TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Belinda Beatricia Borodin 185336IACB

Turvateadlikkuse koolitus kodukontoris töötajatele

Bakalaureusetöö

Juhendaja: Kaido Kikkas
Tehnikateaduste doktor

Tallinn 2021

Autorideklaratsioon

Kinnitan, et olen 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.

Autor: Belinda Beatricia Borodin

10.05.2021

ABSTRACT

Security awareness training for home office users

During the COVID-19 pandemic, many companies had to deploy the work from home solution. In the long running pandemic, home office was the only way employees could continue working. The problems regarding the home office are making it safe, making sure that employees have a good understanding of information security, and lack of security awareness training. Employees have much less access to cybersecurity help than usual and therefore people working from home should be more aware of the security risks in home office.

This topic is important because during a pandemic, it is necessary for people to be able to work from home and do so safely. In addition, the Covid-19 pandemic proved to the whole world that the home office solution is a possible way of working, and many companies can continue to use it. This thesis will also help employers to identify possible lacking in security that need to be addressed to ensure that employees are well resilient to cyber security risks in the home office.

The main research questions are, what are the differences between employees and the management regarding their thoughts about information security in the home office, and what solutions can be offered after the identification of the main problems? The first chapter of the thesis presents the possible differences between the home office and the office and analyses different risks based on the literature. The second chapter describes the methodology, the third chapter presents the analysis, and the fourth chapter has a training programme based on Chapter Three findings.

Based on the analysis of the thesis material it can be concluded that employees themselves can be their biggest helpers at home and a good awareness training can prepare them for that. Companies do their best to provide a secure infrastructure for the job, but the rest is up to the employee. Secondly, unless a clear plan is in place to report security incidents, they can often be overlooked. Thirdly, employees may consider themselves smarter than

they are while working in a home office and may overlook some important security factors.

As a solution the thesis offers a training to increase security awareness in the home office. The training outlines general information security techniques and at the same time focuses more on the dangers of the home office. The training and analysis are based on a specific company's needs but can also be used elsewhere.

The thesis is in Estonian language and contains 27 pages of text, 4 chapters, 5 tables.

Lühendite ja mõistete sõnastik

BYOD	*Bring Your Own Device*, võta oma seade kaasa
DDoS	*Distributed Denial-of-Service*, hajutatud teenusetõkestusrünne
DNS	*Domain Name System*, domeeninimede süsteem
DPI	*Dots per inch*, punkti tolli kohta
EL	Euroopa Liit
GDPR	*General Data Protection Regulation*, isikuandmete kaitse määrus
RDP	*Remote Desktop Protocol*, kaugtöölaua protokoll
VPN	*Virtual Private Network*, virtuaalne privaatvõrk

Sisukord

Tabelite loetelu

Sissejuhatus

COVID-19 pandeemia ajal pidid paljud firmad kasutusele võtma kodukontori lahenduse. Kodukontor on üks viisidest, kuidas töötajad saavad jätkata tööd ning kaua kestnud pandeemias on see muutunud uueks normaalsuseks [1]. Kodukontoris on teatud riskid, mida on pikemalt kirjeldatud peatükis 1.2. Töötajatel on tavalisest palju väiksem kättesaadavus küberturvalisuse vahenditele kui üldse ja seetõttu peaksid kodus töötavad inimesed saama koolitatud informatsiooni turvalisuse ja küberturvalisuse riskide osas. [2]

Teadmatus pandeemia kestvusest on paljud ettevõtted suunanud ideele, et teha kodukontorist püsiv lahendus [1,2]. Kodukontorite laienemine ja kasutusele võtmine annab hea võimaluse küberkurjategijatele, kes üritavad pandeemiast tulenevaid olukordi ära kasutada. Koroonaviiruse teemalised andmepüügi *(phishing)* rünnakud tekitavad probleeme ja on suunatud haavatavatele inimestele. Sellised rünnakud on ohtlikud nii firmadele kui ka inimkonnale. Paljud küberrünnakud on otseselt seotud inimesega ning rõhuvad nõrkadele kohtadele ja probleemidele – eelmisel aastal oli selleks koroona pandeemia. [2]

Käesoleva bakalaureuse töö eesmärgiks on aidata tööandjatel teadlikumalt planeerida oma koolitusi vastavalt töötajate vajadustele. Samuti aitavad saadud andmed tööandjatel leida üles võimalikud kitsaskohad, millega edasi tegeleda, kindlustamaks töötajate hea vastupanuvõime küberturvalisuse riskidele kodukontoris. Töös otsitakse vastust küsimustele, et millised on erinevused tavatöötajate ja juhtkonna arusaamast informatsiooni turvalisusest kodukontoris ning milliste lahendusteni on võimalik jõuda peale peamiste probleemide tuvastamist.

Töö esimeses peatükis on välja toodud kirjanduse põhjal võimalikud erinevused kodu- ja tavakontori vahel ning analüüsitud erinevaid riske. Teises peatükis on kirjeldatud metoodikat, kolmandas peatükis on toodud analüüs ja neljandas selle järelduste põhjal koostatud koolituskava.

Lõputöö raames tehtud koolitus ja analüüs on lähtuv konkreetsest ettevõttest ja selle vajadustest, kuid on kasutatav ka mujal. Firma jaoks on oluline koostada turvateadlikkuse teemaline koolitusprogramm kodukontori kasutajatele. Koolitus näitab, milline on

turvaline kodukontor, ning annab võimaluse tõsta tähelepanu. Samuti saab välja pakkuda lahendusi, et kodukontor turvalisemaks muuta.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 27 leheküljel, 4 peatükki, 5 tabelit.

1 IT-turvariskid ja kodukontor

Infosüsteeme võib defineerida viie peamise komponendiga: riistvara, tarkvara, andmed, inimesed ja protsessid [3]. Infosüsteemid puutuvad sageli kokku ohtudega, mis võivad mõjutada andmete konfidentsiaalsust ning süsteemi ja andmete kättesaadavust. Informatsioon on muutunud suurimaks küberrünnaku sihtmärgiks. Tööandjad peavad teadma, millised on nende ohud ja mõju informatsiooni varale. Kui ohud on teada, siis on neid võimalik tuvastada ja teha vajalikud ennetused nende vältimiseks. [4]

Whitman [5] tegi oma töös kindlaks põhilised ohud informatsiooni turvalisusele, uurides läbi mitmeid töid ja koostades intervjuusid. Leitud riskitegureid oli 12 ning on allpool välja toodud järjekorras, mis näitab, milline oht oli kõige suurem. Rünnakute analüüs peatükis 1.2 on lähtuv nendest punktidest.

1. Tarkvaralised ründed (viirused, ussid, teenusetõkestusründed jpm.)
2. Tarkvaravead ja turvanõrkused (turvaaugud, näiteks SQL-süstimine või puhvri ületäitumine)
3. Inimlik eksimus (andmete kustutamine või ligipääsu avamine volitamata osapoolele kasutaja enda poolt)
4. Küberspionaaž (andmevargus või infoleke süsteemi või andmeid kahjustamata)
5. Kübervandalism (süsteemide või andmete teadlik kahjustamine)
6. Riistvaravead ja turvanõrkused
7. Seadmete vargus
8. Loodusjõud (seadmete või info kahjustamine loodusjõudude poolt, näiteks tulekahju või uputus)
9. Intellektuaalomandi vastased rünnakud (autoriõiguste, litsentsi või patendi rikkumine)
10. Teenusepakkuja vead (elektrikatkestus, sidehäired)
11. Tehnika amortisatsioon (tehnoloogia füüsiline ja moraalne vananemine)

12. Väljapressimisründed (lunavararünne, tundliku info leke koos ähvardusega selle avalikustamiseks jm.)

1.1 Töö kodukontoris ja selle eripärad

Tehnoloogia areng on sundinud organisatsioone looma kaugtöö ja kodukontori lahendusi [7]. Kodukontoris on riskid, mis on seotud nende turvaliseks muutmisega ja töötajate puuduliku küberhügieeniga. Seetõttu on töötajatel väiksem kättesaadavus küberturvalisuse vahenditele ja seetõttu peaksid kodus töötavad inimesed olema koolitatud informatsiooni turvalisuse ja küberturvalisuse riskide osas [2].

Varasemad uuringud on analüüsinud kaugtöö ja kodukontori võimalikke eeliseid ja puuduseid. Kaugtöö eelisteks on suurem tööviljakus, vähem stressi, parem töö- ja eraelu tasakaal ning lühem tööle jõudmise aeg [7,8,9].Kaugtöö puuduste hulka kuuluvad isoleeritus, arusaamatused, vähenenud inimestevahelised kontaktid ja enda töörolli ebaselgus [10,11]. Lisaks on teised uuringud näidanud, et töö- ja eraelu tasakaal võib olla häiritud, inimesed teevad ületunde ning sotsiaalset suhtlemist on vähem, kui seda oleks kontoris tööd tehes [12,13,14]. Oluline on märkida, et mitme teadlase [8,10] sõnul on kodukontoris töötajatel pigem positiivsed kui negatiivsed tööga seotud kogemused võrreldes kontoris töötamise päevadega.

Vyas ja Butakhieo [15] on toonud välja kontori ja kodukontori SWOT (tugevused-nõrkused-võimalused-ohud) analüüsi Hong Kongi olukorra põhjal (Tabel 1). Huvitav tähelepanek on, et Eesti puhul võiks see tabel sarnane olla, kuid erisused tekivad kultuuris ja tööjõus.

	Kontoris töötamine	Kodukontoris töötamine
Strenghts	Suhtlemisvõimalused Koostöö võimalused Ennetada möödarääkimisi, järelevalve Töö ja eraelu eraldamine Kuuluvustunne Parem uute töötajate värbamine Hea keskkond keskendumiseks Ligipääs tehnoloogiale Andmelekete vähene risk	Paindlik Kontori segajate puudumine Vabadus Mugav, tuttav keskkond Ajakulu säästmine Raha säästmine Tööelu tasakaal Puudumiste vähenemine

Weaknesses	Ei ole paindlik Istuv elustiil Lärmakas keskkond Konflikt töökohas Ebaolulised vestlused Kasutud koosolekud Transpordi kulud Kallimad kommunaalkulud	Tähelepanu segajad Ebamugav keskkond Järelevalve puudumine Suhtlemisbarjäärid Sotsialiseerumise puudumine Puudulik riistvara tugi Töö ja eraelu segunemine Ebaõiglus
Opportunities	Säilitada professionaalne suhe klientidega	Hübriid töökoha mudelid Uued talendid üle maailma
Threats	Vähem tööjõu mitmekesisust Liiklusest tekitatud õhusaaste	Küberturvalisus Privaatsus Puudulikud kodukontori reeglid Lisakulutused kodukontoris töötamisega Kõrge konkurents

Tabel 1. SWOT analüüs Hong Kongi olukorra kohta. Autori tõlge allikast. [15]

Kaugtööd võimaldavad ettevõtted peaksid kindlasti:

- Rakendama määruseid, mis salvestaks dokumendid ja andmed automaatselt turvalisele kettale. Töötajaid tuleks julgustada salvestama oma tööfaile ettevõtte failiserverisse, millel on vajalikud turvameetmed. [16,17]
- Olema kindlad teadmises, et ettevõtte taristu on kaitstud turvaliste ühendustega sisevõrku. Osa sellest on kindla VPN-lahenduse (virtuaalse privaatvõrgu) ja asjakohase tarkvara tagamine. [16,17]
- Julgustama oma töötajaid konsulteerima kõiki probleeme IT-toe tiimiga. See tagab probleemide kiire ja turvalise lahendamise ning aitab vältida suuremat probleemi.[6,16]
- Investeerima töötajate koolitamisse. See on eriti oluline arvestades, et inimeste vead moodustavad veerandi kõigist andmetega seotud rikkumistest [18]. Nõuetekohase koolituse ja hea ettevalmistuse korral võivad töötajad osata erinevaid rünnakuid paremini tuvastada ja

lahendada. Samuti peaksid töötajad saama selged juhiseid koduruuterite ja Wi-Fi turvalise haldamise kohta ja olema teadlikud turvaliste DNS (domeeninimeserverite) seadistustest, et parandada kaitset pahavara ja andmepüügi vastu [16].

