuti otsiti internetist sarnaseid vahendeid ja tuvastastati, et neid eksisteerib mitmeid aga mitte selliseid, mis käsitleksid teemat laialdasemalt ja oleks kergemini aru saadavad erinevates rollides olevatele ettevõtte töötajatele. Samas olukorras, kus selline teadlikkus on ülioluline ja üks baasaluseid küberturbehügieenile, on loodaval tööriistal kindlasti vajadus olemas.

Edasi analüüsisid autorid olemasolevaid sarnaseid küsitlusi, sh AS Telia Eestis kasutusel olev ca 100 küsimusega küsitlus, mida kasutatakse ettevõtetes intervjuude käigus, et kaardistada ettevõtte IT ja küberteadlikkuse seisukorda.

Eelpool nimetatud tegevustega saadi parem ülevaade, mida on selles valdkonnas juba tehtud ning mida ja kuidas saab teha veel paremini. See kõik osutus väga väärtuslikuks sisendiks uue tööriista loomisel ja püstitatud probleemi lahendamisel.

Lõpuks on soov uut tööriista võimaldada kasutada kõigil, kellel sellekohane huvi olemas. Eelkõige ootame vastama just antud töö sihtrühma, et anda tagasiside ettevõtte töötajale tema enda infoturbe alastest teadmistest aga ka üldhinnangu ettevõtte olukorrale.



Joonis 2. Tegevusuuringu sümbioos disainiteadusega (autorite joonis allikate alusel)

1.3 Ettevõte AS Telia Eesti

1.3.1 Taust ja andmed

AS Telia Eesti emafirma Telia Company on üks Euroopa suuremaid telekommunikatsioonieттevõtteid, mis tegutseb klientide jaoks aina enam ühtse ettevõttena. Kõik see loob võimalused kliendil kasu saada grupi ettevõtete kliendiks olemisest ka välismaal, teiste grupi ettevõtete juures. Ettevõte omab terviklikku strateegiat kogu grupi ulatuses, kuid erinevates riikides tegutsevad grupi ettevõtted vastavalt antud turu ja klientide vajadustele.

AS Telia Eesti missiooniks on panustada ühiskonna arengusse, et Eesti oleks parem paik nii elamiseks kui töötamiseks. Ettevõtet innustab võimalus muuta tehnoloogia abil inimeste elu lihtsamaks ja mugavamaks. Neil on tehnoloogiline kompetents, klienditundmine ja investeerimisvõimekus, et viia ellu visioon uue põlvkonna telkost.[21]

Juhtivast tehnoloogiast inspireerituna on ettevõtte eesmärk arendada maailmaklassi tooteid ja teenuseid, mis aitavad tuua maailma lähemale sellele, mis on Telia klientidele ja ühiskonnale tõeliselt oluline. Sarnaselt oma tehnoloogiaga on ka ettevõte pidevas arengus.[21]

AS Telia Eesti prioriteedid on toodete ja teenuste lihtsustamine, analüütilise võimekuse ja täpsuse kasv, digitaliseerimine, hübriidpilv, tark linn ja 5G. Soov olla liider nii kvaliteedis kui innovatsioonis. Kõige aluseks on kvaliteet ja usaldus. AS Telia Eesti on ka Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu liige [21].

Viimase aastaga on sagenenud ca 90% küberturbe ründed. AS Telia Eesti andmetel on küberturvalisus üks esmaprioriteete, mille arendamisse investeerib ettevõte pidevalt. Olemasolevad turvalahendused võimaldavad blokeerida suurema osa rämpspostitustest ja kahjurvara tunnustega e-kirjadest, siiski jõuab osa neist saajateni. Sellega seoses on väga oluline kasvatada pidevalt inimeste teadlikkust, et võimalikke ohte varakult ära tunda ning õppida neid vältima. [9]

Valmiv tööriist on eelkõige suunatud ettevõtetele, eelkõige väike- ja keskmise suurusega Telia mõistes, ca 3000. Jätame välja suurettevõtted, riigiettevõtted ja rahvusvahelised organisatsioonid, kuna nendes on üldjuhul olemas pikaajalised strateegiad, kuidas ohtusid vältida. Rahvusvahelistes organisatsioonides on juba laialt kasutusele võetud ka erinevad pakutavad tööriistad ja kuna rakendatakse neid korporatiivsel tasandil, siis üldjuhul on kaasatud ka Eesti filiaalid ja ettevõtted.

Probleemseks peame me just autorite poolt valitud sihtrühma, kuna seal ei osata hinnata riski suurust, puudub ka piisav teadlikkus kuidas riske vältida ning peetakse väga ebatõenäoliseks ohvriks langemist. Seda teadmist kinnitab ka eelpool mainitud Telia läbiviidud uuring. [11]

1.3.2 Üldine arendusprotsess Telias

Arendusprotsess AS Telia Eesti´s algab teenuse visiooni loomisega, mille osaks on mitteformaalne ideede filtreerimine koos valdkonna eest vastutajatega ettevõttes, selgitamaks välja millise ideega tahetakse edasi liikuda. Visiooni kinnitamiseks peab olema selge, kas teenus on klientide jaoks vajalik ja kas ta annab väärtust ka ettevõttele, vastab kokkulepitud nõuetele ja strateegiale. Seejärel teenus disainitakse ja hakatakse planeerima teenuse arendamist.[20]

Järgneb teenuse arendamine ja selle kliendile kasutusse andmine. Olulise osana järgneb hilisem tagasiside kogumine/mõõdikute jälgimine.[20]

Vaja on läbi kaaluda riskid ja loodava kasumlikkus ettevõttele ehk vaja on riskide haldamise plaani ja tasuvusarvutust. Projekti avamisel defineeritakse selle eesmärgid, skoop, ajakava ja eelarve, Oluline on omada riskide juhtimise plaani, kaasa arvatud GDPR teemad. Lisaks määratakse projekti kaasatud inimesed ja nende rollid projektis. Kirjeldada üldisel tasemel läbimõeldud testimise plaani ja lahenduse arhitektuurilist kontseptsiooni. [20]

Joonis 3. AS Telia Eesti arendusprotsessi etapid

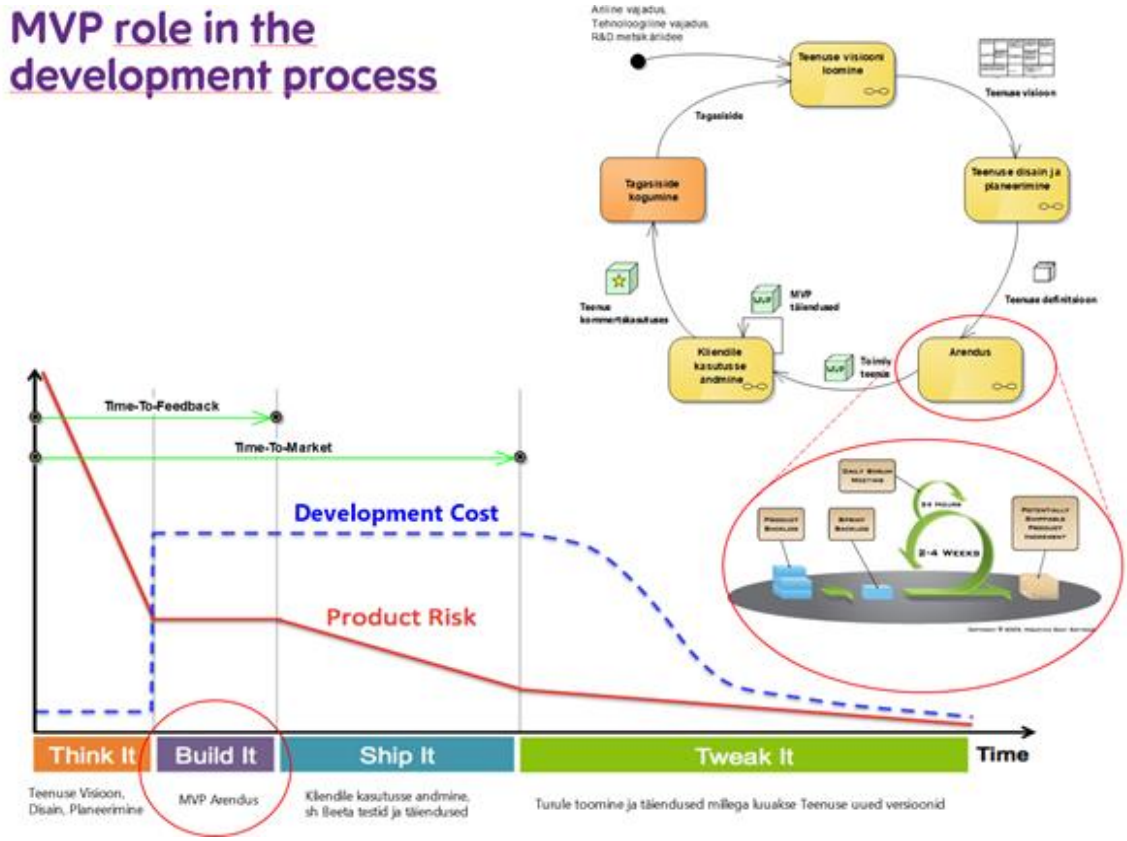
Projektide arendusprotsess koosneb etappidest ja nende vahel olevatest otsustuspunktidest (Decision Points DP). (Joonis 3)[20]

Otsustuspunktid on järgmised:

- DP0 Visiooni kinnitamine (otsus investeerida);
- DP2 Projekti avamine (otsus investeerida);
- DP5 Kliendikasutusse andmine (beetasse või kommertsi);
- DP6 Projekti lõpetamine;
- EP (Evaluation Point) Äriliste tulemuste hindamine.

Telia arendusprotsess on tuletatud *Lean Startup* metodoloogiast, mis keskendub selle osaks olevale minimaalselt elujõulise toote (MVP) kontseptsioonile. Peamiseks eeliseks on see, et on võimalik teada saada klientide huvi toote vastu ilma toodet täielikult välja arendamata. Selline lähenemine võimaldab vältida ülemäära suuri kulutusi ja jõupingutusi tootele, mida turg ei oota.

