Karelia-ammattikorkeakoulu
Tradenomi (AMK)

Digitaalisen taloushallinnon kyberuhat ja niihin varautuminen

Riikka Turunen

Opinnäytetyö, marraskuu 2023

www.karelia.fi

Karelia AMMATTIKORKEAKOULU	**OPINNÄYTETYÖ** **Marraskuu 2023** **Liiketalouden koulutus** Tikkarinne 9 80200 JOENSUU +358 13 260 600 (vaihde)

Tekijä
Riikka Turunen

Nimeke
Digitaalisen taloushallinnon kyberuhat ja niihin varautuminen

Tiivistelmä

Opinnäytetyön tavoitteena oli tutkia, mitkä ovat tällä hetkellä suurimmat digitaalista taloushallintoa uhkaavat kyberuhat ja onko niihin riittävästi varauduttu. Lisäksi tavoitteena oli selvittää, mitkä ovat yleisimmät hyökkäystavat, mitä haittavaikutuksia kyberhyökkäyksillä voi yrityksille olla ja kuinka niihin tulisi varautua. Opinnäytetyön avulla haluttiin edistää turvallista digitaalista työskentelyä taloushallinnon alalla.

Tutkimus toteutettiin laadullisena eli kvalitatiivisena tutkimuksena. Tutkimusmenetelminä käytettiin kirjallisuuskatsausta sekä puolistrukturoituja teemahaastatteluja. Opinnäytetyön tietoperustassa käsiteltiin kyberturvallisuutta ja -uhkia sekä digitaalista taloushallintoa. Kirjallisuuskatsauksen aineiston avulla sekä asiantuntijahaastatteluja analysoimalla, tutkittiin digitaalista taloushallintoa uhkaavia kyberuhkia ja alan toimijoiden varautumisen tasoa sekä yleisimpiä hyökkäystapoja, kyberhyökkäysten vaikutuksia ja niihin varautumista.

Tutkimuksessa selvisi, että tällä hetkellä suurimpia digitaaliseen taloushallintoon kohdistuvia kyberuhkia ovat toimitusjohtajahuijaukset, tietojen kalastelu sekä palvelunestohyökkäykset. Hyökkäyksiä tehdään eniten sähköpostin välityksellä. Varautumisen taso osoittautui puutteelliseksi, etenkin pienten tilitoimistojen osalta. Suurimpia haittavaikutuksia ovat rahan, henkilötietojen ja liikesalaisuuksien menetykset sekä liiketoiminnan estyminen. Henkilökunnan tieto- ja kyberturvakoulutukset, hyvä tietoturvan taso sekä varmuuskopioiden teko ovat tehokkaita varautumiskeinoja kyberuhkia vastaan.

Kieli suomi	Sivuja 54 Liitteet 2 Liitesivumäärä 7

Asiasanat
digitaalinen taloushallinto, kyberturvallisuus, kyberuhka, tietoturva

Karelia
UNIVERSITY OF APPLIED SCIENCES

THESIS
November 2023
Degree Programme in Business Economics

Tikkarinne 9
80200 JOENSUU
FINLAND
+ 358 13 260 600 (switchboard)

Author
Riikka Turunen

Title
Cyber Threats of Digital Financial Management and Preparedness for Them

Abstract

The aim of the thesis was to investigate what are the current biggest cyber threats to digital financial management and if companies are sufficiently prepared for them. In addition, the goal was to investigate what are the most common methods of attack, what adverse effects cyberattacks can have on companies and how to prepare for them. The purpose of the thesis was to promote safe digital working in the field of financial administration.

The study was carried out as qualitative research. The used research methods were a literature review and semi-structured theme interviews. The information basis of the thesis covered cyber security and threats as well as digital financial management. Using the literature review material and by analysing expert interviews, the cyber threats on the digital financial management were investigated and furthermore, the preparedness level of operators in the sector was studied, as well as the most common methods of attack and the effects of cyberattacks and the preparedness for them.

This study shows that the biggest cyber threats currently targeting digital financial management are CEO Frauds, phishing and Denial-of-Service attacks. The most attacks are carried out via email. The level of preparedness turned out to be deficient, especially in small accounting companies. The main adverse effects are the loss of money, the loss of personal data and of business secrets and inability to do business. Data and cyber security trainings for personnel, a good level of data security and backups are effective preparedness measures against the cyber threats.