1.2 Kodukontori turvariskid

Järgnevate punktide aluseks on Whitmani [5] 12 riskitegurit, mida autor aga vaatleb kodukontori kontekstis.

1.2.1 Tarkvaralised ründed

Kõige tavalisemad ja efektiivsemad rünnakud pandeemia ajal on olnud seotud andmepüügi ja pettustega [21]. Paljud sellistest rünnakutest kasutavad ära koroonapandeemia ajal tekkinud hirme ning koroonaviiruseteemalised andmepüügi pettused võtavad võimu [2,22]. Kuna küberkurjategijad on olukorrast teadlikud, on neil lihtsam luua võltssõnumeid või veebisaite, mis sarnanevad tuttavatele ametiasutustele [21,22].

Pandeemia ajal on rohkem levima hakanud ka pahavara, mis on kõige ohtlikumad pandeemiaga võitlemisega seotud asutuste, finantsasutuste ja valitsuse jaoks [22]. Pahavara hõlmab näiteks arvutiviiruseid, usse, trooja hobuseid, nuhkvara ja lunavara [23]. Samuti on oluline märkida, et DDoS-rünnakuid kasutatakse tervishoiuorganisatsioonide õõnestamiseks kogu maailmas [22,24]. NETSCOUT [25] ohu raporti andmetel käivitasid võrgukurjategijad kiiresti üle 10 miljoni DDoS-i rünnaku, mis olid suunatud sihtmärkidele, kes tuginesid tugevalt veebiteenustele. Rünnakute sagedus tõusis aastaga 20 protsenti ja 2020. aasta viimase kuue kuu jooksul 22 protsenti, millest võib järeldada, et pandeemia ajal on levik tõusnud [25].

1.2.2 Tarkvaravead ja turvanõrkused

Kodukontoris on kõige suuremaks ohuks tugiteenuse puudumine probleemide korral. Kontoris on võimalus kohe abi paluda ja kiirelt probleemile lahendus leida, kuid kodukontoris tuleb töötajal ise tegutseda [2]. Tarkvararikked võivad olla tingitud erinevatest vigadest, tähelepanematusest või tarkvara eeldatava spetsifikatsiooni valest tõlgendamisest. Samuti võib see olla tarkvaraarendaja hooletusest, puudulikust testimisest ja tarkvara valest kasutamisest. [26]

Covid-19 pandeemia on põhjustanud mitmeid tarkvararikkeid, mida tavaliselt juhtunud ei oleks. Kaugõpe ja veebieksamid ning valitsuse nõuded kodukontoris töötamisele on põhjustanud kasutajate arvu kasvu mitmes rakenduses. Need on avaldanud suurt survet serveritele ja tarkvararakendustele, mis ilmselt ei olnud mõeldud nii suure kasutajate käsitlemiseks. 2020. aasta juulis leiti Zoomi tarkvaras kriitiline turvanõrkus, mis võimaldas kurjategijatel ligi pääseda arvutitesse, milles töötas Windows 7 või varasem versioon. [27]

1.2.3 Inimlik eksimus

Inimesed on kodus olles haavatavamad, sest neil ei pruugi olla kodukontori korral kontoris pakutavaid turvameetmeid. Kaugtöö ja kodu siseküsimuste segamisel suureneb töötaja hajameelsus, mis paneb unustama infoturbe. Samuti ei saa tööandja kontrollida kodus toimuvat ning seega jääbki kõik töötaja enda vastutada. Enamus rünnakuid on suunatud inimfaktorile ja inimese ärakasutamisele. Pandeemia ajal on rünnakud muutunud koroonateemalisteks ning kasutavad ära inimeste soovi saada kiirelt informatsiooni.[2] 84% küberrünnakutest toetuvad sotsiaalsele manipuleerimisele [28] ja lisaks on ühes uurimuses [29] välja toodud, et 53% osalenutest ei ole saanud mingeid juhiseid turvaliselt kodus töötamiseks.

1.2.4 Küberspionaaž

Spionaaž toimub siis, kui volitamata isik üritab saada keelatud juurdepääsu ettevõtte teabele või alale [31]. Pandeemia ja kodukontori ajal on suureks probleemiks tööandja teadmatus, mis inimeste kodudes toimub. Pereliikmed või kolmandad isikud võivad saada ligipääsu keelatud informatsioonile ning kurjategijad saavad sellist olukorda ära kasutada. Kui kontoris töötades, on tööandja võimalik enda poolt lisa turvameetmeid rakendada, siis kodus olles peavad töötajad selle peale ise mõtlema. [32] Lisaks on riskigrupiks suuremate rollidega inimesed, kes kodus tööd teevad, nt. tööandja ise või IT tiim, omades rohkeid ligipääse firma infosüsteemidele [6]. Oskuseid ülehinnates võivad nende vead tekitada firmale palju suuremat kahju, kui kontoris olles.

1.2.5 Kübervandalism

Vandalismi võib lugeda füüsiliseks rünnakuks ettevõtte riistvaraseadmete pihta. Ründaja tekitab füüsilist kahju ning põhjustab sellega teenuste kasutusvõimetuse. [33] Nagu ka spionaaži puhul on kontoris töötades tööandjal võimalik tagada omalt poolt kõrgemad

turvameetmed [32]. Kodukontoris võib ilmneda ka suuremaid tahtmatuid vandalismi juhtumeid, kus töötaja rikub oma seadme ise ära. Samuti võib lugeda tahtmatuks vandalismiks kodukontoris asjaolu kui mõni pereliige kogemata arvutile kahju teeb (nt. ajab kohvi peale) või lemmikloom arvuti laualt maha lükkab. Asendust pole kohe saada ning probleem võib minna palju suuremaks kui see läheks kontoris tööd tehes. [19]

1.2.6 Riistvaravead ja turvanõrkused

Kontoris töötades on tööandjal võimalus pakkuda firma poolt riistvara ja vajalikke turvameetmeid ettevõtte võrku ühendumiseks. Kodukontoris ei pruugi seda võimalust olla, sest kõigile töötajatele riistvara jagamine on kulukas. Sellisel juhul peab töötaja võtma kasutusele oma seadme ehk kasutama BYOD-lahendust ja parimal juhul saab tööandja pakkuda ettevõtte infosüsteemidega ühendumiseks VPNi (virtuaalne privaatvõrk). [19]

Ohustatud riistvaraline komponent võib nõrgestada süsteemi küberturvalisuse kõiki täiendavaid kihte. Riistvaraturvalisus keskendub süsteemide kaitsmisele seadmete füüsilises kihis olevate turvanõrkuste eest. Riistvaravead võivad jääda avastamata, ning leitakse alles siis kui riistvara on laialdaselt integreeritud ettevõtte taristusse. [30] Kontoris töötades on tööandjal võimalus pakkuda firma poolt riistvara ja probleemi korral koheselt lahendust pakkuda, kuid kodukontoris on sellise intsidendi haldus keerulisem ja ajakulukam, nt seadme vahetamine uue vastu [19]. Lisaks on ühes uurimuses [29] välja toodud, et 52% kaugtööks kasutatavast riistvarast on puudulike turvaeeskirjadeta ning järelevalveta. Kontoris olles peab tehnika rikkeid ja vigu jälgima tööandja ise, kuid kodukontoris on vajalik töötajal selle eest ise vastutada. Tuleb kindel olla, et tehtud oleks vajalikud uuendused ning veenduma tarkvara asjakohasuses [11] .

1.2.7 Seadmete vargus

Varguse puhul on oluliseks asjaoluks, et kodukontoris töötavad inimesed on kas üksinda või oma tuttava leibkonnaga, mis tegelikult muudab varguse riski kodus väiksemaks. Kontoris liigub kolmandaid isikuid, kes võivad olla ohuks, nt koristaja, tarnijad jne. [19] Siiski on kaugtöö tulekuga hakatud saatma salastatud infot läbi telekommunikatsioonikanalite ja halvasti kaitstud lõpp-punktide kaudu, mis annab küberkurjategijatele võimaluse informatsiooni teistmoodi varastada [30]. Varguse riski võib kodukontoris lugeda pigem väiksemaks kui kontoris töötades.

1.2.8 Loodusjõud

Looduskatastroofid nagu tulekahjud, tsüklonid ja üleujutused kujutavad endast ohtu ka IT-süsteemidele, andmetele ja taristule. Hoonete ja riistvara kahjustumine võib põhjustada klientide või muude andmete kadumist ning tuua suurt kahju [33]. Näiteks on Elisa Eesti öelnud intervjuus [34] sõltuvalt Riigi Ilmateenistuse äikesehoiatuse astmest pannakse kokku vajalik reageerimisrühm võimalike rikete kõrvaldamiseks. Lisaks on Elisa teinud enda klientidele kodulehele levikatkestuste kaardi, kus on võimalus levikatkemisi jälgida. Sama oht jääb ka kodukontorisse, kuid erinevus tuleb taaskord intsidentihaldusest, kus kodukontori puhul peab töötaja selle lahendamisega ise hakkama saama. [34]

1.2.9 Intellektuaalomandi vastased ründed

Paljud organisatsioonid tegelevad intellektuaalse vara loomisega, mille alla käivad näiteks autoriõigused, kaubamärgid ja patendid. Ehkki enamik suuri ettevõtteid kaitseb end spionaaži eest, on intellektuaalseomandi vargus enamasti just siseringi oht. [35] Kodukontoris suureneb tahtmatu intellektuaalomandi ründamine, näiteks töötajad ei keskendu sellele, mida nad arvutisse alla laadivad, ning rikuvad nii mõne litsentsi nõudeid. Samuti võib ohtlik olla, kui tööarvutit kasutab veel mõni pereliige, kes ei tea turvanõuetest midagi ja teeb teadmatult intellektuaalomandile liiga. [36]

1.2.10 Teenusepakkujate vead

Teenusepakkuja kõrvalekalded tekitavad riske, kus tooted või teenused ei toimi ootuspäraselt. Enamasti sõltub ettevõtte infosüsteemi töötamine mitmest tugiteenusest ja paljud Interneti-, side- ja elektriteenusepakkujate vead mõjutavad süsteemide kättesaadavust. [35] Erinevus kodukontoris võib tulla sellest, et teenusepakkuja jaoks on firma äriklient ning töötaja üldiselt tavaklient. Mingitel juhtudel võib selline jaotus mängida suurt rolli, sest äriklientide teenindamine ja probleemide lahendamine käib efektiivsemalt ja kiiremini, kui tavaklientide oma [19]. Samuti võib kodus kasutatav teenusepakkuja erineda ettevõtte omast, sel juhul aga tuleb töötajal kõik teenusepakkuja vead ise lahendada ja tuvastada.