Kliendikasutusse antakse teenus siis, kui kokkulepitud minimaalne kliendikasutuseks sobiv lahendus (MVP) on valmis.(Joonis 4), mis on koostatud tänase Telia üldise arendusprotsessi joonise baasil, annab ülevaate otsustuspunktidest ja etappidest.[20]



Joonis 4. MVP roll arendusprotsess AS Telia Eesti näitel

Telias kasutatakse projektijuhtimiseks *Jira* tarkvara (Tabel 2). DP edukal kaitsmisel Valdkonna juhtrühmas paneb juhtrühma volitatud esindaja (reeglina valdkonna arendusjuht) selle kohta märkuse jiras projekti comment-na. [20]

Tabel 2. JIRAs kirjeldatud projektide etapid

Arendusprotsessi etapp	***JIRA* project status**	**Etapi sisu ja lõpukriteeriumid**
Arendus	*DEVELOPMENT*	Toimub teenuse arendus. Etapp lõppeb, kui on täidetud DP5 nõuded
Kliendile kasutusse andmine	*LIVE-BETA*	Toimub teenuse täiendamine beetast/kommertsist kogutava tagasiside põhjal. Etapp lõppeb, kui on täidetud DP6 nõuded.
Lõpetatud	*CLOSED*	Töö antud ideega/visiooniga on lõppenud, kogutud tagasiside / EP õppetunnid saab arvesse võtta uute teenuse ideede / visioonide loomisel.
Teenuse disain ja planeerimine	*DEV PLANNING*	Toimub teenuse disaini ja teostusplaani loomine ning kaitsmine IT projektijuhi vedamisel. Etapp lõppeb, kui antakse vastused DP2 küsimustele.
Teenuse visiooni loomine	*VISIONING*	Toimub teenuse visiooni loomine, valideerimine ja kaitsmine teenuse ärilise omaniku vedamisel. Etapp lõppeb, kui antakse vastused DP0 küsimustele.
Uus Idee	*IDEA*	Toimub idee paigutamine valdkonna arenguplaani (3a) ja arendusplaani (12k) - sh esmane prioriseerimine. Edasist idee täpsustamist veel ei tehta.
(3a ja 1a planeerimine)		Etapp lõppeb, kui valdkond alustab Idee täpsustamiseks visiooni loomist (DP0 küsimuste vastamist).

1.3.3 Töö autorite tutvustus ja rollid

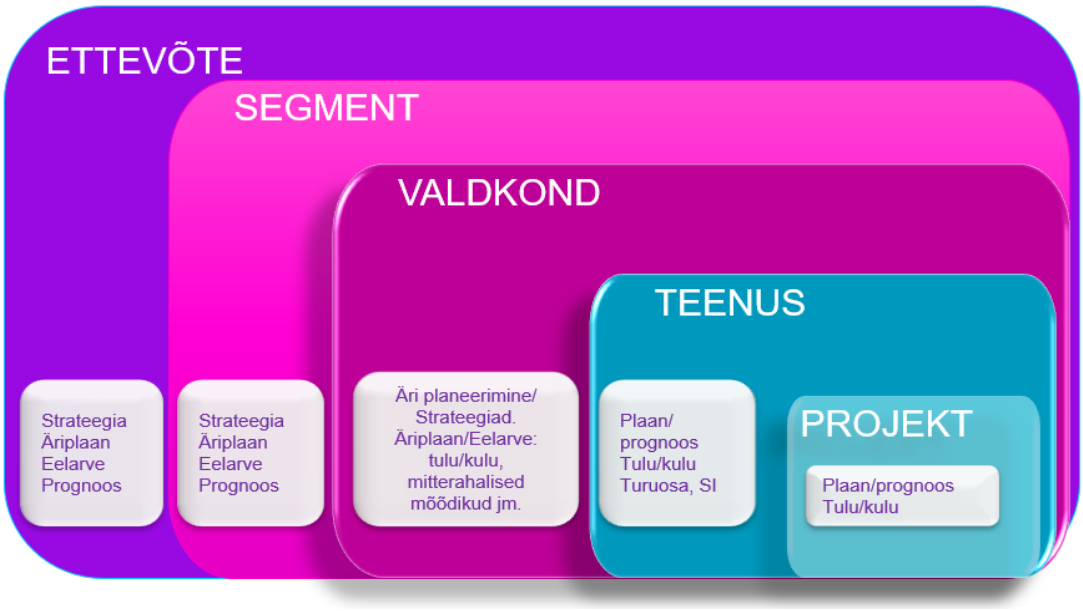
Töö autorid on üle 10 aasta töötanud Telia suurkliendi osakonnas kliendihalduritena. Oma igapäevatöös puutuvad autorid aina rohkem kokku probleemide ja küsimustega, mis on seotud klientide küberturvalisusega. See sai ka üheks ajendiks antud töö teema valikule.

Töötades klientidega tajuvad autorid, et teadmised antud valdkonnast on väga erinevad ja ka hinnangud mida kliendid annavad iseendale on igalühel oma arusaamiste järgi ja ühtselt mõõtmiseks puudub sobilik vahend.

Alustasime oma tööd analüüsides turuolukorda, tutvusime pakutavate lahendustega ning viisime läbi küsitluse, kas sellise tööriista jaoks on vajadus olemas. Edasi jagasime rollid vastavalt kokkulepitud tegevuskavale.

Pireti vastutusalaks jäi projektimeeskonna kokkukutsumine/leidmine ja nende töö koordineerimine. Erki tegeles küsimustiku sisulise poole ja andmete salvestamise võimaluste ning analüüsimise võimaluste välja selgitamisega.

Oma tegevustes lähtusid autorid AS Telia Eestis kehtivatest protsessidest ja ärijuhtimise mudelist (Joonis 5)[20]



Joonis 5. AS Telia Eesti ärijuhtimise mudel

1.4 Ülevaade tööst

Magistritöö koosneb viiest peatükist. Selleks, püstitatud eesmärgid ja soovitud tulemused saavutada on töö üles ehitatud vastavalt disainiteaduse etappidele. Lisaks uurisid autorid ka võimalusi, kuidas muuta valitud meetod valideeritavaks.

Töö esimene peatükk on sissejuhatuseks autorite tööle, kus nad annavad ülevaate töö taustast, sh. millised on magistritöö eesmärgid ja ülesanded, probleemi aktuaalsusest, metoodikatest mida kasutati. Lisaks ka ülevaade ettevõttest, kus loodav tööriist kasutusele võetakse ja ka autoritest taust.

Töö teises peatükis kirjeldatakse olemasolevaid lahendusi, uuritakse teadusartikleid ja tehakse kokkuvõtteid.

Kolmandas peatükis kirjeldatakse küsimustiku väljatöötamise protsessi, millised olid algsed probleemkohad, milliseid takistusi läbiti ja kuidas valmis lõplik valik ning tööriist ise.

Neljandas peatükis autorid kontrollivad esitatud hüpoteesi ja esitavad selleks valideerimise plaani.

Viiendas peatükis analüüsitakse, mis sai autorite poolt tehtud ja millised võimalused ja plaanid on edasi antud teemaga minemiseks. Milliseid ettepanekuid ja soovitusi tehakse Telias selles valdkonnas vastutavatele isikutele. Ühtlasi tehakse ka kokkuvõte magistritööst.

2 Kasutusel olevad tööriistad ja analüüsi meetodid

Erinevate artiklite põhjal võib öelda, et täpselt samasugust lahendust tehtud ei ole. Ettevõtted kasutavad turul olevaid tööriistu peamiselt erinevate riskide maandamiseks. Pigem püütakse olemasolevate protsesside käigus vältida/minimeerida tekkivaid riske ja mõelda sellele kuidas neid paremini prognoosida. Samas väidetakse, et pidevalt muutuva väliskeskkonna tõttu ei suuda juhid siiski suure hulga andmete seest reaalset ohtu ülesse leida.

Katsetatakse uusi võimalusi, nt uus riskihindamise meetod võib dünaamiliselt keskenduda CPS globaalsetele töötingimustele ja arvutada riski reaalajas. Selleks, et see aitaks kasutajatel reageerida riskile õigeaegselt, siis aidata neil valida ja rakendada ulatuslikke turvameetmeid, et vältida ohtusid ja kaotusi, mis võivad juhtuda

Olemasolevate tööriistade koostamisel on kasutatud erinevaid standardeid (nt. ISO / IEC 27001: 2013) ja nende alusel tehtud analüüse. Paraku on need väga keerulised tavainimesele läbitöötamiseks, vastamiseks ja ka väga ajamahukad.

Proovitakse läheneda asjale teiselt poolt, nimelt uue võimalusena analüüsitakse konkreetseid küberkuritegevuste tagamaid ja tuvastatatakse viisid, kuidas küberkuritegevuses kasutatavad maailmad ja küberiseerimis protsessi võimalikud tõkked küberkuritegevuses ja -tehnikas edukamaks saavad.

Järjest rohkem pööratakse tähelepanu küberhügieenile. On uuritud erinevaid olukordi ja tuuakse välja, et kui suurettevõtted tegelevad küberturbe eest muretsemisega siis väikesed ja keskmised pühendavad sellele väga vähe aega. Erinevate uuringute järelduste põhjal, on juhitud tähelepanu sellele, et väikeettevõtjad seisavad üldotstarbeliste turvastandardite (nt ISO 27001) kohaldamisel silmitsi paljude takistustega, sealhulgas kvalifitseeritud ressursside nappus, standardi rakendamiseks vajalik aeg, standardi keerukus, sertifitseerimisprotsessi maksumus ja standardi kohaldamise eeliste selge kvantifitseerimine.[14]

Uuematest lahendustest on ettevõtetes kasutusele võetud kasutajatele teadlikkuse tõstmiseks animeeritud kiirkursused, veebiseminarid ja/või virtuaalsed loengud/õpped. Läbinutel palutakse sooritada ka test, kus animeeritud multifilmi või video vaatamisel luuakse elulisi situatsioone, kus töötaja peaks tajuma riski, kas endale isiklikult või ettevõttele. Neid koolitusi viiakse läbi teatud regulaarsusega, et oma töötajatele tuletada meelde, mis on sellel hetkel oluline ja kuidas jätkuvalt käituda endale ja ettevõttele turvaliselt.

Kuna kasutajat loetakse jätkuvalt infoturbe ahela nõrgimaks lüliks siis turvateadlikkuse järjepidev parendamine ning rünnete läbimängimine on olulised märksõnad võimalike õngitsusrünnete ja manipuleerimisrünnete vastu võitlemiseks. [22].