Language
Finnish

Pages 54
Appendices 2
Pages of Appendices 7

Keywords
digital financial management, cyber security, cyber threat, data security

Sisältö

Liitteet

1 Johdanto

1.1 Opinnäytetyön tausta

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen mukaan kyberhyökkäyksiä tapahtuu Suomessa päivittäin ja kyberuhkien määrä on jatkuvassa kasvussa. Tällä hetkellä Suomen kyberturvallisuuden uhkataso on kohonnut ja nousun odotetaan jatkuvan. Palvelunestohyökkäyksistä sekä eritasoisista tietomurroista ja kiristyshaittaohjelmien levittämisestä on tullut päivittäistä. Erityisesti ovat kasvussa kohdistetut kyberhyökkäykset, joissa kohde on ennakkoon tarkkaan valittu. Venäjän suunnalta on havaittu myös Suomeen kohdistuvan kybertoiminnan ja verkossa tapahtuvan tiedustelun lisääntyneen. (Liikenne- ja viestintävirasto Traficom 2023a.)

Suomessa on taloushallinnon digitalisoitumista ja siirtymistä reaaliaikatalouteen haluttu edistää Työ- ja elinkeinoministeriön vuosille 2021–2024 asettaman Yrityksen digitalous -hankkeen avulla. Tuottavuus lisääntyy, kun sähköisessä muodossa olevan ajantasaisen tiedon siirto on automatisoitua eri järjestelmien välillä. (Työ- ja elinkeinoministeriö 2021.) Kaikki sähköistymiseen ja digitalisoitumiseen liittyvä laitteiden ja ohjelmistojen nopea kehitys on kuitenkin lisännyt yritysten kyberuhkien määrää. Tietoliikennevirukset ovat vuosien saatossa lisääntyneet samaa tahtia uusien laitteiden kanssa. Vielä 1990-luvulla viruksia saatettiin koodata huvin vuoksi ilman taloudellisia taka-ajatuksia, mutta tilanteeseen tuli muutos ensimmäisten rahaa tekevien haittaohjelmien myötä 2000-luvun alussa. (Peltomäki & Norppa 2015, 17.)

Yrityksillä on digitaalisessa muodossa paljon kyberrikollisia kiinnostavaa kriittistä tietoa, kuten esimerkiksi asiakastietoja ja yrityssalaisuuksia (Peltomäki & Norppa 2015, 59). Tilitoimistoissa käsitellään päivittäin tietoja sekä tuotetaan palveluja, jotka ovat erittäin tärkeitä yritysten liiketoiminnan sekä työntekijöiden kannalta. Palkanmaksun ja yritysten rahaliikenteen pysähtyminen aiheuttaisi koko yhteiskunnalle erittäin suuria vaikeuksia. Kriisitilanteissa taloushallinnon alan tarjoamat palvelut ovat tärkeä osa huoltovarmuutta. (Fredman 2023.)

1.2 Tavoitteet ja rajaukset

Tämän opinnäytetyön tutkimuskysymyksenä on: Mitkä ovat tällä hetkellä suurimmat digitaalista taloushallintoa uhkaavat kyberuhat ja onko niihin taloushallinnon alalla varauduttu riittävästi? Työn tavoitteena on myös lisätä alan toimijoiden tietoutta hyökkääjien motiiveista, kuinka hyökkäyksiä tehdään, mitä vaikutuksia hyökkäyksillä voi olla ja kuinka niihin tulisi varautua. Opinnäytetyön tutkimuskysymys ja tavoitteet on esitetty kuviossa 1.

Kuvio 1. Opinnäytetyön tutkimuskysymys ja tavoitteet

Kyberturvallisuus on tällä hetkellä erittäin ajankohtainen aihe ja tekemieni havaintojen perusteella kyberuhkia käsittelevä opinnäytetyö on taloushallinnon alalle erittäin tarpeellinen. Olen työskennellyt yli kymmenen vuoden ajan ICT-alalla (Information and Communications Technology), jossa turvallinen työskentely digitaalisessa ympäristössä on hyvin keskeinen teema. Taloushallinnon ala on digitalisoitunut kovaa vauhtia ja sen myötä myös kyberuhkien määrä on kasvanut.