1.2.11 Tehnika amortisatsioon

Vananemise võiks jaotada kaheks – füüsiline vananemine ehk mingi seade hakkab kuluma ja moraalne vananemine. Moraalne vananemine toimub tavaliselt siis, kui vanema versiooni asemele on loodud uus toode. Tavaliselt on kontoris firma poolt ette nähtud tehnika uuendamise määrused, kuid kodukontoris peab töötaja ise veenduma enda tehnika asjakohasuses. Suurimaks ohuks on moraalne vananemine, mis juhul töötaja ei pruugi tahta oma vana töötavat seadet uuema versiooni vastu välja vahetada. Vanemad seadmed võivad olla ohuks paljudele uutele riskidele ning kodukontoris see risk suureneb. [19]

1.2.12 Väljapressimisründed

Väljapressimine tähendab võõra vara või muu varalise kasu üleandmise nõudmist ähvardusega kasutada isiku kallal vägivalda, piirata isiku vabadust või avaldada häbistavaid andmeid [36]. Näiteks võib lunavara muuta erinevad failid ligipääsmatuks, mis sunnib ohvrit lunaraha maksma, et oma faile lukust lahti saada [39]. Koroonapandeemia ajal on teabe välja pressimine suurenenud. See kasv on tingitud nõrgenenud koduste infotehnoloogiliste süsteemide tõttu ja kasutajate klõpsamisest Covid-19 teemaliste lunavara sisaldavate e-kirjadele. [31] Inimesed on kodus olles haavatavamad, sest neil ei ole kontoris pakutavaid turvameetmeid. Tähelepanu hajub kiiremini ja võib viia mõtted mujale, mis paneb unustama informatsiooni turvalisuse. Samuti ei saa tööandja kontrollida kodus toimuvat ning seega jääbki kõik töötaja enda vastutada. [2]

Väljapressimise suureks riskiks on kodukontoris töötajate unustamine varukoopiad teha. Kontoris on teabe varundamine ja koopiate tegemine sisse juurutatud protsess, kuid kodus tuleb töötajal ise sellele mõelda. [19] Dokumentide kaitseks on teha vähemalt kolm varukoopiat, kahel erineval meediumil ja vähemalt üks füüsiline koopia. Selline viis muudab lunaraha väljapressimise riski kodukontoris palju väiksemaks.

1.3 Covid-19 mõju kodukontoris töötamisele

Covid-19 ehk koroonaviiruse pandeemia tabas aastal 2019 Wuhani, Hiinat. Koroonaviirus levis laialdaselt üle maailma ning aastal 2020 hakkasid firmad üle maailma inimesi suunama kaugtööle ehk kodukontorisse [40]. Eesti valitsus palus turvalisuse

tagamiseks kodust töötada ja kodukontorit rakendada [41]. Paljud ettevõtted on sunnitud oma kontorit ja reegleid ümber kujundama, et töötajad saaksid kodus töötada [22].

Veebikeskkonda kolimisega on organisatsioonid ja ettevõtted kogu maailmas rakendanud kodust töötamise (Work From Home) ärimudelit, mis suurendab ründeid ja riske firma siseandmetele. Enamikus stsenaariumides tähendab see töötajate nõuet kasutada oma isiklikke seadmeid ja koduvõrke, mis on oma olemuselt vähem turvalised ja millel puuduvad nõutavad standardite turvameetmed. [22]

Organisatsioonid peavad tagama, et kõik kasutatavad seadmed on täielikult kaitstud. Seetõttu peaksid kodukontoris töötavad inimesed saama haritud nende küberelu ja küberturvalisuse kohta, mitte ainult tavalise informatsiooni turvalisuse osas [2]. Mitmed allikad on välja toonud kolm peamist küberrünnakutüüpi, mis on pandeemia ajal kõige rohkem levinud – nendeks on andmepüük ehk *phishing*, pahavara ja DDoS (Distributed Denaial-of-Service) rünnakud [22,25,29].

Kaugtöö kasutusele võtt on toonud suure nõudluse virtuaalsetele ekraanidele, nt *Remote Desktop*. Kuigi kaheastmeline autentimine on ühenduste puhul enamasti nõutud ja VPN tihti kasutuses, unustavad kodukontori töötajad ära kõige tavalisemad turvalisuse õpetused. Avatakse erinevad meilimanuseid, kopeeritakse välistele andmekandjatele, edastatakse töö meile oma personaalsetesse arvutitesse või jagatakse dokumente, kellegagi kes neid näha ei tohiks. Kodus ei pöörata sellele nii palju tähelepanu või unustatakse sootuks. IT tiimidel ei ole piisavalt nähtavust kodukontoritele, et tagada turvalisus ja töötajat kaitsta. [40]

1.4 Rünnakute näited Covid-19 pandeemia ajast

Allpool tabelis 2 on välja toodud erinvad rünnakud Euroopa Liidu riikides. Valitud on vaid mõned näited ning arvesse võttes, et EL riikides on samad andmekaitse põhimõtted ja seadused (GDPR).

Kuupäev	**Riik**	**Rünnaku tüüp**	**Detailid**
Märts 2020	Tšehhi	Pahavara	Brno ülikoolihaiglat kui ühte Covid-19 testimislaborit riigis tabas küberrünnak ja nad olid sunnitud kogu oma IT-võrgu sulgema. [42]
Juuni 2020	Saksamaa	*Phishing*	Firma juhtkonnale, mis tegeleb kirurgiliste maskide jms. tootmisega, saadeti andmepüügi e-kirjad. Lingid viisid Microsofti veebilehena näivale võltslehele, kus paluti oma andmetega siseneda, ning seejärel need andmed varastati.[43]
Mai 2020	Eesti	*Phishing*	Eesti Keskkonnateenused AS nimel saadeti välja e-kirju, mis tegelikult olid saadetud küberkurjategijate poolt. Eesmärgiks oli õngitsus kampaania käigus paroole varastada. [44]
August 2020	Belgia, Prantsusmaa, Taani	DDoS	Mitmeid rünnakuid suunati erinevate finantsfirmade ruuteritele ja DNS taristule. Enamus rünnakuid olid DNS üleujutused ja kestsid mitmeid tunde, mille ajal ei olnud teenused kättesaadavad. [45]
Märts 2020	Saksamaa	DDoS	Kaugõppe platvormi Mebist rünnati esimesel koolipäeval. Süsteem ei töötanud mitu tundi ja õpilased ei saanud kaugõppes osaleda. [46]

Tabel 2. Rünnakute näiteid Covid-19 pandeemia ajal.

2 Metoodika

Käesoleva bakalaureusetöö andmete kogumine ja analüüs koosnes järgmistest etappidest:

- teooriale toetudes intervjuukava koostamine (Lisa 2)

- intervjuude läbiviimine tavatöötajatega

- intervjuude analüüsimine ja märksõnade välja kirjutamine

- intervjuude läbiviimine juhtkonnaga

- teooriale ja analüüsile tuginedes järelduste ning kokkuvõtete tegemine

Uurimus on kvalitatiivne ja kasutatud on intervjueerimismeetodit. Uuritud on kindlat valimit, kelleks on Eesti keskmise suurusega firma töötajad. Valitud ettevõte pakub erinevatele klientidele kõnekeskuse teenust ehk kliendituge. Samuti on oluline lisada, et valitud ettevõte on oma protsessidega kontoris GDPR-ga kooskõlas ja teadlik isikuandmekaitse seadustest.

Intervjuu osalejateks on valitud töötajad, kes puutuvad igapäevaselt kokku kõige rohkem andmetöötlusega ja on see tõttu kõige suuremaks riskigrupiks. Töötaja puutuvad kokku erinevate andmetüüpidega iga päev – nimi, isikukood, krediitkaardi andmed jms. Sealsete töötajate tööstaažid varieeruvad palju ning on võimalik uurida nii lühi kui ka pikaajalisi töötajaid. Selles intervjuus loetakse pika tööstaažiga inimeseks 2 aastat või kauem töötanud töötajat. Lisaks on intervjueeritud firmas kolme oma ala spetsialisti – juhatajat, IT juhatajat ning personali juhti. Selle eesmärgiks on koguda tausta ning erinevaid vaatenurki. Nende vastuseid on analüüsitud eraldi peatükis, kuna küsimused olid natuke erinevad (Lisa 4).

Intervjuu eesmärgiks on uurida erinevustest töötajate arusaamast kodukontoris töötamise turvalisusest ning millised on selle puudused. Intervjuu võimaldab uurida teemasid, mis ei ole muud moodi kättesaadavad. Pealt näha võivad kõik töötajad kodukontoris öelda, et nad jälgivad reegleid, kuid kui tagada neile anonüümsus ning uurida ausat vastust, siis on lootust leida ka erisusi. Andmeid kogutakse poolstruktureeritud intervjuuga, mis koosneb 10st küsimusest (Lisa 2). Poolstruktureeritud intervjuus kasutatakse avatud vastustega küsimusi. Avatud vastustega küsimusi kasutatakse siis, kui uurija soovib, et uuritavad

vastaksid oma sõnadega, kui uurija ei tea kõiki võimalikke vastusevariante või soovib saada uut informatsiooni uuritava nähtuse kohta [47].

Intervjuude toimumise ajaks oli märts – aprill 2021. Intervjuud toimusid Microsoft Teams-i keskkonnas, kuna pandeemia tõttu kokku saamine ei olnud võimalik. Kõik intervjuud on salvestatud. Lisaks toimusid intervjuud inglise keeles, kuna paljud töötajad on välismaalased ning ei räägi eesti keelt.

Saadud teave aitab tööandjatel teadlikumalt planeerida oma koolitusi vastavalt töötajate vajadusetele, samuti aitavad saadud andmed tööandjatel leida üles võimalikud kitsaskohad, millega edasi tegeleda, et kindlustada töötajate hea vastupanuvõime küberturvalisuse riskidele kodukontoris.

3 Analüüs

Selles peatükis tuuakse välja intervjuude [48] analüüs ja uuritakse erisusi intervjueeritavate vastustes. Intervjuu küsimused on leitavad lisast 2. Intervjuude analüüs toimub küsimuste kaupa nii nagu nad osadeks jaotatud on. Kuna intervjuud olid inglisekeelsed, on kõik vastused ümber tõlgitud eesti keelde.

Analüüsi põhjal saab uurimistulemused jagada kaheks: 1) erinevused tavatöötajate ja juhtkonna arusaamast informatsiooni turvalisusest kodukontoris ja 2) lahenduste pakkumine, milleni jõuti peale peamiste probleemide tuvastamist.