2.1 *State of the Art* kirjanduse ülevaade

2.1.1 Designing a Evaluation Tool for IT Security Solution Implementation for IT Enterprises

Artiklis kirjeldatakse tööriista, millega on võimalik reageerida riskile õigeaegselt ja ka seda, kuidas riski muutuste kõverat saab kasutada tuleviku riski prognoosimiseks. Antud tööriist on mõeldud kuni 50 töötajaga ettevõtetele. Läti näitel on neid lausa 98,8%. (2014 a andmete järgi). [2]

Uuring sisaldab ISO / IEC 27001: 2013 standardi ja teiste standardite ja allikate täielikku analüüsi, et saavutada nõutav teadmiste baas, et õigesti hinnata praeguseid küberohtusid ja nende lahendusi. Selleks, et saavutada nii täpset küberjulgeoleku rakendamise hindamisvahendit, on vaja saada põhjalikke teadmisi küberjulgeoleku ohtudest, kontrollidest ja meetodid nende ohtude käsitlemiseks ja ligikaudne aeg nende kontrollide rakendamiseks erinevate ettevõtte tüüpide ja suuruste jaoks. [2]

Kirjeldatud tööriista väljatöötamine ja kasutamine koosneb kolmest etapist: töömahu andmebaasi loomine, sisenemise andmed sisend- või katsefaasi ja tulemuste väljundfaasi. [2]
Aegade hindamine infotehnoloogias ja muus valdkonnas on äärmiselt häiriv ülesanne, kuna töökoormus võib ootamatult mitmekordistuda. Sellise stsenaariumi võimalikkuse

minimeerimiseks ja täpsemaks ajaplaneerimiseks on kohustuslik kasutada kõrgekvaliteedilist ennustusmeetodit. Selleks kasutati antud tööriista jaoks *PRAGMATIC Security* meetodit.[2]

Uuring viidi läbi teadlikkuse tõstmiseks küberjulgeoleku kasvavate riskide osas ning tutvustamaks seda, kuidas piiratud ressurssidega saab ettevõte konkureerida globaalsel ja kohalikul turul. See uurimistöö on aluseks tulevastele uuringutele ja loodud tööriistale, mis annab ülevaate IT-turvameetmete rakendamise kuludest ilma üksikasjadeta.[2]

2.1.2. Perspectives on Cyber Science and Technology for Cyberization and Cyber-enabled Worlds

Artiklis tutvustatakse küberkuritegevuse tausta ja protsessi ning selgitatakse küberkuritegevuse teadust ja tehnoloogiat, nägemusi ja väljavaateid uute võimaluste, oluliste küsimuste ja küberkuritegevuse ja -tehnoloogia oluliste väljakutsete kohta. Kirjeldatakse küberkuritegevusega seotud tehnoloogiaid ja sellega tihedalt seotud olemasolevaid uurimisvaldkondi ning nähakse tulevasi uurimissuundi küberfüüsikalise, küberkuritegevuse, küberelu, küberteabe ja küberjulgeoleku osas, mis on küberteaduse ja -tehnoloogia viis põhimõõdet. [3]

Artiklis kirjeldatakse, et maailm, kus me elame, muutub küberiseerumise tõttu pidevalt. Küberkuritegevuse protsessis genereeritakse küberkuritegevuses suur hulk küberühiskondi ja suur hulk asju füüsilistel, sotsiaalsetel ja vaimsetel maailmadel, mis omavad mõningaid uusi omadusi, nagu näiteks konjugeerivad küberkaardid või komponendid, mis eksisteerivad nii küber- kui ka füüsilises maailmas.[3]

Artiklis tutvustatakse ka CyberSciTechi põhimõistet, võimalikke võimalusi, küsimusi ja väljakutseid. Samuti tuuakse välja viis tõekspidamist ja mõõdet.[3]

Kokkuvõtvalt antud artiklis tuvastastati viisid, kuidas küberkuritegevuses kasutatavad maailmad ja küberiseerimisprotsessi võimalikud tõkked küberkuriteaduses ja -tehnikas edukamaks saavad. Samuti märgitakse ära see, et seda ülevaadet tuleks kasutada selleks, et seda võetaks arvesse küberteaduse -ja tehnoloogia uurimisstrateegias. Esile toodi kübermaatilist raamistikku olemasolevate väljakutsete tuvastamiseks ja selgitamiseks,

mida saab kasutada küberkuritegevuse ja tehnoloogia uurimise uute suundade kujundamiseks küberkasutatavate maailmade suunas.[3]

2.1.3. Risk Assessment Method for Cyber Security of Cyber Physical Systems

Artikkel käsitleb küberjulgeoleku olemust ja sellega kaasnevat riski hindamist. Küberjulgeolek on üks tähtsamaid riske kõigi küber-füüsiliste süsteemide (*CPS-cyber physical systems*) puhul. CPS-i küberjulgeoleku ohu hindamiseks koosneb kvantitatiivne hierarhiline hindamismudel ründe tõsidusest, edukuse tõenäosusest ja ründe tagajärgedest, mille abil saab hinnata vastuvõtva tasandi ja süsteemi tasandil käimasoleva ründe põhjustatud riski. Samas väidetakse, et pidevalt muutuva väliskeskkonna tõttu ei suuda juhid siiski leida reaalset ohtu suure hulga andmete seest. Peale selle võivad staatilised hindamismeetodid olla vaid ligikaudsed hinnata teatud aja jooksul riski, kuid ei saa seda hinnata konkreetsetes ajapunktides täpselt.[4]

Artiklis arutatakse üksikasjalikult kolme indeksi definitsioonide ja arvutusmeetodite üle. Lõpuks esitatakse ka riskianalüüsi algoritm, mis kirjeldab rakendamise erinevaid etappe. Arvuline näide näitab, et mudel võib reageerida ründele õigeaegselt ja anda süsteemi turvalisuse riskimuutuse kõvera. Selleks, et see aitaks kasutajatel reageerida riskile õigeaegselt. Leitakse ka et riski muutuse kõverat saab kasutada ka tulevase aja riskide prognoosimiseks. Uus riskihindamise meetod võib dünaamiliselt keskenduda CPS globaalsetele töötingimustele ja arvutada riski reaalajas. Selleks, et see aitaks kasutajatel reageerida riskile õigeaegselt, siis aidata neil valida ja rakendada ulatuslikke turvameetmeid, et vältida ohtusid ja kaotusi, mis võivad juhtuda.[4]

Selles mudelis saab küberrünnete informatsiooni hankida sissetungi avastamise süsteemi või tulemüüri logide abil ning nõrkuste kohta saab teavet haavatavuse skaneerimise või leviku testimise abil.[4]

CPSi riskianalüüsi saab edukalt rakendada esitatud riskihindamise mudelile ja algoritmile, milles võetakse arvesse ründe tõsiduse kolme indeksit, ründe edukuse tõenäosust ja ründe tagajärgi.[4]

2.1.4. Situational Awareness Framework for Cyber Crime Prevention Model in Cyber Physical System

Artiklis kirjutatakse sellest, kuidas järjest rohkem reaalses maailmas kasutatakse IoT, 5G mobiilseid, suuri andmeid ja tehisintellekti. Need tehnoloogiad põhinevad *Cyber Physical Systemis* (CPS) konvergentsil. CPS-tehnoloogia nõuab usaldusväärsuse, reaalajas, ohutuse, autonoomsuse ja turvalisuse tagamiseks põhitehnoloogiaid. CPS on süsteem, mis saab ühendada küberruumi ja füüsilise ruumi omavahel. Küberruumi ründed on tekitanud palju segadust ja kahju reaalses maailmas. Selle vältimiseks mõõdetakse riskitegurit ja kasutades *Factor Analysis of Information Risk* (FAIR) mudelit, mis võib mõõta elementide kaupa olukorrale teadlikkust CPS keskkonnas. FAIR mudel on mudel, mis mõõdab riski riske mõjutavate tegurite kaudu. FAIRi metoodikat pakkus esmakordselt välja Jack A. Jones ja tema ajakirjas tutvustatakse üksikasjalikku metoodikat. See uuring viidi läbi FAIRi analüüsi oma ajakirjas esitatud metoodika ja terminoloogia kaudu. FAIRi metoodika liigitab iga teguri viiest tasemest väga madalast väga kõrgele. Lisaks klassifitseerib FAIR-mudel riski riskianalüüsi sageduse (LEF), ohtude esinemissageduse ja ohu korral kadude suuruse (LM) kaudu.[1]

Artiklis mõõdetakse küberriski ründeid kübertasemel CPS-keskkondade vahel ja võrreldakse pärast CPTEDi rakendamist.[1]

Risk väheneb, rakendades CPTEDi mõõdetud suurele riskile FAIR mudelis. Reaalsete rünnete andmete abil on võimalik vähendada riski väärtust ja kaitsta CPS-i rünnete eest.[1]

Lisaks võivad CPS-i kasutavad ettevõtted rakendada CPTEDi platvormi küberruumile, vähendades CPS-i ründe ohtu. Ja ka masinõppe ja sügava õppimise abil CPS-is saate õppida varasemaid andmeid, et vältida ründeid kõigis valdkondades.[1]

2.1.5 Pragmatic Security: Modelling IT Security Management Responsibilities for SME Archetypes

Autorid esitlevad abstraktset mudelit, mis aitaks arvutada kaudseid kulusid, mis tekivad küberturvalisuse baastasemete sisseviimisel ja turvakontrollide juurutamisel väikestes ja keskmistes ettevõtetes. Ka seda, et neil ei pruugi olla ettevõttesiseseid oskusi ja

tulemuseks on kollektiivne suutlikkus tõhusalt juhtimisseadmeid juhtida tahtmatu andmete lekkimise ja ohtu sattumise korral. [5]

Tuuakse näide Ühendkuningriikide näitel, kus 99% ettevõtetest on just väikesed või keskmise suurusega, töötajaid 250 või vähem, sama seis on ka Euroopa Liidus ja USA-s. Need väikesed ettevõtted kasutavad infotehnoloogiat erinevatel viisidel ja neil võivad puududa IT-turvalisuse haldamiseks vajalikud oskused. Lisaks mängivad antud juhul olulist rolli just IT ettevõtted ja teenuseosutajad; väikeettevõtted võivad kasutada renditud teenuseid ja ruume, mille üle neil puudub kontroll ja piisav järelevalve, tuginedes vastasel juhul koduturule mõeldud turvakontrollile, mitte ettevõttelahendustele. See toob välja siseringi haavatavusele, ning kuidas seda hallata, piirata andmete lekkimist ja ärakasutamist väliste ründajate poolt. Turvakontrollide tõhusaks kasutamiseks väiksemates ettevõtetes peavad need olema kuluefektiivsed ja peavad esitama mõistlikud nõudmised ka töö- ja ajakulule. [5]