Helsingin seudun kauppakamarin (2022) teettämän selvityksen mukaan oman riskienhallintatyönsä kehittämiseksi yrityksen olisi hyvä saada kokonaiskuva siihen kohdistuvista kyberuhista sekä siitä, kuinka hyvin uhkiin on varauduttu.

Näiden tietojen avulla yritys pystyy puolustautumaan siihen kohdistuvia uhkia vastaan. (Helsingin seudun kauppakamari 2022, 1.)

Opinnäytetyö on rajattu käsittelemään kyberuhkia digitaalisen taloushallinnon näkökulmasta katsottuna. Tässä työssä digitaalisen taloushallinnon käsitteeseen on sisällytetty myös sähköisen taloushallinnon toiminnot. Alueellisesti opinnäytetyö on rajattu koskemaan Suomessa toimivia taloushallinnon alan palveluja tarjoavia kirjanpito- ja tilitoimistoja sekä yritysten sisäisiä taloushallinnon yksiköitä.

1.3 Aiempia opinnäytetöitä ja tutkimuksia

Digitaalisen taloushallinnon kyberuhkia koskevia aiempia opinnäytetöitä en löytynyt Theseus -tietokannasta kuin yhden. Kyberturvallisuutta on käsitelty opinnäytetöissä pääosin kohdennetusti muilta toimialoilta tai yleisesti ottaen yritysten kyberturvallisuutta koskien, jolloin niissä on käsitelty useampaa toimialaa. Muutamista digitaalista taloushallintoa käsittelevistä opinnäytetöistä löytyi mainintoja tieto- ja kyberturvallisuuteen liittyvistä riskeistä, mutta hyvin pienimuotoisesti.

Opinnäytetyö, jonka kyselytutkimuksen tuloksia hyödynsin tämän työn tulosten vertailussa oli Pauli Martinmaan (2017) kirjoittama ”Taloushallinnon sähköistymisen ja digitalisoitumisen tuomat riskit ja niiden hallinta taloushallinnon työntekijän näkökulmasta”. Työntekijöiden haastattelut oli toteutettu sähköpostitse avoimella kyselylomakkeella. Kyselyyn osallistui neljä useita vuosia taloushallinnon alalla työskennellyttä henkilöä, joilla oli myös kokemusta eri kokoisissa yrityksissä työskentelystä. Opinnäytetyön tavoitteena oli tutkia työntekijöiden näkökulmasta taloushallinnon nopean teknologisen kehityksen mukanaan tuomia riskejä ja niiden hallintaa. (Martinmaa 2017, 2.)

Tämän opinnäytetyön tulosten vertailussa käytin myös Helsingin seudun kauppakamarin (2022) teettämän selvityksen tuloksia. Tutkimus on nimeltään ”Yrityksiin kohdistuvat kyberuhat” ja sen avulla selvitettiin, millaisia käsityksiä

suomalaisilla yrityksillä on niihin kohdistuvista kyberuhista ja kuinka hyvin niihin on varauduttu. Kyselytutkimus oli toteutettu syyskuussa vuonna 2022 ja siihen vastasi 258 suomalaista eri aloja edustavaa yritystä. Kyselyyn vastanneista valtaosa oli pieniä alle 50 hengen yrityksiä. Tutkimuksen tulosten tavoitteena oli auttaa yrityksiä oman riskienhallintatyön kehittämisessä antamalla kokonaiskuvaa kyberuhista ja niihin varautumisesta. (Helsingin seudun kauppakamari 2022, 1.)

1.4 Rakenne

Opinnäytetyön ensimmäinen luku koostuu johdannosta. Työn tietoperustassa käsitellään kyberturvallisuutta ja digitaalista taloushallintoa. Luvussa 2 käydään läpi kyberturvallisuuden keskeisiä käsitteitä, Suomen kyberturvallisuuden tilannetta, huoltovarmuutta sekä kyberturvallisuusstrategiaa. Luvuissa 3 ja 4 käsitellään yleisimpiä kyberuhkia ja niihin varautumista sekä kyberriskien haittavaikutuksia ja hallintaa.