3.1 Tavatöötaja intervjuude analüüs

Tavatöötajate intervjuud tehti eesmärgiga koguda andmeid ja arvamusi kodukontori turvalisusest ning leida võimalikke kitsaskohti turvalisuses. Intervjuu tehti firma klienditoe spetsialistidega ehk agentidega (Tabel 3).

Intervjueeritav	**Vanus**	**Amet**	**Staaž praegusel ametikohal**
Vastaja 1	35	klienditugi	2 aastat
Vastaja 2	23	klienditugi	1 aasta
Vastaja 3	32	klienditugi	2 aastat
Vastaja 4	21	klienditugi	2 aastat
Vastaja 5	25	klienditugi	2.5 aastat
Vastaja 6	32	klienditugi	5 aastat
Vastaja 7	33	Administraator	1 aasta

Tabel 3. Intervjuu osalised.

Intervjuu teise osa küsimused keskendusid töötajate arusaamale üldisest informatsiooni turvalisusest. Intervjueeritavatel paluti öelda, miks nad firmas töötavad ning pakuti välja

ka võimalikke vastuseid. Eesmärgiks aru saada, kas selline põhjus võib mõjutada suhtumist firma informatsiooni turvalisusest ning tausta kogumiseks.

Vastustest tuli välja, et intervjueeritavatele, kes käivad samal ajal koolis, on see hea töökoht koolikõrvalt (vastajad 2 ja 4). Töötajad, kes on juba vanemad ning firmas kaua olnud, on ametipositsiooniga rahul ning neile meeldib see töö (vastajad 1, 5, 6, 7). Samuti toodi välja hea palk, mis on motiveeriv – „Ma olen rahul, sest saan siin töökohal sama palka, mida sain eelmises kohas, kus ma töötasin. Eelmisest kohast pidin ma ära tulema, sest tegu oli seisva tööga.“ (vastaja 2) ning karjääri edendamise võimalused.

Enamus vastajad tundsid ennast kindlalt turvalisuse määruste tundmises ning informatsiooni kaitsmises. Vastaja 7 tõi välja, et kindlasti oleks rohkem, mida teada, kuid tema töökohal on teadmistest piisavalt. Kõik töötajad vastasid, et on saanud vajaliku turvateadlikkuse koolituse, ilmselt põhjusel, et kõik töötajad on kohustatud seda läbima firmaga liitudes ning peavad seda iga aasta kordama.

Intervjuu kolmanda osa küsimused keskendusid otseselt kodukontoris töötamisele ning selle turvalisusele. Kõige pealt pidid intervjueeritavad vastama, kas nad elavad üksi või kellegagi koos. Üksinda elamise puhul oleks mitmed turvariskid palju väiksemad. Vastused jagunesid pooleks – 5 elab üksi ning 6 kellegagi koos.

Kõik intervjueeritavad töötavad praegu kodukontoris ning on seda teinud juba pikalt. Mõned töötajad said vahepeal käia kontoris, kuid pandeemia halvenedes liikusid nad tagasi kodukontorisse. Töötajad, kes liitusid firmaga pandeemia ajal ehk 2020 aasta jooksul, on firmas kohapeal käinud ainult koolituse ajal. See tähendab, et kontoris töötamise kogemus neil puudub (vastaja 2) – „Mul ei ole palju kontoris käimise kogemust, sest liitusin firmaga pandeemia ajal.“

Kodukontoris töötamise juures toodi välja nii plusse kui ka miinuseid. Plussidena toodi välja näiteks, et on rohkem aega oma asjadele hommikuti ja pauside ajal – „Ma ei pea bussiga hommikuti tööle minema, seega saan sellega rohkem vaba aega ja säästan raha.“ (vastaja 5), „Pauside ajal meeldib mulle suitsetamas käia, kuid kontoris võttis kaua aega treppides üles-alla käimine, ning ma kaotasin kogu oma pausi aja sellele.“ (vastajad 2, 3, 5). Miinustena leidsid vastajad, et tunnevad puudust kolleegide ja sõpradega suhtlemisel ning seda, et tähelepanu hajub kodus toimuvate asjade peale kiiremini.

Intervjuus üritati panna töötajaid tööandja rolli ja analüüsida, et milliseid miinuseid näevad nad sellest vaatepunktist. Vastajad 1, 2 ja 3 tõid välja, et ilmselt on tööandjal raskem jälgida kui hästi töötaja tööd teeb, ning kas töötaja päriselt on arvuti taga või on seal keegi teine. Vastaja 2 ütles – „Ma arvan, et kontoris olles on tööandjal lihtsam turvalisust kindlustada, aga kui me oleme kodus, siis nad ei saa meid kontrollida.“, ja vastaja 3 – „me peame ise kindlad olema, et hoiame informatsiooni turvaliselt ja rakendame vajalikke meetmeid.“. Vastaja 7 ütles vastupidiselt, et tema sellist probleemi ei näe ning tööstatistikast on näha, et kas töö on tehtud. Sellisel arvamusel oli ka vastaja 3, kes arvas, et kuna tööandja ei kaota töökvaliteedis, siis -„/../ töö saab tehtud, seega on tööandja ka võitja positsioonis“.

Enamus töötajaid vastasid, et nad on kursis ja teadlikud kodukontori võimalikest riskidest. Samas oli kuulda kahtlust mõne osalise vastustes – „Ma arvan, et teatud maani tean ohtudest ja ma alati üritan kindlaks teha, et ei jaga informatsiooni valesti.“ (vastaja 5). Sama vastaja lisas, et kuna ta kasutab koduinternetiühendust, siis peab ta selle jaoks tagama vastavad turvalisuse meetmed – parool jms.

Teema arenduseks paluti intervjueeritavatel mõelda kas nad on kodukontoris kokku puutunud mõne turvariskiga või kas nad on leidnud viise, kuidas oma töö lihtsamaks muuta. Vastajad 3 ja 5 tõid välja, et on avastanud süsteemis vea, mis nõuab neil dokumentide allalaadimist arvuti kõvakettale, kui need on vaja järgmisesse meili edasi saata. Kui dokument on edasi saadetud kustutavad kõvakettalt selle faili ära ning jätkavad tööd. Vastaja 5 ütles veel - „Kui mina oleks klient, siis ma ei tahaks, et minu pangaandmed või midagi sarnast laetakse alla kellegi isiklikku arvutisse.“ Vastaja 2 leidis viisi, kuidas ta ei pea 7 minutit tööd tegema ehk tema töönumber on hõivatud – „/../ kui inimene helistab ja ma ühendan tema kõne edasi teisele liinile ning panen siis pileti (töö ülesande) kinni, ei saa ma uusi kõnesid 7 või 8 minutit.“ Toodi välja ka seda, et kui arvutit ei kasutata isiklikuks tarbeks, siis on neil alati arvuti kõrval telefon, mis sisustab vaba aega. Kontoris olles ei ole telefonid tööalale lubatud, kuid kodus kasutatakse neid pidevalt. Pooled vastajatest tõid välja ka *phishing* meilide saamise (vastajad 3,4,6,7), kuid ütlesid, et kustutavad sellised meilid lihtsalt ära.

Mõned töötajad tunnevad ennast kodukontoris reegleid järgides kindlalt, kuid mõned arvavad, et nad teeks seda kontoris paremini. Vastaja 2 ütles, et ta on reeglitega leebem kodukontoris töötades, kuigi ta pole kontoris kaua töötanudki. Sarnaselt arvas vastaja 1,

kes tunneb, et kui tema tegevust ei jälgita, siis on tal kergem kõrvale kalduda. Intervjueeritav 3 ütles, et reegleid on tema arvates lihtne järgida, ning kui keegi tema tegemisi pidevalt ei kontrolli, teeb see ta töö vähem stressirohkeks. Vastaja 6 ütles, et ta üritab reegleid järgida sama hästi nagu kontoris. Aastate pikkuse tööstaažiga on tal välja kujunenud enda süsteem ning üritab seda kodukontoris ära kasutada. Teistsugusel arvamusel oli vastaja 7, kes arvas, et kodukontoris töötamine on turvalisem kui kontoris töötaimine. Ta põhjendas seda sellega, et kodus on ta üksi ning kontoris liigub ka teisi inimesi, kes võivad ohuks olla.

Lisaks küsiti soovitusi ja ideid, kuidas turvalisust kodukontoris edendada. Ideid oli erinevaid, kuid ühiseks jooneks oli koolituse soov (vastajad 1, 3, 5, 6) – „Ma tahaksin ennast kontrollida ja sellepärast oleks hea kui koolitus oleks kättesaadav kõigile.“ (vastaja 3), „Võib-olla oleks hea idee lisada kodukontori turvalisuse osa juba olemasolevale turvakoolitusele.“ (vastaja 6)

3.2 Juhtkonna intervjuu analüüs

Juhtkonna intervjuu tehti eesmärgiga koguda tausta ning leida võimalikke erinevusi tavatöötaja ja spetsialisti arvamuse vahel. Intervjuu tehti firma, personaliosakonna ning IT juhtidega (Tabel 4). Intervjuu küsimused on leitavad lisast 4.

Intervjueeritav	**Tööstaaž**
Firma juht	16 aastat
Personalijuht	7 aastat
IT juht	5 aastat

Tabel 4. Juhtkonna intervjuu osalised.

Kõik intervjueeritavad on firmas töötanud juba pikalt ning palju kauem kui tavatöötajad. Nii firma kui ka personalijuht osalesid firma turvalisuse määruste üles seadmisel ning on hästi kursis kõigi nõuetega. IT juht vastas samamoodi, et on kõigega hästi kursis.

Kõikidel paluti hinnata firma turvalisust nõrgast kuni tugevani. Firma juht ja personalijuht ütlesid mõlemad, et see on tugev, kuid IT juht, et ilmselt on see kuskil keskel. Kodukontorisse liikumisel arvas firma juht, et ta loodab, et turvalisus on samaks jäänud, kuid ei saa selles kindel olla. Personalijuht tõi aga välja, et „Turvalisus on kindlasti ohus,

sest meil ei ole selget pilti sellest, et millistes tingimustes meie töötajad tööd teevad.“ ja tõi välja keskkonna, taristu ning ühes ruumis töötavad inimesed.

Positiivseteks kodukontori pooleks ütlesid kõik, et on oluline pandeemia ajal töötajaid kaitsta ning see lahendus lubab inimestel kodus püsida. Miinusteks, et raske on näha mis kodukontoris tehakse ja turvalisuse tagamise – „/…/ taristu, mida me kasutame, ei ole tegelikult mõeldud kodukontori stsenaariumile, ja seetõttu võib see mõjutada üldist turvalisust.“ (firma juht), „/…/ vähem kontrolli, vähem ülevaadet turvalisuse üle, sest nii on meie tehnika üles seatud.“, „Mured on, et inimesed saavad teha kodus seda, mida nad ise tahavad.“ (IT juht), „Juhtkond peab muutuma töötaja kontrollimisest töötaja usaldamiseni.“ (personalijuht). Samuti lisasid kõik, et nad ei tea palju turvalisuse juhtumitest, millest oleks teada antud - „Me ei tea ühestki turvaintsidendist, mis kodus juhtunud on“ (firma juht), „Meile ei ole saadetud infot turvaintsidentidest.“ (personalijuht), „Tehniliselt võivad olla raportid, kuid päriselt ei ole võimalik teada, mis töötajate kodudes toimub.“ (IT juht).