Selles artiklis kasutatakse küberjulgeoleku põhikaitse raamistikuna programmi *Cyber Essentials Scheme* (CES). CES on suunatud suurtele ja väikestele organisatsioonidele, määrates kindlaks organisatsioonilised kontrollid põhiliste veebipõhiste küberohtude, eriti andmepüügirünnete ja häkkimisrünnete vastu võitlemiseks. [5]

Teemasid käsitletakse 3 arhetüübi näitel: üksikettevõtted (kuni 1 kasutaja); mikroettevõtted (kuni 9 kasutajat) ja ning väikeettevõtte (kuni 50 kasutajat).[5]

Tulemused viitavad sellele, et kahefaktorilist autentimist, korrektseid juurdepääsuõigusi ja kahjurvara vastaseid juhtelemente saab kombineerida, et pakkuda väiksematele ettevõtetele turvataset, mis minimeerib töötajate kollektiivset koormuset. [5]

2.1.6 Basic Cyber Hygiene: Does It Work?

Artiklis analüüsitakse kui palju ettevõtted tegelevad küberhügieeniga. Autorit on uurinud olukorda ja toovad välja, et kui suurettevõtted tegelevad küberturbe eest muretsemisega siis väikesed ja keskmised pühenduvad sellele väga vähe samas. 2017 aasta andmetel 49% UK ja

61% USA väiksemaid ja keskmisi ettevõtteid kannatavad rünnete all. Artikkel toob välja, et suur osa ettevõtteid on väga vastuvõtlikud ja ohustatud kõigi peamiste netis varitsevate suurte ohtude osas. Ka teenusepakkujad peaksid sellele tulevikus rohkem tähelepanu pöörama, et oma kliente kaitsta [6]

Antud artiklis hinnatakse *Cyber Essentialsi* tõhusust ja leiti, et selle turvakontroll toimib hästi ohtude leevendamiseks. *Cyber Essentialsi* turbekontrolli tegevused võib kokku võtta järgmiselt

- Tulemüürid ja lüüsid : takistada loata juurdepääsu eravõrkudele või nende kaudu.
- Turvaline konfigureerimine : tagab süsteemide konfigureerimise organisatsiooni vajadustele kõige turvalisemal viisil.
- Juurdepääsu kontroll : tagab, et ainult need, kellel peaks olema juurdepääs süsteemidele, pääsevad neile sobival tasemel juurde.
- Kahjurvara kaitse : tagab viiruste ja kahjurvara kaitse, sealhulgas veebisaitide mustade loendite installimise ja ajakohastamise.
- Patch juhtimine : tagab, et viimase toetatud versioon rakendused kasutatakse ja et kõik vajalikud plaastrid tarnija poolt on rakendatud. [6]

Cyber Essentialsi ja samalaadsete skeemide turvakontrollide eesmärk on eelkõige pakkuda võimalikult odavat küberturvalisuse taset; siiski peaksid nad kaitsma kaugelt kasutatavate toodete tasandil haavatavuste eest. [6]

Lisaks nimetatud tööriistale võrreldakse ja tehakse erinevaid turvanõrkuste kontrolle ka teiste väikefirmadele pakutavate tarkvaradega ja analüüsitakse saadud vastuseid. Lisaks mainiti, et kui ISO 27001 rakendati keskmise suurusega ettevõtetele, olid paljud standardi nõuded kättesaamatud. See kinnitab muude uuringute järeldusi, mis on juhtinud tähelepanu sellele, et väikeettevõtjad seisavad üldotstarbeliste turvastandardite (nt ISO 27001) kohaldamisel silmitsi paljude takistustega, sealhulgas kvalifitseeritud ressursside nappus, standardi rakendamiseks vajalik aeg, standardi keerukus, sertifitseerimisprotsessi maksumus ja standardi kohaldamise eeliste selge kvantifitseerimine. [6]

Selles artiklis kasutatu vähem agressiivset lähenemisviisi, rakendades eriti arhitektuurilisi ülevaateid, konfiguratsiooni ülevaateid ja intervjuusid (mis on teadaolevalt siiski praktikas kõige kuluefektiivsemad turvatestide tehnikad). Hindamise ühe osana

kaardistati kõigepealt ühe valitud väikeettevõtte tunnused ja ühelt poolt võrguomadused ning teiselt poolt 200 juhuslikult valitud haavatavust. Vaatadi arhitektuuri- ja konfiguratsiooniülevaadete ning intervjuude käigus välja töötatud teavet, et teha kindlaks, kas haavatavus on kohaldatav igale ettvõttele ning organisatsiooni tavadele ja poliitikale. Seejärel viidi läbi topeltkontrollitud leevendamise hindamise protsess, võttes arvesse kohaldatavaid haavatavusi ja seda, kas turvaauke leevendatakse juhul, kui turvakontrolli rakendatakse ettevõtetes. [6]

Järeldus, milleni jõuti oli, et kõige levinumad haavatavused on teenuste keelamine, koodi täitmine ja privileegide saamine. Uuritud *Cyber Essentialsi* puhul olid ainult kaks haavatavust turbekontrollidega vältimatud; need olid juhtumid, kus haavatavused olid tingitud riistvaralise seadme olemuslikest vigadest või tarkvarast, mida ei saa parandada. [6]

Artikli lõpus jõuti järeldusele, et turvasüsteemide kaudu jagatav teave haavatavuse kohta on esitatud väga tehnilises sõnastuses ja kirjeldustes, mis võib muuta need eriti läbimatuks vähem tehniliselt vilunud lugejatele. See on veelgi keerulisem, kui ekspluateerimisi kirjeldatakse ilma probleemi tegelikult selgitamata, nõudes, et lugejal oleks probleemi mõistmiseks kättesaadavad varalised teadmised. Lõppkokkuvõttes tuleb luua haavatavusega seotud probleemidega tegelemiseks hõlpsamini juurdepääsetav vorm, mis võimaldaks väiksematel ettevõtetel enne rünnet kaitsemeetmeid rakendada. Samuti tuleks arvestada ettevõtete ja teenuseosutajate turvalisusega. Isegi kui väikeettevõttel on turvakontroll paigas, sõltub pilveteenuste kasutamine ohu leevendamiseks müüja turvakontrollist. Teisisõnu on pilvepõhine e-post, pangandus ja raamatupidamine, failide jagamine ja muud pilvepõhised või kaugteenused ainult nii turvalised, kui teenusepakkuja neid teeb. Üldiselt tuleks nende teenuste pakkujaid julgustada nende kaitset kinnitama (nt selliste raamistike kaudu nagu ISO 27000 seeria), et ettevõtted saaksid teha paremaid ja teadlikumaid valikuid nende kasutatavate pilveteenuste osas. [6]

2.1.7 Information Visualization Metrics and Methods for Cyber Security Evaluation

Käesolevas artiklis kirjeldatakse mitmeid hindamismeetodeid teabe visualiseerimise vallast ja võimalusi nende kasutamiseks küberjulgeoleku valdkonnas. Keskendutakse tehnikatele, mis on valideeritud autorite endi kogemuste käigus erineva suurusega

ettevõtetega, sealhulgas ka Ameerika Ühendriikide õhujõud. Soovitused on antud ka sellepõhjaliste toodete kujundamiseks. [7]

Küberründed arenevad pidevalt ja ründajad loovad automatiseeritud süsteemide abil „kunsti“. Visualiseerimine hädavajalik, et võimaldada küberanalüütikutel töötada automatiseeritud tööriistadega, mõista kiiresti küberturbe andmeid ja teha teadlikke otsuseid, kuidas reageerida. Teabe visualiseerimisega seotud töö on tavaliselt keskendunud edusammudele, mida saab üldistada valdkondade lõikes. Küberturvalisuse visuaalse analüüsi tööriistade kujundamisel ja hindamisel on vaja rangemaid lähenemisviise. Selles artiklis tuuakse välja olulisemad punktid/seosed, kuidas hinnata vajalikkust ja otstarvet. Lisaks ka lühike ülevaadet andmetest ja ülesande atribuutidest, mis muudavad küberturvalisuse nõuded ainulaadseteks ja aitavad seega kujundada ning hinnata. [7]

Tuuakse välja ka kasutajauuringute vajadus ja ulatus mitteametlikest vestlustest tööriista kasutajatega kuni hästi kavandatud eksperimentideni, mis isoleerivad muutujad ja mõõdavad kasutaja reageerimist visuaalsele stiimulile. Kasutajauuring peaks sisaldama vähemalt küsimustikku. Küsimused võivad hõlmata kasutajate hinnanguid vajalike ülesannete täitmise kiiruse, täpsuse ja lihtsuse kohta. Küsimustiku saab esitada testgrupile kellele ei anta visuaalse analüüsi tööriistu, samuti erinevatele kasutajarühmadele, kellele antakse erinevad tööriistad. Likerti skaalat saab kasutada kasutajate kvantitatiivsete vastuste esilekutsumiseks hõlpsamaks võrdlemiseks. [7]

Ennustamine ja teadmiste avastamine on kaks kõige väärtuslikumat ülesannet, mida visuaalne analüüs saab toetada. Teadlased saavad prognoosimise ja teadmiste avastamise tuge hinnata, lastes kasutajatel dokumenteerida analüüsi käigus saadud teadmisi visuaalse analüüsi tööriistade abil ja ilma. Sissevaated võivad sisaldada seoste, suundumuste või kõrvalekallete vaatlusi ja nende põhjal ennustada tuleviku sündmusi. Prognooside hindamiseks saavad teadlased kasutada pärismaailma andmekogumit ja selle ajaliselt segmentida. Katsealustele antakse varasem segment ja neil palutakse ennustada võimalikke tulemusi. Neid prognoose saab seejärel hinnata hilisemates andmesegmentides näidatud alusetu tõe alusel. [7]

Teadlased peavad selliste hinnangute kavandamisel silmas pidama küberturbeülesande omavahelist olemust: teadmised on kasulikud ainult niivõrd, kuivõrd need võimaldavad analüütikutel ebasoovitavatest sündmustest aru saada, neid ennustada ja ennetada. [7]