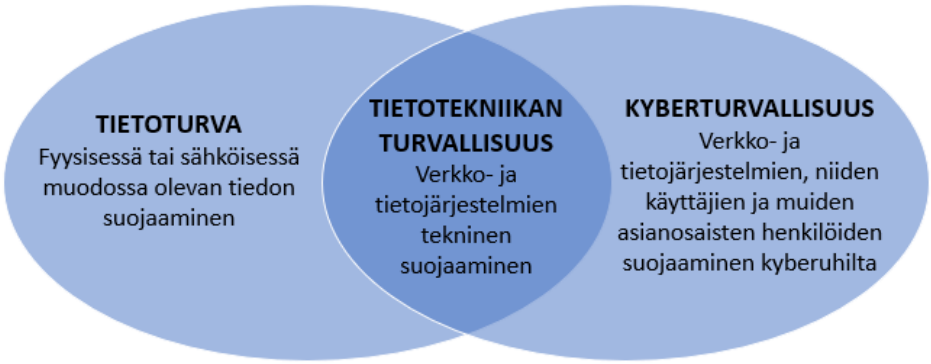
Opinnäytetyön keskiosassa käsitellään digitaalista taloushallintoa. Luvussa 5 käydään läpi taloushallinnon tehtäviä sekä paperisen taloushallinnon kehitystä digitaaliseksi taloushallinnoksi ja digitalisoitumisen vaikutusta kyberuhkiin. Lisäksi selvitetään työtehtävissä ilmeneviä kyberriskejä sekä tietoturvan vaikutuksia tietosuojan toteutumiseen. Lopuksi tarkastellaan taloushallinnon alan tehtävien kriittisyyttä.

Opinnäytetyön loppuosassa käsitellään työssä tehtyä haastattelututkimusta ja siitä saatuja tuloksia. Luvussa 6 käydään läpi haastattelututkimuksen tavoitteita, tutkimusmenetelmien valintaa ja tutkimuksen toteutusta. Luvussa 7 esitetään tutkimuksen tulokset ja niistä tehdyt analyysit. Luvussa 8 tarkastellaan opinnäytetyön tutkimuksen tavoitteiden saavuttamista, luotettavuutta ja eettisyyttä sekä arvioidaan valittuja tutkimusmenetelmiä ja omaa oppimista. Lopuksi pohditaan nykytilanteen kehitystä sekä mietitään taloushallinnon kyberturvallisuuden tulevaisuudennäkymiä ja jatkotutkimuskohteita.

2 Kyberturvallisuus

2.1 Keskeisiä käsitteitä

Kyberturvallisuus eroaa tietoturvallisuudesta siten, että se on tietoturvaa laajempi käsite. Tietoturvallisuudella varmistetaan tietojen luottamuksellisuus, eheys ja saatavuus. Se on tietojen, tietoliikenteen, palvelujen ja järjestelmien suojaamista, kun taas kyberturvallisuuden avulla voidaan varmistaa sähköisessä muodossa olevan tietojenkäsittelyyn tarkoitetun kybertoimintaympäristön luotettava ja tarkoituksenmukainen toiminta (kuvio 2). Kybertoimintaympäristö on maailmanlaajuinen digitaalinen ympäristö, joka koostuu tietojärjestelmistä. Siihen voi kohdistua kyberuhkiksi kutsuttuja tapahtumia tai tekoja, jotka toteutuessaan voivat vaarantaa kybertoimintaympäristöstä riippuvaisia toimintoja. (Peltomäki & Norppa 2015, 170,172.)



Kuvio 2. Tieto- ja kyberturvallisuus (mukaillen Euroopan tilintarkastustuomioistuin 2022).

Kyberuhkan muuttuessa tietoverkossa tapahtuvaksi hyökkäykseksi, puhutaan kyberhyökkäyksestä. Kyberhyökkäykset tapahtuvat bittien välityksellä kybertoimintaympäristössä ja niillä voidaan aiheuttaa haittaa ja tuhoa sekä fyysisessä että bittien maailmassa. Motiivina kyberhyökkäykselle voi olla esimerkiksi järjestelmien ja laitteiden käytön estäminen tai tiedon varastaminen. Kyberhyökkäyksillä voidaan häiritä ja lamauttaa yhteiskunnan kriittisiä toimintoja. (Limnéll, Majewski & Salminen 2014, 240; Peltomäki & Norppa 2015, 170.)