Uuriti ka arvamust turvalisuse parandamiseks ja mis võib olla peamiseks ohuks firmas. Personalijuht tõi välja inimfaktori, mis on tema arvates kõige suuremaks probleemiks – „/…/ ei ole vahet, mis informatsiooni turvalisuse koolituse saad, aga alati on mainitud, et inimese viga on kõige suure risk või teadmiste puudumine. /../ Ma ei usu, et töötajad meelega seaks informatsiooni turvalisuse ohtu, kuid seal on puudulikud teadmised. /…/ Me peame nüüd iseennast (juhtkonda) usaldama, et me oleme selgeks teinud, mis informatsiooni turvalisus päriselt on.“

IT juht vastas infotehnoloogiliste aspektide poolest ning ütles, et valmisolek kodukontori olukorraks oli väga nõrk - „ See näitas kui ettevalmistamata me olime, meil ei olnud piisavalt VPN seadmeid ja me saime aru, et süsteem isegi ei kannataks nii suurt hulka inimesi samal ajal VPNi kasutamas.“ Ta lisas veel ühe kitsaskoha teatud programmis, mida kasutatakse - „Inimesed saadavad igasuguseid ID-kaarte meile, kuid programm, mida me kasutame, ei tööta õieti. Seega töötajad peavad ise mõnda ID-kaardi pilti parandama ja et seda teha, laevad nad kliendi ID kaardi mingisse pilve programmi, kus seda teha saab. “ Samuti tõi ta välja, et mõned töötajad on saanud oma töötelefonile spämm kõnesid – „Mõned meie töötajad on saanud kõne sisuga, et Swedbank on teie numbri politseisse andnud ning nüüd on vaja pangaandmeid.“

Erinevatel arvamustel oldi ka töötajate jälgimise osas kodukontoris - „Mina eelistan ekraani jälgimise programmi, et näha mida töötajad kodus arvutis teevad.“ (firma juht), „Mina ei soovita mitte mingisugust jälgimist, õiguslike põhjuste pärast. Eesti seaduse põhiselt on väga raske midagi sellist inimese kodus teha.“ (personalijuht).

3.3 Kodukontori lahendus uuritavas ettevõttes

Selles peatükis selgitatakse lühidalt, et milline on kodukontori lahendus uuritavas firmas (Tabel 5).

Firma kodukontorid on jaotatud viieks osaks, sest nii palju erinevaid kliente kasutab teenust. Lisaks on kõikide klientidega tehtud vähendatud turvameetmete lepingud, sest samu turvameetmeid, mida lubatakse tagada kontoris ei saa tagada kodus.

Klient	Lahendus
1	Riistvara pakub ettevõte, lubatud on isikliku riistvara kasutamine, kui see on vajalik (isiklikke arvuteid kasutavad ainult tavatöötajad). Juhatus ühendub firma Cisco VPN-iga. Tavatöötajate jaoks kasutatakse AWS VPN-i. Samuti kasutavad nad RDP-ühendust oma kontoriarvutiga.
2	Riistvara pakub firma ja juhatus ühendub firma Cisco VPN-iga. Mõne tavatöötaja jaoks on ka AWS VPN. Samuti kasutatakse RDP-ühendust kindlasse kontoriarvutisse. Agentidele võimaldas klient ise VPN ühenduse, kasutades selleks spetsiaalset *Work at Home* portaali.
3	Riistvara pakub ettevõte, lubatud on isikliku riistvara kasutamine, kui see on vajalik (isiklikke arvuteid kasutavad ainult tavatöötajad). Juhatus ühendub firma Cisco VPN-iga. Tavatöötajate jaoks kasutatakse AWS VPN-i. Samuti kasutavad nad RDP-ühendust oma kontoriarvutiga
4	Riistvara pakub firma ja kõik töötajad kasutavad Cisco VPN-i.
5	Riistvara pakub firma ja kõik töötajad kasutavad Cisco VPN-i.

Tabel 5. Kodukontori lahendused uuritavas ettevõttes.

3.4 Järeldused

Käesoleva töö raames uurisin informatsiooni turvalisuse riske kodukontoris. Intervjuud keskendusid sellele, millisena näevad kodukontoris töötajad selle turvalisusust, kuid sellest tuli välja ka üldisemaid probleeme, millega firma juhid peavad selles uudses olukorras tegelema. Väga palju mõjutab turvalisust töötajate suhtumine oma töösse ning nende teadmised sellest.

Kodukontori turvalisus uurimisteemana on keeruline, sest tegemist on võrdlemisi uue asjaga, mistõttu on sellele tausta ja toetava informatsiooni kättesaamine ka raskem. Siiski ei saa väita, et turvalisusest intervjuudest midagi teada ei saadud, vaid räägiti peidetud kujul, mis raskendas analüüsimist. Vastustega võidi olla pigem ettevaatlikud kui avatud, sest intervjuu läbiviijat ehk mind tajuti kui informatsiooni turvalisuse spetsialisti, kellena ma seal firmas töötan.

Materjali analüüsides leidis kinnitust see, et informatsiooni turvalisus ja teadlikkus sellest on kodukontoris väga olulised. Kõige enam toodi välja, et töötajad ise saavad olla enda kõige suuremad abimehed kodus ning koolituste abil on võimalik neid selleks treenida. Ühtlasi mõjutab töötajate emotsioon ja motivatsioon nende töö tegemise kvaliteeti ja vajalikke näitajaid. Tooksin välja ka selle, et suureks probleemiks on töötajate jälgimine kodukontoris, mis on seotud nii töö kvaliteedi kui ka turvalisusega. Samuti ollakse informatsiooni turvalisuse riskidest üldiselt kursis, kuid küberturvalisuse ja erinevate rünnakute kohta teatakse vähe. Kindlasti ei saa öelda, et töötajad oleks ebakompetentsed, vaid et kodukontoris töötades võiks olla teadlikum rünnakute sisust ning kuidas need toimivad.

Vestluste käigus ilmnes palju probleeme, mida ilmselt ei osata riskiks ise hinnata. Nt. kodu võrguühenduse kasutus, telefoni kasutamine tööajal, kõrvaliste isikute viibimine ruumis, tööjaoks mitte oluliste lehekülgede külastamine. Juhtkond eelistaks kindlasti, et kõik saaks kontorist tööd teha, kuid paljud töötajad ei näe kodukontoris mingit probleemi. Lisaks oli üks tavatöötaja arvamusel, et kodukontoris töötamine on turvalisem kui kontoris olemine, mis tegelikult ei klapi juhtkonna arvamusega.

Samuti saab välja tuua probleemi seoses turvaintsidentides mitte teatamisega. Juhtkonna arvamus probleemides teavitamisel oli ühtne, et kuna pole riske raporteeritud, siis järelikult need puuduvad. Tavatöötajate intervjuudest tuli välja aga mitu juhtumit, kus

toodi välja *phishing* kirjad, spämm ning näiteks isikuandmete kopeerimist arvutisse programmi vea tõttu. Seda arvesse võttes võib järeldada, et paljudest intsidentidest tööandjat ka ei teavitata, vaid tegeletakse nendega iseseisvalt.

Intervjuumaterjali analüüsi põhjal võib järeldada:

- Töötajad ise saavad olla enda kõige suuremad abistajad kodus ning koolituste abil on võimalik neid selleks ette valmistada. Firmad teevad enda poolt kõik võimaliku, et tagada turvaline taristu töö tegemiseks, kuid ülejäänu jääb töötaja enda teha.

- Infoturbe riskidest ollakse üldiselt teadlikud, kuid küberturvalisuse ja erinevate rünnakute kohta teatakse vähe.

- Kui ei ole koostatud ja selgitatud kindlat plaani, kuidas turvaintsidentidest teada anda, siis võivad need tihti tähelepanuta jääda.

- Töötajad võivad ennast kodukontoris töötades targemaks pidada kui tegelikult on ning võivad jätta tähelepanuta olulisi turvalisust mõjutavaid tegureid.

- Pikema ja lühema tööstaažiga töötajate vahel uurimuses erisusi välja ei tulnud ning mõlema puhul on koolitamine oluline.

4 Väljapakutav lahendus

Järelduste põhjal on välja pakutud lahendusena turvateadlikkuse koolitus kodukontoris töötajatele (Lisa 5).

4.1 Üldpõhimõtted

Täna on kasutusel palju kodukontori lahendusi ning sealseid ohte on praegustes koolitustes väga vähe kirjeldatud. Koolitus näitab, milline on turvaline kodukontor ning annab võimaluse tõsta tähelepanu. Samuti saab välja pakkuda lahendusi, et kodukontor turvalisemaks muuta. Lisaks on käsitletud analüüsi käigus välja tulnud probleeme nagu näiteks turvaintsidentidest teavitamine õigetesse kohtadesse. Koolituse nõueteni jõuti intervjuu analüüsi käigus ning järgnevate küsimustele vastates.

- Kas on rakendatud uusi tehnoloogiaid või määrusi, mis seavad kasutajatele uusi nõudeid, nt kaugtöö?
- Millised töötajad on minevikus infoturbeintsidentide suhtes käitunud / reageerinud ebapädevalt või üldse mitte?
- Kas on mobiilseadmete kasutajaid, kes on nt. oma arvuti nakatanud mingi viirusega USB-mälupulkade abil?
- Millised on turvaeeskirjade, määruste või turvasüsteemi standardite nõuded?
- Kas koolituse tegemise jaoks on nõudlust?

Meedia või suhtlemiskanali valimine turvateadlikkuse programmis lähtub selle eesmärgist - luua ja säilitada informatsiooni turvalisus kodukontoris. Õige koolituse jaotuskanali valimine on oluline, sest koolituse sisu peab jõudma kõigi töötajateni, kelle jaoks see vajalik on. Selle koolituse jaoks on valitud meediad vastavalt sellele, et töötajad peavad olema kodukontoris.