2.1.8 Can We Evaluate the Impact of Cyber Security Information Sharing?

Artiklis kajastatud uuringust selgub, et küberjulgeoleku alase teabe jagamise nõuetekohaseks rakendamiseks on endiselt oluline inim- ja finantsressursside kaasamine. Järjest enam eraldatakse vahendeid küberjulgeoleku tootmiseks ja jagamiseks. Kaasuses käigus läbiviidud küsitlusest (304 ettevõtja seas) selgus, et ¾ vastanutest on valmis järgmise kahe aasta jooksul investeerima küberjulgeoleku ohtusid tuvastavatesse programmidesse. See uuring tõendab küberjulgeoleku teabe jagamise olulisust ja aitab kaasa üldisele tulemuslikkusele ja tootlikkusele. Välja on toodud, et automatiseeritud küberjulgeoleku teabe jagamise süsteemid aitavad analüütikutel oma tööülesandeid efektiivsemalt täita. Küberteabe jagamise positiivse mõju kohta esitatud väidete toetuseks on siiski vähe ja empiirilisi tõendeid. Lisaks üldisele teabevahetuse eelistele ja anekdootlikele tõenditele peitub kogu küberteabe jagamise jõupingutuste ja tehnoloogia valdkond ning küsimus nende rollist organisatsiooni küberturvalisuse parandamisel. [8]

Küberjulgeoleku alase teabe jagamise kogemusliku toe puudumine toob välja kaks põhilist puudust. Esiteks on erasektori organisatsioonid mõnikord ettevaatlikud või ei soovi teabe jagamise jõupingutustega liituda mitmesugustel põhjustel, sealhulgas konkurents, vastutus ja investeeringu tasuvus. Ilma empiiriliste tõenditeta küberjulgeolekualase teabe jagamise väärtuse kohta on osalemist stimuleerida raskem. Teiseks takistab küberjulgeoleku teabe jagamise jõupingutuste ja tehnoloogia hindamismeetodite puudumine nende puuduste tuvastamist ja kõrvaldamist. [8]

3 Infoturbe küsimustiku koostamine

3.1 Küsimuste koostamise põhimõtted

Küsimustik koostati eesmärgiga, et see oleks arusaadav kõigile, olenemata vastaja rollist ettevõttes nt. juhtkonna liige, tavatöötaja ja ettevõtte IT-ga seotud inimene. Küsimustik on jaotatud infoturbe valdkondade kaupa viieks küsimuste plokiks, igas 5 küsimust. Küsimustele vastamisel eeldame, et see, kellele see küsimustik on suunatud vastab esitatud väidetele iseseisvalt ilma kõrvalise abita.

Küsimustikku koostamisel arvestasime heade tavadega ja reeglitega [13]. Eesmärk oli teha küsimustiku küsimused lühikesed ja kergesti mõistetavad. Koostasime küsimused, mis vastavad järgnevatele kriteeriumitele:

- iga küsimus mõõdab omas valdkonnas midagi olulist,
- kogub vastaja kohta täiendavat informatsiooni, mis võimaldab tulemusena anda soovitusi,
- küsimused on ühtselt mõistetavad ja ei vaja erialaseid teadmisi ega kõrvalist abi
- vastaja on valmis küsimusele vastama ausalt, soovikorral saab seda teha ka anonüümselt

Igale küsimusele tuleb valida sobivaim vastus järgnevatest küsimuste vastuste variantidest:
JAH- 1 punkti
EI OSKA HINNATA- 0 punkti
EI -0 punkti

Küsimusteploki alajaotused:

1. Isikuga seotud turvalisus
2. Turvaliseus ettevõtte töötajana
3. Teadlikkus võimalikest ohtudest
4. Planeerimine ja kaitsmine
5. Tagajärgedega tegelemine

Kõigile küsimustele vastamine ei võta aega rohkem kui 5-7 minutit.
Tulemused arvutatakse kokku igas alajaotuses eraldi.
Skaala on järgmine:
0-2 näitab selget vajadust turvalisuse tõstmiseks, info jagamiseks ja ka koolitusvajaduseks, 3-4 turvalisuse peale on mõeldud aga vajab kaasajastamist või põhimõtete ülevaatamist
5- kõik on väga hästi ja olulisi muudatusi tegema ei pea lähiajal, aga oluline on end hoida kursis uute võimalustega korra aastas

Esialgu luuakse küsimustikust vaid eesti keelne versioon, hiljem tulevad juurde ka vene keelne ja inglise keelne versioon.

3.2 Küsimustiku katsetamine seotud osapoolte peal ja kasutajatestid

Küsimustiku esimene versioon valmis Google Forms platvormil ja selles oli poole rohkem küsimusi ja küsimuste sõnastused olid kohati liiga keerukad. See tuli välja kogutud tagasisidest kui autorid esmast versiooni 2020 aasta augustis testgrupi peal testisid. Lisaks tekkis probleem ka sellega kuidas kogutud andmeid turvaliselt säilitada ning mil viisil võimalik neid hiljem ka töödelda ja analüüsida.

Protsessi käigus katsetati erinevaid olemasolevaid platvorme, aga saadi aru, et ükski neist ei ole sobiv küsitluse kasutamiseks. Probleem seisnes ka selles, et valiku sai teha platvormide vahel, mis oli juba AS Telia Eesti poolt aktsepteeringu saanud ning neid ei olnud väga palju ning nende sobivaks kohandamine oli väga piiratud võimalustega. Paraku ei sobinud need autorite ideega ning olime sunnitud alustama päris algusest uue tööriista loomisega. Protsessi olid kaasatud lisaks projekti meeskonnale ka AS Telia Eesti turundus, veebitiim, küberturbe osakond, B2B ja ka kliendikogemuse- ja uuringute eest vastutavad inimesed.

Saadud tagasiside põhjal vähendasime küsimuste arvu igas osas 5-le, et vastamine ei võtaks ülearu palju aega ja kasutajal ei tekiks soovi enne lõppu katkestada. Lisasime ka nn. vastamisjoone, mis kuvab protsendiliselt kui palju on vastatud. Samuti muutsime küsimusi selgemini mõistetavateks erinevatele taustateadmistega vastajate jaoks.

Selleks, et hiljem saadud andmeid analüüsida, lisasime ka vastaja profiili kirjeldavad andmed, mille alusel seda teha, juhuks kui kasutaja ei soovi sisseregistreerida ja oma isikut tuvastada. Kasutasime enda jaoks vajalikke plokke, et määratleda kasutaja kohta olulise info saamist (vanus, haridus, ametipositsioon, organisatsioonis töötatud aeg). Nende alusel on võimalik luua kasutaja profiile, mis aitavad edaspidi tootede ja teenuste väljatöötamisel teha paremini sihitud pakkumisi.

3.3 Küsimustiku lõplik valmimine

Küsimustiku koostamisel valmisid esimesena sisuline pool ja veebidisain. Järgmise sammuna skoori arvutamise loogika ja vastuste sisu. Telia Küberturbe osakonnaga läbitöötatud küsimused andsid ka ülevaate, milliseid järeldusi/soovitusi on võimalik kliendile anda/kuvada.

Töökäigus selgus ka, et ühtse loogika järgi igale alajaotusele siiski skoori ja hinnanguid anda ei õnnestu. Seetõttu said 1, 2 ,5 osa küsimustikust ühtse lähenemise ja 3 ning 4 teisese lähenemise. Esimese, teise ja viienda puhul antakse vastajale üldised soovitused, mida peab tegema, et oma taset tõsta. Kolmandas ja neljandas osas soovitatakse konkreetseid teenuseid AS Telia Eesti portfellist.

Kahjuks ei ole hetkel ka Telial kõigile vastustele pakkuda kohe sobivaid lahendusi Telia poolt pakutavate teenuste näol. Samas soovitusi saab anda ja küsimuste eesmärk on siiski aidata mõõta teadlikkust, seega lahenduse pakkumine Telia teenustena on pigem boonuseks kui eesmärk iseenesest.

Samaaegselt sisulise poole kokkupanemisega toimus ka küsimustiku frontendi ja backendi valmimine. Ühtlasi oli see ka protsessis kõige keerulisem ja aeganõudvam tegemine . Selle peamiseks teostajaks oli bakalaureuse tudeng, kes küsimustikku ehitades sai ka ise palju targemaks ja teadlikkumaks. Paraku ainult temaga ikkagi küsimustiku lõpliku valmimiseni ei jõutud ning viimases faasis pidid autorid kaasama ka täiendavalt arendajaid väljastpoolt AS Telia Eestit, kuna ettevõtte sees arendusmeeskonda pakkuda ei ole.

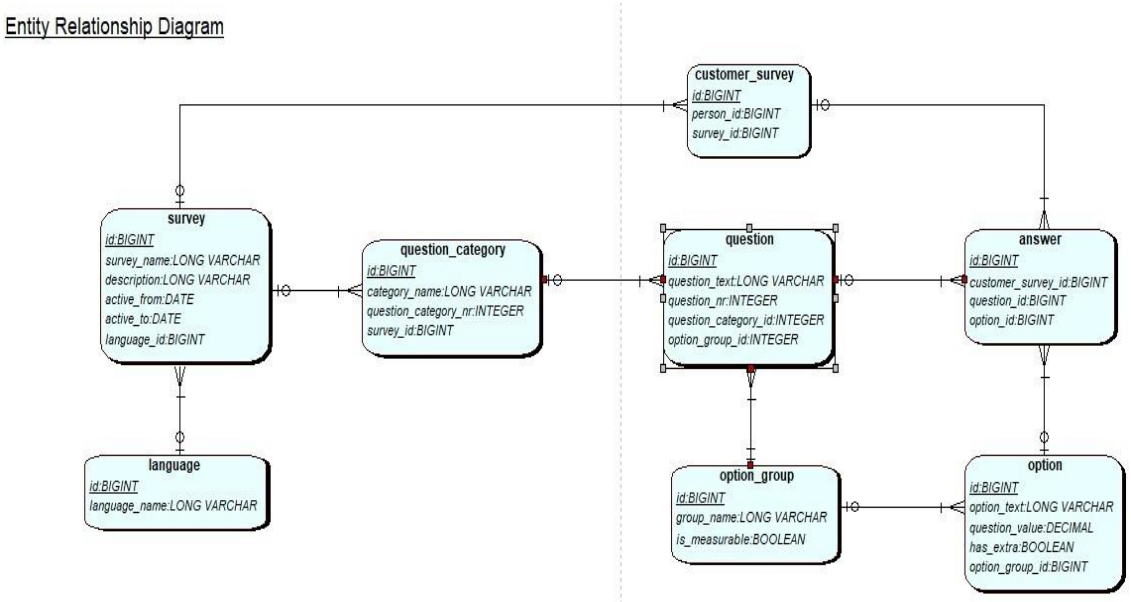
Peale pikka arendusfaasi ja testimisi sai lahendus valmis ja on leitav AS Telia Eesti küberturbe kodulehelt ja ka AS Telia Eesti IT portaali sisse logides.