Kriittinen infrastruktuuri sisältää yhteiskunnalle elintärkeitä fyysisiä sekä sähköisiä rakenteita ja toimintoja, joiden varassa yhteiskunta pyörii. Yhteiskunnan toiminta ja arkipäivän sujuvuus ovat riippuvaisia kriittisestä infrastruktuurista, joihin kuuluvat muun muassa sähköiset viestintäjärjestelmät, raha- ja finanssijärjestelmät, vesihuolto sekä muu yhdyskuntatekniikka, kuljetuslogistiikka, energian siirto ja jakelu, julkisen hallinnon järjestelmät, maanpuolustus sekä pelastus- ja terveyspalvelut. (Limnéll ym. 2014, 239; Peltomäki & Norppa 2015, 169.)

2.2 Kansallinen turvallisuus

Kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristön toiminta on turvattua ja siihen voidaan luottaa. Nopeasti digitalisoituvaa yhteiskuntaa ja sen toimintakykyä halutaan suojella vihamieliseltä kybervaikuttamiselta sekä tietoverkkotiedustelulta. Kansallisen turvallisuuden kyberuhat mielletään usein kohdistuvan valtiollisiin kohteisiin, joissa tietoverkkojen avulla uhataan kriittistä infrastruktuuria, maanpuolustusta tai valtion johtoa. Hyökkäyksiä kuitenkin suunnataan yhä enemmän myös muiden sektoreiden toimijoihin. Myös valtiolliset toimijat hyödyntävät eri kyberrikollisryhmiä silloin kun haluavat peitellä omaa osallissuttaan. (Sisäministeriö 2023.)

Kyberuhkien pyrkimyksinä on useimmiten vaikuttaa valtion ja yhteiskunnan toimintakykyyn sekä päätöksentekoon häiritsevästi tai jopa lamauttavasti. Tiedot, jotka liittyvät esimerkiksi valtion päätöksiin, yritysten kehittämiseen tai tutkimuksiin ovat usein kyberrikollisten kiinnostuksen kohteena. Kybervaikuttamisen keinoin väärää informaatiota levittämällä, voidaan myös painostaa ja vaikuttaa päätöksentekoon. Hyökkäysten takana olevien tahojen tunnistaminen on usein hankalaa, koska jäljet pystytään melko tehokkaasti peittämään erilaisin keinoin. Kuitenkin esimerkiksi toimintatavat, valitut kohteet sekä käytetyt haittaohjelmat voivat auttaa löytämään tekijän jäljille. Syyllisen selvittyä voidaan ryhtyä diplomaattisiin toimiin tai ottaa käyttöön taloudelliset keinot tekijätahon hillitsemiseksi. (Sisäministeriö 2023.)

Petteri Järvinen (2018) kertoo teoksessaan ”Kyberuhkia ja somesotaa”, kuinka Ukrainassa vuoden 2015 lopulla tehtiin ensimmäinen siviiliväestöön kohdistuva laajamittainen kyberhyökkäys Venäjän toimesta. Hyökkäys oli kohdistettu kolmea sähköyhtiöitä vastaan ja sen seurauksena yhteensä 225 000 asiakkaalta katkesivat sähköt. Tietojen mukaan se on ensimmäinen sähkölaitokseen kohdistuva isku, joka toteutettiin tietoverkon kautta. Tutkimuksissa selvisi, että hyökkääjät olivat päässeet sisälle järjestelmiin urkkimaan tietoa jo puoli vuotta aiemmin vakoiluohjelman sisältäneen Excel-tiedostoliitteen avulla, jonka varomattomat työntekijät olivat avanneet energiayhtiön koneella. (Järvinen 2018, 46–47.)

2.3 Kyberturvallisuus Suomessa

Kybertoimintaympäristö on maailmanlaajuinen valtioita, yrityksiä ja ihmisiä yhdistävä tekijä, mutta sen myötä myös kyberaktivismi, -rikollisuus ja -vakoilu ovat lisääntyneet globaalisti ja kasvua on nähtävissä sekä valtiollisissa että ei-valtiollisissa toimijoissa. Kybertoimintaympäristössä ei valtioiden fyysisellä suuruudella ole enää niin suuri painoarvo kuin osaamisella. Suomi on pieni maa, mutta se on yksi kehittyneimmistä tietoyhteiskunnista. Riippuvaisuus sähköisistä verkoista ja niiden tarjoamista toiminnoista, altistaa entistä enemmän kansainvälisille kyberhyökkäyksille. Suomeen on jo kohdistunut kyberoperaatioita ja hyökkäysten määrän odotetaan kasvavan. (Turvallisuuskomitean sihteeristö 2013, 17–19.)