1. Läbi veebi tehtav koolitus koos koolitajaga (nt. Microsoft Teams-i keskkonnas)
2. Materjalide üleslaadimine jagatud kanalisse ning ise õppimine

4.2 Sihtgrupp

Koolituse sihtrühmaks on valitud ettevõttes agendid ehk klienditoe töötajad, kes töötavad enamasti kodukontoris ning on oma töö sisu tõttu kõige haavatavamad. Klienditoe

teenindajad peavad täielikult mõistma turvalisuse tähtsust ja järgima süsteemide kasutamise reegleid nii kodus kui ka kontoris.
Sihtrühma valik:

- Klienditoe esindajad
- Partneritoe agendid
- Tehnilise toe agendid
- Kasutajatoe agendid
- Help Desk agendid

4.3 Sisu

Kodukontori kasutajatel põhinev sihtrühm peab täielikult mõistma turvateadlikkust ning järgima reegleid ja eeskirju. Sihtrühm peab olema koolitatud turvaeeskirjade osas ning peab omama laia arusaama turvariskidest organisatsiooni infotehnoloogiliste ressursside ja süsteemide osas.
Teemad, mida sellisel koolitusel käsitleda:

- Informatsiooni ja vara vastutustundlik kasutamine kodus
  - Miks informatsiooni turvalisus?
  - Mida teeb ettevõte, et tagada informatsiooni turvalisus?
  - Mida saad sina teha, et hoida informatsioon turvaliselt ka kodus?
- Ühendused kodukontoris
  - WiFi
  - VPN
- Inimfaktor kodus
  - Ümbruskond
  - Sotsiaalne manipulatsioon
- E-posti turvalisus
  - *Phishing* – mõtle kaks korda enne kui avad
  - Ohtlikud lisad meilis
  - E-posti krüpteerimine ja konfidentsiaalsus
- Pahavara ja DDoS teadlikkus
  - Nuhkvara
  - Tarkvara installeerimine
- Mobiilsete seadete turvalisus

    - Ühendused, turvalisuse sätted
    - Kuidas muuta oma seade turvalisemaks
- Turvaline süsteemide kasutamine
    - IT varade kasutamine
    - Ligipääsu load ja õigused
    - Tarkvara installeerimine
    - VPN ja krüpteerimine
- Autentimine
    - Salasõna turvalisus
    - Hea salasõna leidmine
- Turvaintsidentidest teavitamine
    - Mis on turvaintsident?
    - Kuidas sellest teada anda?

4.4 Eeldatav tulemus

Projekt on planeeritud läbi viia uuritavas ettevõttes juunikuu jooksul kõikidele tavatöötajatele läbi Microsoft Teams-i keskkonna. Koolituse heaks tulemuseks on töötajate teadlikkuse parandamine kodukontori turvalisusest ning turvaintsidentidest teavitamise juurutamine. Samuti on plaanis koostada „korduma kippuvad küsimused“ leht, et muuta kodukontoris turvalisuse teadmised kättesaadavamaks. Projekti tulemusi on plaanis kontrollida koostades anonüümse tagasiside küsitluse koolituse läbinud töötajatele, kus nad saavad hinnata oma teadmisi enne ja pärast ning vastata, kas koolitus oli nende jaoks vajalik. Tulemused näitavad ettevõttele projekti tõhusust ja selle vajalikkust. Tulevikus on plaanis lisada kodukontori ja tavaline turvalisuse koolitus ühte ning koostada programm, kus kõigil oleks võimalus oma teadmisi aeg-ajalt värskendada.

Kokkuvõte

Hiljutise koroonaviiruse pandeemia puhkemisega ja andmetöötluse kasvamisega on võrgus töötavate kasutajate arv palju suurenenud. Veebikeskkonda kolimisega on organisatsioonid ja ettevõtted kogu maailmas rakendanud kodust töötamise ärimudelit, mis suurendab ründeid ja riske firma siseandmetele.

Selles uurimuses on analüüsitud andmetöötlemisega tihedalt seotud töötajate igapäeva elu kodukontoris ning kuidas nemad ennast sellises uudses olukorras tunnevad. Samuti on analüüsitud peamisi ohte, mida on pandeemia olukorras väga oluline tunda ja vältida. Sellised küberturvalisuse ohud on põhjustanud tõsiseid privaatsusprobleeme ja andmeturvalisuse ohte.

Teooriaosas käsitlen informatsiooni turvalisust üldiselt ning peamised riskitegureid. Uurin erinevusi kontoris ja kodukontoris olevate riskide vahel ja millele võiks kõige rohkem tähelepanu pöörata. Uurimuses on analüüsitud erinevaid küberrünnakuid ning on tehtud analüüs ühe andmetöötlemisega seotud firma kodukontori turvalisusest.

Analüüsi põhjal võib järeldada:

- Töötajad ise saavad olla enda kõige suuremad abistajad kodus ning koolituste abil on võimalik neid selleks ette valmistada. Firmad teevad enda poolt kõik võimaliku, et tagada turvaline taristu töö tegemiseks, kuid ülejäänu jääb töötaja enda teha.

- Infoturbe riskidest ollakse üldiselt teadlikud, kuid küberturvalisuse ja erinevate rünnakute kohta teatakse vähe.

- Kui ei ole koostatud ja selgitatud kindlat plaani, kuidas turvaintsidentidest teada anda, siis võivad need tihti tähelepanuta jääda.

- Töötajad võivad ennast kodukontoris töötades targemaks pidada kui tegelikult on ning võivad jätta tähelepanuta olulisi turvalisust mõjutavaid tegureid.

- Pikema ja lühema tööstaažiga töötajate vahel uurimuses erisusi välja ei tulnud ning mõlema puhul on koolitamine oluline.

Samuti valmis uurimistöö raames koolitus turvateadlikkuse tõstmiseks kodukontoris, mis on koostatud lähtuvalt ühe ettevõtte vajadustest, kuid on kasutatav ka mujal. Koolituses on välja toodud üldised informatsiooni turvalisuse tagamise võtted, kuid samas on keskendutud rohkem kodukontori ohtudele ja nende tuvastamisele.

Bakalaurusetöö uurimisteema on aktuaalne, kuna varasemad uuringud keskenduvad pigem firma informatsiooni turvalisusele kontoris. Samuti on teema oluline, kuna pandeemia ajal on vaja, et inimesed saaksid tööd teha kodust ning seda turvaliselt. Lisaks tõestas pandeemia aeg tervele maailmale, et kodukontorite lahendus on täiesti võimalik töötegemise viis ning paljud firmad saavad seda ka edaspidi kasutada. Selle töö raames on võimalus igal tööandjal analüüsida enda firma kitsaskohti ning vajadusel välja töötada koolitus töötajate tähelepanu tõstmiseks.

Kasutatud kirjandus

1. Bonacini L, Gallo G, Scicchitano S. Working from home and income inequality: risks of a ‘new normal’with Covid-19. Journal of population economics. 2021.

2. Ahmad T. Corona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity. 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3568830 (15.03.2021)

3. Bourgeois, David T.; Smith, James L.; Wang, Shouhong; and Mortati, Joseph, "Information Systems for Business and Beyond" (2019). *Open Textbooks*. 1. https://digitalcommons.biola.edu/open-textbooks/1

4. Dokuchaev VA, Maklachkova VV, Statev VY. Classification of personal data security threats in information systems. 2020. https://cyberleninka.ru/article/n/classification-of-personal-data-security-threats-in-information-systems/viewer (15.03.2021)

5. Whitman, Michael E. INFORMATION SECURITY. COMMUNICATIONS OF THE ACM. 2003. https://www.researchgate.net/publication/220422187_Enemy_at_the_gate_threats_to_information_security (16.03.2021)

6. Bell, B.S.; Kozlowski, S.W.J. A typology of virtual teams: Implications for effective leadership. *Grade Organ. Manag.* 2002.

7. Hesketh, I.; Cooper, C.L. *Wellbeing at Work: How to Design, Implement and Evaluate an Effective Strategy*; Kogan Page: London, UK, 2019.

8. Kurland, N.B.; Bailey, D.E.; Kurkland, N.B.; Bailey, D.E. Telework: The advantages and challenges of working here, there, anywhere, and anytime. *Organ. Dyn.* 1999.

9. Bailey, D.E.; Kurland, N.B. A review of telework research: Findings, new directions, and lessons for the study of modern work. *J. Organ. Behav.* 2002.

10. Anderson, A.J.; Kaplan, S.A.; Vega, R.P. The impact of telework on emotional experience: When, and for whom, does telework improve daily affective well-being? *Eur. J. Work Organ. Psychol.* 2015.

11. Stich, J.-F. A review of workplace stress in the virtual office. *Intell. Build. Int.* 2020.

12. Charalampous, M.; Grant, C.A.; Tramontano, C.; Michailidis, E. Systematically reviewing remote e-workers' well-being at work: A multidimensional approach. *Eur. J. Work Organ. Psychol.* 2019.
13. Jackson, P.J. *Virtual Working: Social and Organisational Dynamics*; Routledge: London, UK, 1999.

14. Mitchell, D. *50 Top Tools for Employee Engagement: A Complete Toolkit for Improving Motivation and Productivity*; Kogan Page: London, UK, 2017.

15. Vyas L, Butakhieo N. The impact of working from home during COVID-19 on work and life domains: an exploratory study on Hong Kong. Policy Design and Practice. 2020.

16. Malecki F. Overcoming the security risks of remote working. Computer Fraud & Security. 2020. https://www.sciencedirect.com/science/article/abs/pii/S1361372320300749 (15.04.2021)

17. Bendiab G, Grammatikakis KP, Koufos I, Kolokotronis N, Shiaeles S. Advanced metering infrastructures: security risks and mitigation. InProceedings of the 15th International Conference on Availability, Reliability and Security. 2020. https://core.ac.uk/download/pdf/334597145.pdf (28.04.2021)

18. 'How much would a data breach cost your business?'. IBM. www.ibm.com/security/data-breach (28.04.2021)

19. Pandya LB. Cyber Security" When Working From Home. Emerging Trends in Commerce & Management.:36. 2020.

20. Deogirikar J, Vidhate A. Security Attacks inIoT: A Survey.

21. National Cyber Security Centre (NCSC) and Cybersecurity and Infrastructure Security Agency (CISA). Covid-19 exploited by malicious cyberactors. https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory (15.04.2021)

22. Pranggono B, Arabo A. Covid-19 pandemic cybersecurity issues. Internet Technology Letters. 2020. https://onlinelibrary.wiley.com/doi/full/10.1002/itl2.247 (10.04.2021)

23. Crown Prosecution Service. Cybercrime - prosecution guidance. https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance (15.04.2021)

24. Khan NA, Brohi SN, Zaman N. Ten deadly cyber security threats amid Covid-19 pandemic.https://www.techrxiv.org/articles/preprint/Ten_Deadly_Cyber_Security_Threats_Amid_Covid-19_Pandemic/12278792/1 (15.04.2021)

25. NETSCOUT. Netscout threat intelligence report. DDoS in a Time of Pandemic. 2021 https://www.netscout.com/threatreport (28.04.2021)

26. Continelli, A., 2017. Business.com. https://www.business.com/articles/aaron-continelli-identify-and-prevent-software-failure/ (04.05.2021)

27. Blyler J. 2020 Software Failures Linked to COVID-19. designnews.com. 2020 https://www.designnews.com/design-software/2020-software-failures-linked-covid-19 (04.05.2021

28. ENISA. Main incidents in the EU and worldwide. 2020. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents (29.04.2021)

29. Georgiadou A, Mouzakitis S, Askounis D. Working from home during Covid-19 crisis: a cyber security culture assessment survey. Security Journal. 2021.

30. Okereafor K, Manny P. 2020. Understanding Cybersecurity Challenges of Telecommuting and Video Conferencing Applications in the COVID-19 Pandemic.