Teadlikkuse tõstmise trendi jälgimiseks plaanime kaasata samasid vastajaid ning paluda neil täita küsimustikku uuesti vähemalt korra aastas.

3.3.1 Küsitluse andmemudeli tehniline kirjeldus

Magistritöö alguses andsid autorid oma arendajale sisendi, milline on nägemus valmivast küsitlusest. Selle alusel joonistas arendaja küsitluse andmemudeli. (Joonis 6)

Küsimustiku loomisel kasutati andmemudelit , mis koosneb kaheksast olemist, mis omavahel suhtlevad. Igal olemil on vajalik identifikaator, mis peab arvestust, mitu kirjet andmebaasis sellesse olemisse salvestatud on. Identifikaatorid tunneb ära nende nimes sisalduva "id" järgi. Olemid, milles sisaldub mõnest teisest tabelist pärinev identifikaator, vajavad seda identifikaatorit saamaks aru, millise vanemolemi "küljes" nad on.



Joonis 6. Küsitluse andmemudeli tehniline joonis.

Kõige ülemine olem on "*language"* (keel). See sisaldab teavet, mis keeles antud küsimustikku kuvada.

Olem "*survey*" (küsimustik) sisaldab teavet küsimustiku enda kohta. Selles sisalduvad kirjed on küsimustiku kuvatav nimi, küsimustiku eesmärki selgitav kirjeldus ning kuupäevad, millest alates kuni milleni välja on küsimustik aktiivne.

"Question Category" (küsimuse kategooria) nimeline olem võimaldab küsimustiku jaotamise erinevatesse kategooriatesse. Sellesse olemisse salvestatav teave hõlmab endas

küsimustiku alamkategooria nime ja järjekorranumbrit, mille järgi on võimalik määrata kindlaks kategooriate kuvamine rakenduses.

Järgmine olem, nimega *"question"* (küsimus) sisaldab andmeid küsimuse enda kohta. Peale teda siduvate identifikaatorite sisaldub temas küsimuse tekst, mida küsitluse täitjale kuvatakse.

Ühendused olemite vahel tähistavad tabelite sõltuvust teineteisest. Ühenduste seletamiseks vaatleme seost olemite "survey" ja "*question_category*" vahel. Olem "*question_category*" vajab eksisteerimiseks vähemalt ühte kirjet olemis "survey". Olemi "survey" jaoks ei ole tähtis, et "*question_category*" sisaldaks kirjeid. Ühe kirje kohta olemis "survey" võib olla mitu kirjet olemis *"question_category*". Need kirjed pannakse omavahel kokku, andes olemisse "*question_category*" olemi "survey" identifikaator. Olemis "question_category" on see väli "survey_id". Lihtsustatult: olemi "survey" ühe kirjega võib olla seotud mitu kirjet olemis "*question_category"*. Kirje olemis "*question_category"* ei saa eksisteerida ilma ühegi kirjeta olemis "survey".

Ainus olem, mis peale "*language*" teiste olemite kirjete olemasolust ei sõltu, on "option group" (valikugrupp). Selle olemi eesmärk on grupeerida küsimuste vastusevariandid, et muuta andmebaasi andmete sisestamine kergemaks (jah-ei küsimuste puhul piisab sellest, kui neid andmebaasi vaid üks kord sisestatakse selle asemel, et iga küsimuse jaoks eraldi uuesti jah-ei-ei oska vastata lisada). Valikugrupis on selle eristamiseks grupile antud nimi, mille olemasolust lõppkasutaja midagi ei tea ning kirje selle kohta, kas mainitud valikugrupis sisalduvate valikute abil arvutatakse kokku küsimuse tulemust.

"Option" (valik) on olem, mis esindab ühte mitmest võimalikust vastusevariandist. Olemi kirjed sisaldavad valiku teksti, mida lõppkasutaja näeb ja teavet arendajale, kas sellel küsimusel on väärtus (1 või 0, tulemuse arvutamiseks vajalik) ning ega tal lisaküsimusi ei ole, mis selle kindla vastusevariandi valimisel kuvatakse.

Selleks, et teada, kes hetkel küsimustikku täidab, on andmebaasis olem *"customer_survey*" (klient/vastaja küsimustikus). Selle olemi eesmärk on siduda küsimustiku vastaja isik küsimustiku ja selle vastustega.

Viimane olem, *"answer"* (vastus) on kasutaja valitud vastus küsimusele. See olem sisaldab identifikaatoreid, mis seovad omavahel ära küsimuse, valiku (vastusevariandi) ja selle, kes küsimusele vastas.

3.4 Andmete hoidmine ja analüüs

Andmete hoidmine ja analüüs on planeeritud kahte etappi. Esimeses etapis autorid lasevad vastata küsimustele, selliselt, et isikustamist ei nõuta ja soovi korral saab küsimustikule vastaja ise oma andmed lisada ning saata koos vastustega Teliasse oma kliendihaldurile, kes koostab pakkumised vastavalt soovitustele.

Teises faasis valmib küsimustikule lisa võimalus isikustamiseks *(SSO)*, st kui kasutaja on küsimustiku täitnud, siis tekib võimalus sisselogimiseks ja eraldi kasutaja ise andmeid saatma kuhugi ei pea.

.Küsimustiku juurde on loodud *PostqreSQL* baas, kuhu andmed maha loetakse peale nupule vajutamist “VALMIS”. Kirjed salvestatakse esimeses etapis siis anonüümsete andmete alusel (sugu, vanus, haridus, ametipositsioon, ettevõttes töötatud aeg) ja teises etapis juba lisatud isikustatud andmetega (nimi, ettevõte).

Lihtsamaks analüüsimiseks ja järelduste tegemiseks transporditakse andmed exceli formaati

Andmete salvestamine toimub vastavalt kirjete tekkimisele. Isikustatud andmete puhul on võimalik korduvalt sooritatud küsimustiku vastuste hilisem võrdlev analüüs andmebaasi lisatud tunnuse järgi.

Selleks, et saada aimu küberteadlikkuse muutusest säilitame kogutud andmeid kaks aastat, et oleks võimalik hilisem, andmete analüüs ja trendide jälgimine.

Planeeritud on andmete mugavamaks ja lihtsamaks kasutamiseks luua AS Telia Eestis kasutusel olevasse Tableau programmi armatuurlaud. kus on võimalik andmeid kätte saada nii ettevõtte kui ka isiku tasandil. Vajalik on info suunatud pakkumiste tegemiseks ja kliendihaldurile parema ülevaate saamiseks.

4 Valideerimise plaan

Autorid seadsid töö alguses hüpoteesi, milleks oli, et nende poolt loodud küsimustiku küsimustele vastaja saab ülevaate teda ohustavatest võimalikest küberturbe riskidest ja hakkab teadlikumalt tegelema vastustest välja tulnud probleemidega ning välja pakutud soovitustega, et saavutada vajalik küberturbe baastase (Joonis 1) [20]. Sellega aitavad autorid ka kaasa kogu Eesti ettevõtluse turvalisemaks ja efektiivsemaks toimimiseks.

Selleks, et töös püstitatud eesmärki valideerida on autorid teinud järgmisi valideerimisele eelnevaid tegevusi.

- küsimused lisati küsimustikku selliselt, et need on kõigile arusaadavad ja mõistetavad
- küsimustele vastates antakse vastajale kohene vastus hinnangutega nõrk, keskmine ja tugev, mis näitab tema hetke olukorda
- peale seda antakse soovitused oma taseme tõstmiseks
- saata küsimustikku vähemalt korra aastas samaväärsele valimile vastamiseks

Lihtsad ja mõistetavad küsimused, loovad aluse ausalt ja tõeselt vastamiseks. Vastamise lõppedes saadakse kohe tulemus, mis on hästi või mida vaja kiiremas korras muuta. Soovitused on antud selliselt, et kasutajale ei tekiks tunnet, et see kõik on liiga keeruline ja arusaamatu. Lisaks on loodud küsimustiku lõppu link, kuhu vajutades on võimalik kohe saada ka AS Telia Eesti poolset abi/nõuandeid. Sarnasele valimile küsimustiku saatmisega saavad autorid hinnata osalejate vastamise aktiivsust ja võimaluse näha ka trende paremuse või halvemuse poole.

Töö alguses, kirjeldasid ka autorid sihtgruppi, kellele see tööriist on eelkõige suunatud, nendeks on eelkõige väike- ja keskmise suurusega Telia mõistes, ca 3000 ettevõtet. Autorid jätsid välja suurettevõtted, riigiettevõtted ja rahvusvahelised organisatsioonid, kuna nendes on üldjuhul olemas pikaajalised strateegiad, kuidas ohtusid vältida. Rahvusvahelistes organisatsioonides on juba laialt kasutusele võetud ka erinevad pakutavad tööriistad ja kuna rakendatakse neid korporatiivsel tasandil, siis üldjuhul on kaasatud ka Eesti filiaalid ja ettevõtted. Kokkuleppe kohaselt saadetakse esimest korda küsimustiku link AS Telia Eesti äriklientide uudiskirjaga, ca 8000 kasutajale.

Parameetrid millega plaanime mõõta hüpoteesi on:

- vastajate protsent
- keskmine skoor alajaotuste üleselt

AS Telia Eestis on üldiselt 10-15% vastamise määr uuringutes ja küsitlustes, kus vastused on anonüümsed ja vastajad otseselt tagasisidet ei saa, siis hindame meie küsimustiku vastamise protsenti kõrgemaks esimesel korral kuni 18% ja juba järgmisel korral kuni 20%, kuna autorite küsimustik annab vastajale ka midagi tagasi, sh olulisi soovitusi, kuidas oma teadlikkust ja turvalisust tõsta.

Autorid ei pea tulemusi usaldusväärseteks kui vastajate protsent jääb alla 10%. Samas leiavad, et kui vastajate protsent tõuseb, siis on teadlikkus tõusnud ja inimeste huvi enda olukorra hindamiseks ja muudatuste tegemiseks olemas.

Kogu skoori arvutamisel on aluseks alamkategooriate hinnangud iga osa kohta kuni 5 punkti, maksimum skoor 15 punkti. Seeläbi saame ka näha trendi, kas teadlikkus kasvab või hoopis on trend vähenev.

Autorid loevad oma püstitatud hüpoteesi valideerituks, juhul kui mõlemad kokkulepitud parameetritest näitavad kasvu võrreldes eelneva perioodiga, st vastajate arvu suurenemine ja keskmise punktiskoori tõus.