Ukrainan sodan poliittiset vaikutukset näkyvät Suomen kyberturvallisuudessa Venäjän maantieteellisen läheisyyden vuoksi. Suomessa on tapahtunut useita poliittisia hyökkäyksiä, joiden jäljet viittaavat Venäjälle. Esimerkiksi heinäkuussa 2022, kun Wärtsilä vetäytyi Venäjän markkinoilta, sen tietojärjestelmään murtauduttiin ja rikolliset pääsivät yhtiön laskutus- sekä ostotietoihin. Kyseessä oli kiristyshaittaohjelma, jonka tarkoituksena on saada tuloja myymällä tietoja muille rikollisryhmille, kilpailijoille tai alkuperäiselle omistajalle. Hyökkäyksen takana oli LV-haittaohjelmaa käyttävä hakkeriryhmä Gold Northfield, joka on yhdistetty useampaan vastaavaan tekoon. Wärtsilän kyberasiantuntijoiden nopean

rajauksen ansiosta hyökkäyksen haitat jäivät pienemmiksi mitä hyökkääjät antoivat ymmärtää. (MTV Uutiset 2022.)

Suomen Natoon liittyminen aiheutti 4.4.2023 palvelunestohyökkäyksien sarjan, joiden takana venäläinen hakkeriryhmä NoName 056(16) on ilmoittanut olevansa. Hyökkäyksien kohteena olivat eduskunnan verkkosivut, Teknologian tutkimuskeskus VTT Oy:n verkkosivut sekä pääministeri Sanna Marinin virallinen sivusto, jotka kaatuivat hyökkäyksien vuoksi. Ryhmä väittää olevansa myös elokuussa 2022 eduskunnan sivuille kohdistuneen palvelunestohyökkäyksen takana. (Bogdanov 2023.) Suomi esti syyskuussa 2023 venäläisillä rekisterikilvillä varustettujen autojen tulon maahan, jolloin sama ryhmä ilmoitti tehneensä palvelunestohyökkäykset Liikennevirasto Traficomin, VR:n, ExpressBusin ja Ristelyt Saimalla -verkkosivuille (Mulari 2023).

2.3.1 Suomen kyberturvallisuusstrategia

Tietoyhteiskuntana Suomi on hyvin haavoittuvainen häiriöille, jotka kohdistuvat tietoverkkoihin ja -järjestelmiin. Tämän vuoksi on erityisen tärkeää varmistaa kybertoimintaympäristön toimivuus ja pystyttävä vastaamaan sekä tahallisiin että tahattomiin häiriötekijöihin. Suomen kyberturvallisuusstrategiassa on määriteltynä tärkeimmät tavoitteet ja toimintalinjat, joiden toimeenpanosta, toteuttamisesta ja kehittämisestä vastaavat ministeriöt sekä virastot omilla toimialoillaan. Valtiohallinnon keskeisiä tieto- ja kyberturvallisuuden linjauksia käsittelee ja yhteensovittaa valtiohallinnon tieto- ja kyberturvallisuuden johtoryhmä VAHTI. (Valtiovarainministeriö 2023.)

Ulkoministeriön (2023) mukaan Suomen kansallisen kyberturvallisuusstrategian tavoitteen on ”Vastata kyberuhkiin, vahvistaa yhteiskunnan kokonaisturvallisuutta ja varmistaa kybertoimintaympäristön toimivuus kaikissa oloissa.” Strategiassa on kymmenen tavoitetta, joiden täytäntöönpanoa Turvallisuuskomitea seuraa. Ulkoministeriön tehtävänä on puolestaan huolehtia, että Suomi osallistuu aktiivisesti ja tehokkaasti kansainväliseen yhteistyöhön sekä keskusteluun.

Strategian linjaukset on tehty kansallisen kybertoimintaympäristön haittavaikutusten hallitsemiseksi. (Ulkoministeriö 2023.)