31. Some examples of deliberate threats Espionage or trespass Espionage or trespass | Course Hero Coursehero.com. 2019. https://www.coursehero.com/file/p6pseesf/Some-examples-of-deliberate-threats-Espionage-or-trespass-Espionage-or-trespass/ (04.05.2021)

32. Jäntti M. Studying Data Privacy Management in Small and Medium-Sized IT Companies. In2020 14th International Conference on Innovations in Information Technology (IIT) 2020. IEEE. https://ieeexplore.ieee.org/abstract/document/9299050 (16.03.2021)

33. Deogirikar J, Vidhate A. Security Attacks inIoT: A Survey.

34. Pilk mobiilioperaatori igapäevaellu: Elisa. Forte. 2016. https://forte.delfi.ee/artikkel/75478787/pilk-mobiilioperaatori-igapaevaellu-elisa (12.05.2021)

35. Queensland government. What is an information technology risk. Business.qld.gov.au. 2020. https://www.business.qld.gov.au/running-business/protecting-business/risk-management/it-risk-management/defined (04.05.2021)

36. Allen M, Peterson KE. Information Security and Counterintelligence. InThe Professional Protection Officer. Butterworth-Heinemann. 2020.

37. http://termin.eki.ee/esterm/concept.php?id=11128&term=v%E4ljapressimine

38. Monson K. 4 Reasons to Pay Attention to Technology Obsolescence | CSI. CSI. 2018. https://www.csiweb.com/what-to-know/content-hub/blog/4-reasons-to-pay-attention-to-technology-obsolescence/ (04.05.2021)

39. Young A. Cryptovirology: Extortion-Based Security Threats and Countermeasures.

40. Borkovich DJ, Skovira RJ. WORKING FROM HOME: CYBERSECURITY IN THE AGE OF Covid-19. Issues in Information Systems. 2020. http://www.iacis.org/iis/2020/4_iis_2020_234-246.pdf (10.04.2021)

41. Liikumispiirang, eneseisolatsioon, karantiin | Terviseamet [Internet]. Terviseamet.ee. 2021. https://www.terviseamet.ee/et/liikumispiirang-eneseisolatsioon-karantiin (10.04.2021)

42. Cimpanu C. Czech hospital hit by cyberattack while in the midst of a Covid-19 outbreak. 2020. https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/. (28.04.2021)

43. Lyngaas S. Hackers target senior executives at German company procuring PPE. https://www.cyberscoop.com/germany-ppe-coronavirus-hackers-ibm/. (28.04.2021)

44. Liive R. Eestis mai lõpus toimunud õngitsuskampaania on saanud vähemalt seitse järellainet | Digigeenius. Digigeenius. 2020. https://digi.geenius.ee/rubriik/uudis/eestis-mai-lopus-toimunud-ongitsuskampaania-on-saanud-vahemalt-seitse-jarellainet/ (06.05.2021)

45. Cimpanu C. European ISPs report mysterious wave of DDos attacks. 2020 https://www.zdnet.com/article/european-isps-report-mysterious-wave-of-ddos-attacks/ (28.04.2021)

46. Kurpeev O, Badovksaya e. DDoS attacks in Q1 2020. Securelist.com. https://securelist.com/ddos-attacks-in-q1-2020/96837/ (06.05.2021)

47. Virkus S. Intervjuu liigid | Intervjuu, vaatlus ja sisuanalüüs. Tlu.ee. 2021 https://www.tlu.ee/~sirvir/Intervjuu_vaatlus_ja_sisuanals/intervjuu_liigid.html (28.04.2021)

48. Borodin, B. Intervjuud kasutajatega. Salvestatud veebruarist maini 2021 Teamsis.

Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks[1]

Mina, Belinda Borodin

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "Turvateadlikkuse koolitus kodukontoris töötajatele", mille juhendaja on Kaido Kikkas.
   1.1. reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
   1.2. üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
2. Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.
3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

10.05.2021

1 Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil. Kui lõputöö on loonud kaks või enam isikut oma ühise loomingulise tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtajaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. ja 1.2, siis lihtlitsents nimetatud tähtaja jooksul ei kehti.

Lisa 2 – Poolstruktureeritud intervjuu plaan

1. part: Overall Information
Gender:
Age:
Position:
How long have you worked in this position:

2. part:
What is the reason you are working here? Is it studies, you like this job or something else?

How familiar are you with security guidelines in the company and how to protect information? Have you received any training for that?

Do you live alone or with someone else?

3. part: Working from home

How long have you worked from home?

What are the pros and cons about working from home?

What disadvantages do you see for employers in regards of working from home? If any?

Are you familiar with cybersecurity issues that can appear in working from home scenarios, like misuse of personal data, document management, wrong application use, phishing scams, malware etc?

Have you encountered any security issues during work from home process as described in the previous question? Or have you discovered any loopholes to make your job easier knowing it is actually not good for security?

Do you follow the same rules as in the office? Or are you easier with them at home?

How can the management make data security more efficient?

Would you agree with the statement that human error is the biggest risk to cybersecurity?

Lisa 3 – Informatsioonileht intervjuus osalejatele

Hi everyone,

I am TalTech university student Belinda, and I am currently working on my bachelor's thesis. I am also working as your Local Information Security Officer and maybe you remember me from the security training. I am looking for **agents** for my thesis who are willing to do an interview with me about working from home security. I will need about 10-15 agents and both short-time and long-time employees who are willing to answer a couple of questions.

The information obtained will help employers to better plan their training according to the needs of their employees. It will also help employers to identify possible lacking in security that need to be addressed in order to ensure that employees are well resilient to cyber security risks in the home office.

The results of the research are published in a generalized form. You are guaranteed anonymity and confidentiality. Your name is known only to me as the researcher, and you can always cancel your participation if you wish. The interview can be done in person or by a Teams meeting.

If you are interested or have any questions, please write to my personal e-mail: belinda.borodin@gmail.com and put the subject: "interview". I am grateful for participation!

Thank you,

Belinda

Lisa 4 – Intervjuu küsimused juhtkonnale

1. part: Overall Information
Gender:
Position:
How long have you worked in this position:

2.part:
How familiar are you with security guidelines in the company and how to protect information?

Where would you rank overall security in the company from low to high? Has it changed during work from home?

3. part: Working from home

What are the pros and cons about working from home?

What disadvantages do you see for employers and management in regard to work from home? If any?

Are you familiar with cybersecurity issues that can appear in working from home scenarios, like misuse of personal data, document management, wrong application use etc? Are there any reported incidents or concerns from employees?

What are the main changes you saw during the work from home process?

Do you have any ideas on how to make data security more efficient in the company?

Would you agree with the statement that human error is the biggest risk to cybersecurity?

Lisa 5 – Koolituse kava

Turvateadlikkuse koolitus kodukontoris töötajale

1

Tere tulemast informatsiooni turvalisuse valdkonda!

- **Miks informatsiooni turvalisus?**
  - Ettevõte on sõltuv informatsioonistning kuidas seda kaitstakse
  - Me puutume kokku erinevat tüüpi informatsioonigaiga päev- avalik, sisemine, konfidentsiaalne, väga konfidentsiaalne ja kliendi andmed
  - Kliendid panustavad sellele, et meie oskame informatsiooni turvaliselt ja õigesti kaitsta
- **Millekssee koolitus?**

Tihti kaob informatsiooni turvalisuse vajalikkus muu tegevuse taha ära. Eriti kodukontoris töötades on oluline meeles pidada, kuidas informatsiooni kaitsta.

See koolitus pakub nõuandeid, mida sina saad teha, et informatsiooni kaitsta. Samuti saad teada erinevatest rünnakutest ning kuidas neid ära tunda.

Mida teeb firma, et tagada turvalisus kodus?

Tööandja ülesandeks on tagada omalt poolt kõik võimalikud turvalisuse meetmed.

Vahendid, mida tööandja pakkuda saab:

- Turvaline ühendus töövõrkudesse, nt VPN, serverid
- Riistvara, mis on juba sätestatud vastava turvameetmetega (tulemüürid, viirusetõrjejms.)
- Reeglite ja määruste kehtestamine
- Töötajate koolitamine
- Kättesaadavusabile

3

Peamised küberohud kodukontoris ja kuidas nendega hakkama saada

4

Inimfaktor kodukontoris

Sotsiaalne insener on kurjategija, kes tugineb suuresti suhtlusele, mis hõlmab inimeste manipuleerimisttavapäraste turvaprotokollide, protseduuride ja parimate tavade eiramiseks. Eesmärgiks on rahalise või muu kasu saamiseks pääseda juurde arvutisüsteemidele, võrkudele või füüsilistele asukohtadele.

Läbi inimese on küberkriminaalil kõige lihtsam salastatud andmeteni jõuda ja seega peab töötaja kodus eriti tähelepanelik ja teadlik olema.

Andmepüük ehk *phishing 1/2*

Mis see on?

- Petlikude-kirjad, mis väidetavaltpärinevad tuttavatelt ettevõtetelt et inimesed avaldaks oma isiklikkeandmeid (paroole, krediitkaardiandmeid)
- Küberkurjategijadkasutavad kodukontorit ja pandeemiat enda kasuks teeseldes valitsusorganisatsioonidena tervishoiuna, muude olulisteisikutena
- Kirjad võivad tunduda väga reaalsed ning brändile vastavad

Kuidasära tunda?

- Välimuseltsarnane hea mainega organisatsiooni sõnumitele
- Tundub pakiline või proovib hirmu levitada
- Nõuab lisada olulist teavet või uudiseid
- Palub manused alla laadida või millelegi klõpsata

Andmepüük ehk *phishing 2/2*

Kuidas ennast kaitsta?

- Analüüsi enne oma andmete jagamist põhjalikultsaadetud sõnumi sisu ja asjakohasust
- Mitte kunagi ära jaga oma isiklikevõi tööga seotud andmeid meiliteel.
- Väldi meile, mis käsivad sul kohe tegutseda.
- Otsi kirjaviguja valestisõnastatud lauseid.
- Kontrolli saatja meiliaadressi, eriti saatja domeeni.
- Kontrolli linkienne selle avamist.
- Ole ettevaatlikkolmandate osapoolte allikade suhtes, kes levitavad teavet COVID-19.
- Kaitse oma seadmeid – installirämpsposti-,spämi- ja viirusetõrjetarkvara
- Hoidke oma süsteemid värskendatult

Pahavara 1/2

- **Mis see on?**
  - Tegemisttarkvaraga, mis on kirjutatud eesmärgil teha midagi halba informatsioonile, seadmetele või inimestele
  - Sinna hulka kuuluvad nt. viirused, trooja hobused, ussid, juurkomplektid, nuhkvara, lunavara
  - Pahavara võib varastada seadmetest isikuandmeid, salasõnu, finantsalaseid andmeid jpm.
- **Kuidas pahavaralevib?**
  - Varjatud pahavara sisaldava tasuta tarkvara allalaadimiselInternetist
  - Varjatud pahavaraga kombineeritud ehtsa tarkvara allalaadimisel
  - Pahavaraga nakatunud veebisaidikülastamisel
  - Klikkimiselvõltsitud veateatel või hüpikaknal, mis käivitab pahavara allalaadimise
  - Pahavara sisaldava meilimanuse avamisel

Pahavara 2/2

Kuidas ennast kaitsta?

- Värskenda oma arvutit.
- Kui võimalik, ära kasuta administraatori kontot.
- Mõtle hoolikaltjärele, ennekui mõnel lingil klõpsad ja midagi alla tõmbad.
- Oleme meilimanusteavamisega ettevaatlik.
- Ära usalda hüpikaknaid, mis paluvad tarkvara alla laadida.
- Piira failijagamist
- Kasuta viirusetõrjetarkvara

DDoS ehk *Distributed Denial of Service* rünnakud

Mis see on?