5 Järeldused ja kokkuvõte

Aastal 2020 alanud maailma vallanud pandeemia pidurdas oluliselt ka autorite plaanide elluviimist. Kevadel kadus seoses muudatustele Telias lootus saada ettevõtte poolsest rahastust projekti elluviimisele. AS Telia Eestis tehti muudatusi struktuuris, prioriteetides ja plaanitud arendusele omistati väga madala tasemega huvi ja tähtsus.

Olukorra stabiliseerumisel, sügisel, tekkis taas võimalus Telia poolset toetust kasutada. Üsna palju kulus ka aega praktikandile vajalike ligipääsude tagamiseks, taustategevuste kooskõlastamiseks, et loodav sobituks teiste Telia lahendustega, nii turunduslikult, tehniliselt jne. Nende tegevustega seoses said autorid ka IT projektijuhtimise alast otsest praktikat.

Töö alguses püstitatud eesmärkidest said saavutatud kõik, kuigi väikeste mööndustega. Kõige raskemaks kujunes sobiva meeskonna kokku saamine, eriti just koodi kirjutamiseks bakalaureuse tudengite otsimine. Autorid kasutasid inimeste leidmiseks erinevaid võimalusi, saates ülikooli listidesse praktika pakkumise kuulutusi, kasutades Tallina Tehnikaülikooli dekanaadi abi ning lisaks ka AS Telia Eesti andmebaasi praktikale soovijatest. Olles sobivad kanditaadid leidnud, anti neile nn. prooviülesanne, mille alusel tehti ka lõplik valik ühe inimese kasuks. Autorid polnud enne kokku puutunud ka praktikandi värbamisega AS Telia Eestis, seega ka see protsess võttis aega veidi rohkem aega kui oli esialgselt arvestatud.

Samaaegselt sobivate inimeste leidmise ja meeskonna kokkupanemisega, tegelesid autorid küsimustikku kõige olulisemate teemade valikuga ja küsimuste välja mõtlemisega. Selle tulemusena sündisid kõikehaaravad ja üheselt mõistetavad küsimused. Kõik kirja saanud küsimused on läbi mõeldud selliselt, et oleksid arusaadavad ja vastatavad olenemata vastaja rollidest ettevõttes.

Magistritöö tulemusena on valmis saanud veebipõhine küsimustik, mis annab ülevaate küsimustiku vastajale ülevaate enda infoturbealastest teadmistest ja ka üldhinnangu oma ettevõtte olukorrale. Küsimustiku lõpus saab vastaja soovitused infoturbealaste teadmiste

täiendamiseks. Tulemused kuvatakse kategooriapõhiste hinnangutena, mis on ka heaks orientiiriks ettevõttes infoturbe eest vastutavale isikule.

Kevadel 2021, kus AS Telia Eesti on lansseerinud oma küberturvalisuse maandumislehele www.telia.ee/ari/it-teenused/turvalisus/kuberkaitse/, on autorite poolt loodud küsimustik planeeritud selle oluliseks osaks. Päris alguses, kui teemaks olev küsimustik veel mõtte tasandil küpses, ei olnud ideele Telia organisatsioonis väga palju toetajaid. Projekti arenedes leidis tööriist järjest rohkem toetajaid ja tänu sellele ka rahalisi võimalusi lõplikuks elluviimiseks. Nüüd peetakse selle valmimist oluliseks ja see on paigutumas oma kohale AS Telia Eesti plaanis küberturvalisuse baastaseme info viimisel oma klientideni (Joonis 1). [20]

Koostöös erinevate osakondadega on loodud veebipõhine terviklik mudel, mida saavad täita kõik AS Telia Eesti uuele küberturbe teemalisele vahelehele tulnud kasutajad. Koostöös AS Telia Eesti turunduse-ja küberturbe osakonnaga on lisaks autorite poolt teostatud tööriistale kasutajal võimalik tutvuda enamlevinud küberohtude ja-riskidega mille eest oma äri, kliente ja andmeid kaitsta, samuti Telia poolt pakutavate teenuste, huvitavate artiklite ja arvamuslugudega.

Üheks püstitatud eesmärkidest oli, et kogutud materjali kasutatakse AS Telia Eesti eesmärkide täitmise ja klientidele parema turvataseme loomisel. Kokkulepe kohaselt kasutatakse saadud infot Telia olemasolevate ja uute teenuste/toodete väljatöötamisel ja ka müügiprotsessis turvateenuste/toodete tutvustamisel ja vajaduse tuvastamisel.

Oleme jõudnud ajastusse, kus tehnoloogia kiire arenguga ja pidevate muutustega on raske sammu pidada ja see vormib uue reaalsuse. Ideed, mis olid paari aasta eest veel utoopia on täna olemas või lähitulevikus saamas reaalsuseks, nt ajuoperatsioon arsti juuresolekuta, kuum söök lauale trooni abil, interaktiivne teater ja kontserdid. [10] Tänu sellele julgevad autorid öelda, et teadlikkuse tõstmine on pidev protsess ja saavutatud taset ei saa lugeda lõplikuks. Kindlasti on vajalik inimeste järjepidev koolitamine ja harimine ja loodud tööriist on selle vajalikkuse mõõtmiseks hea võimalus. Autorid leiavad ka, et paari aasta möödudes tuleb neid küsimusi üle vaadata ja täiendada vastavalt muutunud olukorrale.

Kasutatud kirjandus

[1] Minhee Joo, Junwoo Seo, Junhyoung Oh, Mookyu Park, Kyungho Lee, “Situational Awareness Framework for Cyber Crime Prevention Model in Cyber Physical System”, 2018 IEEE

[2] Oskars Podzi5š, Andrejs RomŁnovs, “Designing a Evaluation Tool for IT Security Solution Implementation for IT Enterprises”, 2016 IEEE

[3] Jianhua Ma, Kim-Kwang Raymond Choo, Hui-huang Hsu, Qun Jin, William Liu, Kevin Wang, Yufeng Wang, Xiaokang Zhou, “Perspectives on Cyber Science and Technology for Cyberization and Cyber-enabled Worlds”, 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress

[4] Wenbo Wu, Rui Kang, Zi Li, “Risk Assessment Method for Cyber Security of Cyber Physical Systems”, The First International Conference on Reliability Systems Engineering
(2015 ICRSE)

[5] Simon Parkin, Andrew Fielder, Alex Ashby, “Pragmatic Security: Modelling IT Security Management Responsibilities for SME Archetypes” in Proc. ACM Int. Workshop on Managing Insider Security Threats, 2016,

[6] Jose M. Such, Pierre Ciholas, Awais Rashid, John Vidler, Timothy Seabrook, “Basic Cyber Hygiene: Does It Work?” Computer Year: 2019 Volume: 52 , Issue: 4 Pages: 21-31 IEEE Journals & Magazines

[7] John T. Langton, Alex Baker, “Information Visualization Metrics and Methods for Cyber Security Evaluation” 2013 IEEE International Conference on Intelligence and Security Informatics Year: 2013

[8] Adam Zibak , Andrew Simpson, “Can We Evaluate the Impact of Cyber Security Information Sharing?” 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment
Year: 2018

[9] Telia uudised, „Telia turvafiltrid eemaldavad 4,5 miljonit pahvavara tunnusega e-kirja päevas“. [WWW] https://www.telia.ee/uudised/telia-turvafiltrid-eemaldavad-4-5-miljonit-pahavara-tunnusega-e-kirja-paevas (06.04.2020)

[10] Telia uudised, Andre Visse „Tehnoloogia kiire areng vormib uue reaalsuse, [WWW] https://www.telia.ee/uudised/andre-visse-tehnoloogia-kiire-areng-vormib-uue-reaalsuse (10.06.2020)

[11] „ Infotehnoloogia kasutamine ja tulevikuplaanid Eesti ettevõtetes“ , Telia ja Kantar Emor uuring (2019)

[12] „Uuring: küberturvalisus ei paku eestlastele huvi ja sellest ei saada aru“ , Kristjan Ats Mägi [WWW]
https://digi.geenius.ee/rubriik/uudis/uuring-kuberturvalisus-ei-paku-eestimaalastele-huvi-ja-sellest-ei-saada-aru/ (2019)

[13] Majandus- ja Kommunikatsiooniministeerium, KÜBERTURVALISUSE STRATEEGIA, 2019-2022, [WWW]
https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf

[14] Uuring: Ligi 40% ettevõtetes ei tegele küberturbe teemaga otseselt keegi, [WWW] https://www.telia.ee/uudised/uuring-ligi-40-ettevotetes-ei-tegele-kuberturbe-teemaga-otseselt-keegi, Telia ja Turu-uuringute AS (15.02.2021)

[15] Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019 SYDNEY, Australia, [WWW]
https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019 (August 15, 2018)

[16] Küberkuritegevus aastal 2021: kodutöökohad pättide sihikul, Digitark [WWW] [https://digitark.ee/kuberkuritegevus-aastal-2021-kodutookohad-pattide-sihikul/ (11.03.2021)

[17] Alan R. Hevner, Salvatore T. March, Jinsoo Park, Sudha Ram " Design science in Information Systems research", MIS Quarterly Vol. 28 No. 1, pp. 75-105/March 2004

[18] Maung K. Sein, Ola Henfridsson, Sandeep Purao,Matti Rossim, Rikard Lindgren ," Acttion Design Research"MIS Quarterly Vol. 35 No. 1/March 2011

[19] "Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020,, , HedgeThink, 2020, https://www.hedgethink.com/worldwide-security-risk-management-spending-growth-slow-remain-positive-2020/

[20] AS Telia Eesti sisene dokumendihoidla [Online] IT WIKI
[21] AS Telia Eesti koduleht [WWW] https://www.telia.ee/ettevottest/uldinfo/
[22] KPMG koduleht: [WWW] https://www.xn--kberkaitse-9db.ee/

Lisad

Lisa 1- Küsimustiku küsimused

KUI HÄSTI OLED TURVAOHTUDEGA KURSIS?

Selleks, et saaksid parema ülevaate oma infoturbealastest teadmistest ning üldhinnangu ettevõtte olukorrale, palume allpool tutvuda turvaohte puudutavate väidetega ning valida iga esitatud väite puhul kolme vastusevariandi seast välja see, millega oled kõige rohkem nõus.

Väited on jagatud viide teemakategooriasse ning neile vastuste valimine võtab aega kokku 5-7 minutit. Küsimustiku lõpus esitatakse sulle isiklikud soovitused oma infoturbealaste teadmiste täiendamiseks. Tulemused kuvatakse kategooriapõhiste hinnangutena, mis on ka heaks orientiiriks ettevõttes infoturbe eest vastutavale isikule.

Sul on võimalik saata tulemused endale e-postile ja soovi korral saada Telialt teenusepakkumine. Kogutud andmetest on eelkõige kasu sulle ja sinu ettevõttele, samuti kasutatakse neid ka Telia teenuste ja toodete analüüsimiseks ja arendamiseks. Andmeid ei edastata kolmandatele osapooltele.

1. ISIKUGA SEOTUD TURVALISUS

- Olen kindel, et minu kui töötaja isiklikku informatsiooni sisaldavad andmebaasid on kaitstud autoriseerimata ligipääsu eest.
- Tunnen, et minule tööalaselt usaldatud info on selline, mis ei sea mind ja minu lähedasi ohtlikku olukorda.
- Tean, mis on tundlikud isikuandmed ja oskan nendega õigesti ümber käia.
- Tean, millised ohud kaasnevad, kui tundlike isikuandmetega õigesti ümber ei käida.
- Tean, mida teha siis, ja kuhu pöörduda, kui minule antud ligipääsukaardid on kaotatud või varastatud.

2. TURVALISUS ETTEVÕTTE TÖÖTAJANA

- Tunnen, et koht, mida kasutan töötamiseks (kontor või kodukontor), on piisavalt turvaline.
- Usaldan oma kolleege ja tööandjat ja ei muretse tagajärgede pärast, mis võivad kaasneda seoses isikliku informatsiooni jagamisega.
- Oskan käituda turvaliselt minu käsutuses olevate tööandjale kuuluvate seadmetega ja tööalase informatsiooniga.
- Tean, et kui kasutan tööandja seadet avalikus wifi-võrgus, võib see olla ohtlik mulle ja minu tööandjale.

- Tean, millised on minu praeguse tööandja juures töösuhte lõpetamisega kaasnevad protseduurid.

3. TEADLIKKUS VÕIMALIKEST OHTUDEST

- Tean, et salasõna lekkimisel aitab kahetasemeline autentimine ära hoida kohest ohtu minu organisatsioonile ja seadmetele.
- Tean, et ka nutiseadmed võivad põhjustada ohtu minu ettevõtte andmetele ja seadmetele, kui jätan need lisakaitseta (salasõna, muster, sõrmejäljelugeja jne).
- Tean, et serverite omamisel on oluline lisaks füüsilisele turvalisusele ka andmete ohutu ja kaitstud käitlemine ja varundamine.
- Tean, et tundmatute isikute poolt saadetud e-kirjadega kaasas olevaid manuseid ning linke, mis tunduvad ebaturvalised või kentsakad, pole turvaline avada.
- Minu tööandja on jaganud regulaarselt mulle teavet infoturbe ohtude kohta ning selgitanud, kuidas nende eest ennast ja ettevõtet kaitsta.

4. PLANEERIMINE JA KAITSMINE

- Minu tööandja on paigaldanud kõikidesse seadmetesse ühtselt hallatava viirustõrjeprogrammi.
- Minu tööandjal on kasutusel informatsiooni klassifitseerimise mudel (nt avalik, ettevõttesisene, konfidentsiaalne).
- Minu ettevõte järgib GDPR-i nõudeid.
- Minu tööandja kontrollib korrapäraselt juurdepääsuõiguste kehtivust.
- Olen teadlik, et ettevõte varundab oma andmeid ja informatsiooni, et vältida andmekadu või -hävitust.

5. TAGAJÄRGEDEGA TEGELEMINE

- Olen teadlik, mida teha ja keda teavitada, kui ettevõtte süsteeme on rünnatud.
- Ma ei muretse andmete pärast, kuna tean, et kõik andmed on eelnevalt korrektselt varundatud ja koopiatest taastamine on kontrollitud. See tähendab, et ka peale küberrünnakut on võimalik kogu andmestik taastada.
- Ettevõttes on olemas kriisiplaan ja ma tean täpselt, kust selle vajadusel leian ja mida pean tegema tagajärgede minimeerimiseks
- Ettevõttes on olemas plaan, kuidas äritegevusega ka pärast rünnaku toimumist jätkata.
- Ettevõttes on välja arvutatud võimaliku rünnaku tõenäosus ja sellest tekkiva kahju suurus.

SINU ANDMED

Vanus

18–29

30–49

50–…

Haridustase

Põhiharidus

Keskharidus

Keskeri

Kõrgharidus

Ametipositsioon

Juht

IT-spetsialist

Kontoritöötaja

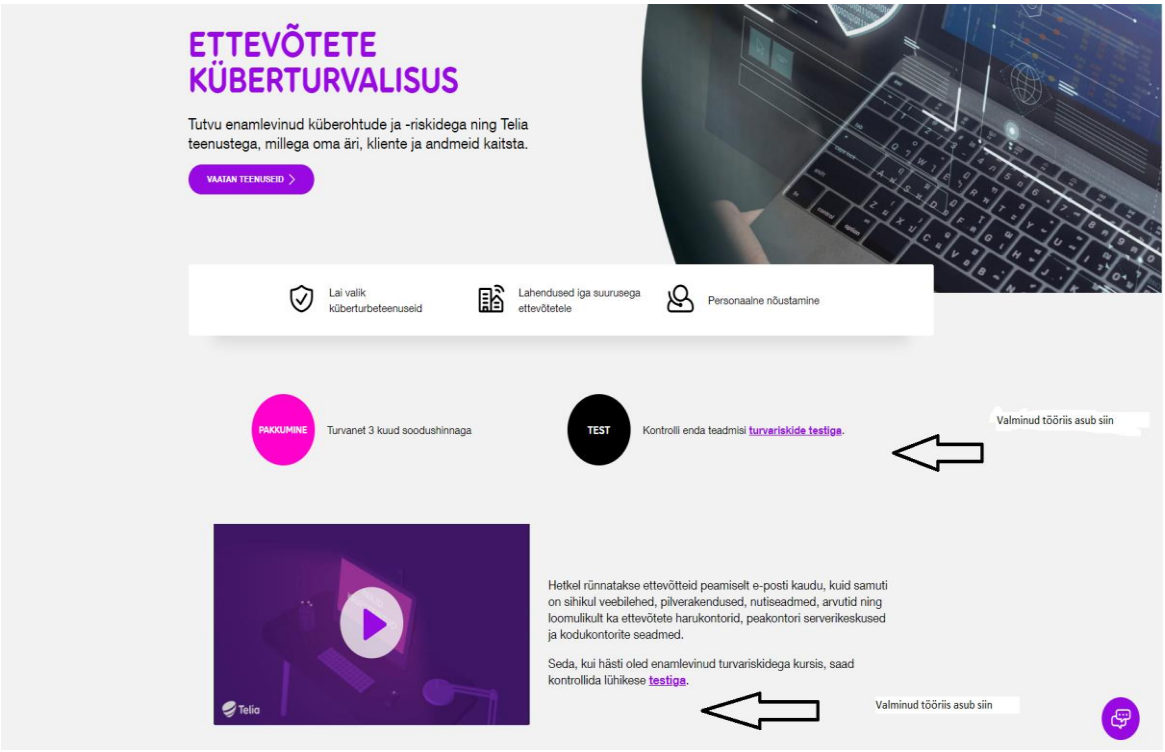
Organisatsioonis töötatud aeg

Alla 1 aasta

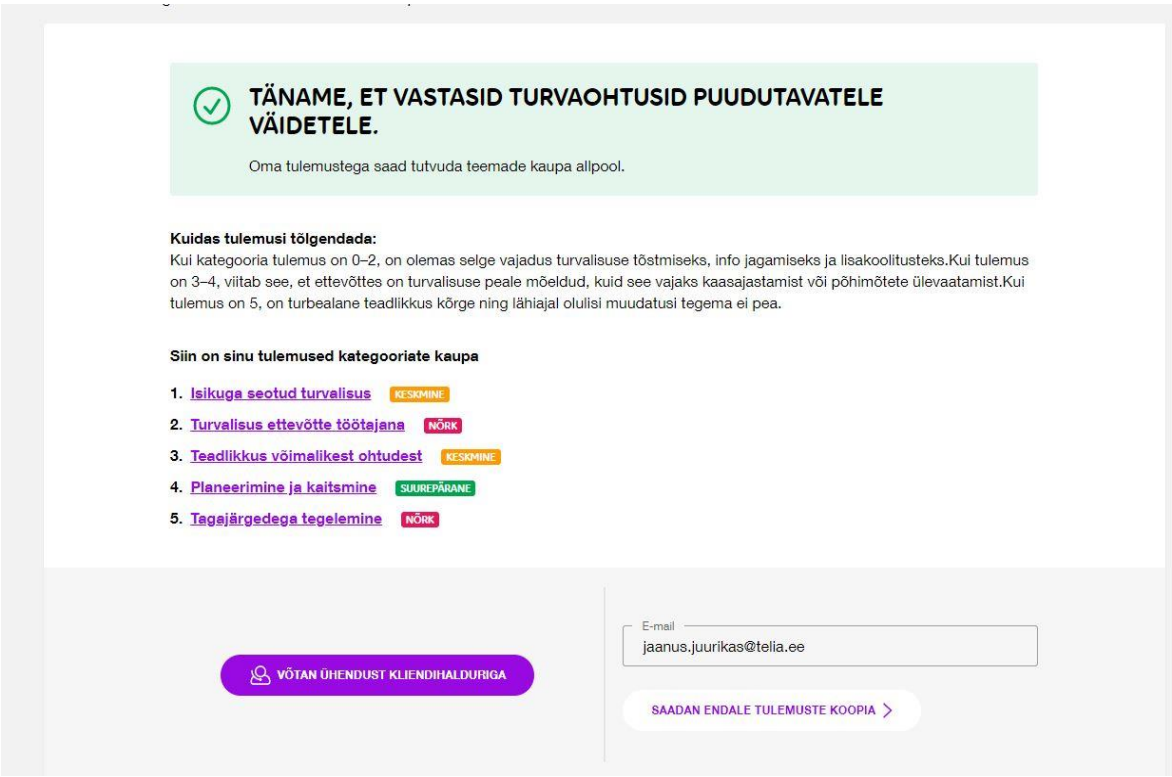
Üle 1 aasta

Lisa 2. Väljavõte Telia küberturvalisuse kodulehelt, kuhu lisatakse valminud tööriist

https://www.telia.ee/ari/it-teenused/turvalisus/kuberkaitse#packages



Lisa 3. Vaated tulemuste ja skooride kuvamisest



Lisa 4. Vastuste lingilt avanev lisaaken