- Hajutatud teenuse keelamise(DDoS) rünnak on pahatahtlik katse häirida sihitud serveri, teenuse või võrgu tavapärast liiklust, ujutades üle sihtmärgi või selle ümbritseva infrastruktuuri Internet-liikluse
- Rünnak pannakse toime pahavaraga nakatunud arvutite abil. Kasutaja ei pruugi sellestisegi teadlik olla.
- Rünnakud suunatud tervishoiule, kaugtöö ja õppe tegemistvõimaldavateleplatformidele

Kuidasennast kaitsta?

- Uuenda oma tarkvara
- Võimalusel muuda veebilehedstaatiliseksvõi kasuta veebipuhvrit
- Kaitse veebivormeCAPTCHA abil
- Kasuta veebitulemüüri
- Võimalusel piira välismaistliiklust

Näited rünnakutest pandeemia ajal

Kuupäev	Riik	Rünnaku tüüp	Detailid
Märts 2020	Tšehhi	Pahavara	Brno ülikoolihaigla kui ühte Covid-19 testimislaboritiigis tabas küberrünnakja nad olid sunnitud kogu oma IT-võrgu sulgema.
Juuni 2020	Saksamaa	Phishing	Andepüügi meilid saadeti firma juhtkonnale, mis tegeleb kirurgiliste maskide jms tootmisega. Lingid viisid võltsile Microsoft lehele, kus palutioma andmetegasisse logidaning seejärelneed andmedvarastati.
August 2020	Belgia, Prantsusmaa, Taani	DDoS	Mitmeid rünnakuid suunati erinevatefinants firmade ruuteriteleja DNS taristule. Enamus rünnakuid olid DNS võimendusedja kestsid mitmeid tunde, mille ajal ei olnudteenusedkättesaadavad.
Märts 2020	Saksamaa	DDoS	Kaugõppeplatvormi Mebist rünnati esimeselkoolipäeval. Süsteem oli maas mitu tundija lapsedei saanudkaugõppesosaleda.

BYOD ehk *Bring Your Own Device* ehk Võta oma seade kaasa

Mis see on?

- Kaugtöö tegemiselon võimalus ettevõttel pakkuda omaltpoolt riistvara või töötaja peab kasutama enda riistvara ehk BYOD lahendust.
- Oma seadmel on tavaliselt nõrgemad turvameetmed, ettevõtteandmed jäävad töötaja isiklikkuseadmesse, töötaja saab vabalt tarkvara allatõmmata ja suvalisi veebilehti külastada.
- Ligipääs ohtlikutelevõrkudele (WiFi)

Kuidas käituda?

- Kustuta ebavajalikt tööga seotud informatsioon ära ja mõtle sellelekoguaeg
- Teavita kohe tööandjat, kui seade on kadunud või varastatakse
- Kasuta VPNi firma võrkudegaü ühendumiseks
- Kasuta tugevaid paroole igalpool ja vaheta neid iga 3 kuu järel
- Kahe-astmelineautentimine ja lõpp-punktide turvalisus

Mida saab töötaja ise selleks ära teha, et tema kodukontor oleks turvaline?

Ühendused kodukontoris

Esimeneasamnkodukontorigeaks olematurvalisvõrguühendusloomine.

Wi-Fi
Kui võimalik kasuta ühenduseks kaablit. Kui sa kasutad oma kodu Wi-Fi võrku, siis veendu, et su ruuteril oleks tugev salasõna ning et võrk oleks krüpteeritud.

VPN
Kohtades, kus ainult avalikud võrgud on saadaval, peaks kasutama VPNi ühendust informatsiooni jagamisel. VPN võimaldab luua turvalise ühenduse sinu koduvõrgu ja töövõrguga.

Kiirus
Veendu, et sul on piisavalt hea ja kiire ühendus oma töötülesannete tegemiseks.

Dokumentide ja informatsiooni haldus 1/2

Kõik, kestegelevad **andmetega** või anna va **digipääsu informatsioonile**, peaksi **d**egemaeda **turvaliselt** ja olemateadlikuoma kohustuse **teatsta** informatsiooni

Ainult need, kes peavadteadma
Jaga informatsiooni ainult valitud publikule . Informatsiooni jagades, pea meeles, kes seda päriselt teadma peab.

Kesskond
Ole tähelepanelik oma kesskonna ja ümbritsevate faktorite suhtes. Õnta välttida ka kodus teiste inimeste pealtkuulamist või salastatud dokumentide paljastamist.

Sotsiaalne suhtlus
Ära avalda enda kohta privaatseid andmeid võõrastele, et välttida sotsiaalse suhtluse tõttu tekitatud ohte. Pea meeles, keegi ei tohi küsida su paroole.

Dokumentide ja informatsiooni kasutamine 2/2

Puhas laud
Hoia oma laud puhas, eritt kodus, et vältida kolmandale isikule konfidentsiaalse teabe paljastamist.

Holustamine
Hoia oma dokumente ja faile turvalises kohas, näiteks ettevõtte poolt jagatud turvalises kaustas või ketta peal. Ära hoia töö dokumente oma isiklikku arvuti kõvakettal.

Prügi
Kustuta või viska ära kõik salastatud infot sisaldavad dokumendid, et vältida nende sattumist valedesse kätesse.

Turvaline süsteemide kasutamine

Logi sisse / Logi välja
Logi sisse ainult töö ajal ja ära kasuta arvutit töövälja muudeks tegevusteks.

Lukusta oma arvuti
Pane oma arvuti lukku, kui selle juurest lahkud. Nii hoiad dokumendid ja informatsiooni kolmanda isiku eest turvaliselt.

Installi värskendused
Uuenda oma süsteeme ja hoia kõik vajalikud rakendused asjakohastena.

Süsteemi seaded
Ära muuda töövarustl mingeid seadeid. Need on IT tiimi poolt sätestatud ning annavad oma panuse turvaliseks arvuti kasutuseks.

Mobiilsete seadmete haldus 1/2

Mobiilsedeadmedon vahendidmillegaaadinformatsioonendagakaasaõtta, ntarvuti,telefonjms.

Krüpteeritud andmed
Hoia oma informatsiooni krüpteeritud kujul (telefonis, arvutis, USB pulgal jne)

Turvalisuse sätted
Configure security setting of your mobile device (automatic locking and PIN), if not already pre- configured by your IT department.

Uuenda ja varunda
Uhenda oma seade turvalisse võrku (nt. VPN abil) ja varunda regulaarset oma mobiilset seadet. Samuti peavadkõik seadmed olema värskendatud ja uusima tarkvara peal.

Ümbruskond

Kodukontorianolulinerusaada, milline on **ümbruskond**ja kuidasee turvaliseks**muuta**.

Asukoht
Kodukontor on kodus töötamiseks, kohvik või muud avalikudkohad ei ole head. Kui kodus ei saa töötada, siis kindlasti avalikus kohas kasutada enda isiklikku võrguühendust.

Inimesed sinu ümber
Koht, kus sa töötad peaks olema üles seatud nii, et keegi ei saaks sinu tegemisi pealt vaadatatega kuulata su vestlusid.

Lisa turvameetmed
Tegeledes salastatud infoga, pead sa kindel olema, et keegi teine sinu tööd ei näe. Sule uksed ja aknad kui vaja ning väldi sotsiaalseerumist.

Mobiilsete seadmete haldus 2/2

Seadme lukk
Pane oma seade lukku alati, kui sa seda ei kasuta.

Wi-Fi
Uhenda oma seade ainult usaldusväärsetesse võrkudesse. Avalikud WiFi punktid (nt. kohvik) ei ole turvalised ühendused.

Bluetooth
Lülita Bluetooth ühendus välja, kui seda ei kasutata.

Anna teada
Anna teada kohe kui sinu seadmega midagi juhtub, nt läheb kaduma või varastatakse.

Salasõna turvalisus 1/2

Tugeva salasõna parimkaitse erinevate küberrünnakute eest, mida on võimalik teha.

Vaheta

Vaheta oma paroole pidevalt, et muuta parooli ära arvamine raskemaks. Ütti siis, kui kahtlustad, et keegi on sinu salasõnast teadlik.

Keerulisus

Kasuta keerulisi salasõnu. Keerulised salasõnad on vähemalt 10 tähemärki pikad ja juhuslikud kombinatsioonid tähtedest ja numbritest.

Tuttavad sõnad

Ära kasuta tuttavaid sõnu, mida on sinuga lihtne seostada. Nt: Sinu nimi, sünnikuupäev, perekliikmete nimed jne.

Salasõna turvalisus 2/2

Erinevad paroolid

Kasuta erinevaid paroole oma töö ja sotsiaalmeedia kontodel. Nii väldid ohtu, et kui üks parool on teada, siis kurjategija ei pääse ligi sinu teistele kontodele.

Jagamine

Ära jaga oma paroole kellelegi ning ära kirjuta neid üles. Kohe kui arvad, et keegi on sinu salasõnast teadlik, siis anna sellest töödandjale teada.

Brauser

Ära kasuta veebilehtedel funktsiooni "mälleta mu parooli". See annab suure eelise küberkriminaalidele juhul, kui nad su arvutile ligi pääsevad.

Turvaintsidentidest teavitamine

Turvaintsidendi ja kahtluse korral kindlasti töödandja abole manendest teadlik ja ülesse andmata stavaprotsessi kendeteavitamiseks.

Teavitamine

Anna intsidentidest teada kindlaks määratud inimesele. See võib olla sinu ülemus või keegi IT firmist.

Abi

Kui sa kahtled, kas tegu on turvaintsidendiga, siis küsi abi ja nõu. Ära jäta probleemi või küsimust vastuseta. Pigem kontrolli, kui kahetse.

Toeta

Osale aktiivselt turvaintsidentide lahendamises. Iga töötaja peaks andma oma panuse ettevõtte turvalisemaks muutmisel.

Meelespea!

- **Turvaline WiFi ühendus.** Muuda ka oma WiFi parool keeruliseks.
- Täielikult uuendatud viirusetõrje.
- Ajakohane turvatarkvara.
- Pea meeles oma andmeid varundada.
- Lukusta oma ekraan kui sa oma arvuti juurest lahkud.
- Ole kindel, et sul on turvaline ühendus oma töövõrguga (VPN).
- Kasuta andmete jaoks krüpteerimistarkvara
- Kasuta raskeid paroole.

22

Aitäh, et osalesid!

Kasutatud kirjandus

1. ENISA. Understanding and dealing with phishing during the COVID-19 pandemic. Enisa.europa.eu. 2020. https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic
2. Arvuti kaitsmine pahavaraeest. Support.google.com. 2020. https://support.google.com/google-ads/answer/2375413?hl=et#zippy=%2Ckasutage-viiruset%C3%B5rjetarkvara
3. Riigi InfosüsteemideAmet. Küberturvalisuseaastaraamat2021. Ria.ee. 2021 https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisus-2021.pdf
4. BorodinB. Turvateadlikkusekoolitus kodukontoristöötajatele. Bakalaureuse töö. Tallinna Tehnika Ülikool. 2021.