2.3.2 Huoltovarmuus

Huoltovarmuustoiminnan tavoitteena on yhteiskunnan elintärkeiden toimintojen ylläpitäminen riittävällä tasolla kaikkein vakavimmissakin kriisi- ja häiriötilanteissa. Huoltovarmuustoiminnan merkitystä Suomessa ovat viime aikoina nostaneet poikkeuksellinen maailmantilanne sekä Venäjän hyökkäyssota. Toiminta- ja turvallisuusympäristöt ovat muuttuneet merkittävästi ja huoltovarmuuden riittävään ylläpitoon liittyvien riskien toteutumisen uhka on kasvanut, kun yhteiskunta joutui siirtymään heti pandemian jälkeen uuteen kriisitilanteeseen. Itärajan takaa tulleiden raaka-aineiden ja energian lähteiden korvaamisen lisäksi, turvallisuustilanteen kiristyminen on vaatinut erityistä huomiota. (Huoltovarmuuskeskus 2023 3–4, 6.)

Nopea teknologinen kehitys, Ukrainan sota ja turvallisuusympäristön muutokset vaativat nostamaan kyberturvallisuusvalmiuksia sekä vahvistamaan toimintakykyä häiriötilanteissa kriittisien toimintojen osalta. Huoltovarmuuskeskus käynnisti vuonna 2022 yhteistyössä Kyberturvallisuuskeskuksen kanssa hankekokonaisuuden yhteiskunnan kyberturvallisuuden parantamiseksi. Kokonaisuudella halutaan varmistaa, että kyberturvallisuusloukkauksen kohteeksi joutuneet huoltovarmuuskriittiset yritykset saavat heti apua. Yhteistyössä toteutetun Digitaalinen turvallisuus 2030-ohjelman myötä on myös selvitetty muun muassa kyberturvallisuuden kehitystä sekä tekoälyn vaikutuksia kyberhyökkäyksiin. (Huoltovarmuuskeskus 2023, 15–16.)

3 Yleisimmät kyberturvallisuusuhat

3.1 Kyberuhkien kasvu

Traficomin Kyberturvallisuuskeskuksen vuoden 2023 kvartaalitilastojen mukaan laskutuspetokset ja toimitusjohtajahuijaukset ovat olleet selvässä kasvussa aiempaan nähden ja niitä tehdään tasaiseen tahtiin. Muiden huijausten ohella pankkitunnusten kalastelu on lisääntynyt ja siinä käytetyt keinot ovat monipuolistuneet. Palvelukatkoksia aiheuttavia palvelunestohyökkäyksiä on myös ilmennyt runsaasti. (Liikenne- ja viestintävirasto Traficom 2023b, 9,11.)

Suomalaiset menettivät verkkorikollisille vuonna 2022 yhteensä 32,4 miljoonaa euroa, vaikka pankit ja viranomaiset saivat estettyä rahansiirtoja yli 14 miljoonan euron edestä. Toimitusjohtajahuijauksien osuus on merkittävä 4,9 miljoonaa euroa. Suurimman osuuden, yhteensä 10 miljoonaa euroa veivät erilaiset tietojen kalastelut sekä valepoliisihuijaukset. Tilastossa eivät ole mukana kaikki huijausmuodot ja koska kaikista tapauksista ei tehdä rikosilmoitusta poliisille tai ilmoiteta pankille niin myös ne jäävät tilastojen ulkopuolelle. (Finanssiala ry 2023.)

3.2 Haittaohjelmat

Haittaohjelmien tarkoituksena on nimensä mukaisesti aiheuttaa haittaa ja harmia koneen käyttäjälle. Erilaisia haittaohjelmatyyppejä ovat esimerkiksi troijalaiset, madot, vakoiluohjelmat sekä virukset. Kun haittaohjelma on asennettu uhrin koneelle, sen avulla pystytään esimerkiksi varastamaan tietoja, vakoilemaan, salaamaan tietoja oikealta käyttäjältä, ottamaan kone kokonaan haltuun tai tehdä muuta lainvastaista toimintaa. Haittaohjelman tekijä voi olla mistä päin maailmaa hyvänsä ja motiivina voi olla vain helppo pääsy tietoihin. Haittaohjelmia levitetään usein sähköpostiliitteiden ja linkkien välityksellä. (Liikenne- ja viestintävirasto Traficom 2020, 7.)

Kiristyshaittaohjelma estää tietokoneelle päästyään sen käytön salaamalla tiedostoja muuntamalla niitä esimerkiksi salakirjoitettuun muotoon. Ilman salauksen purkuavainta ei tiedostoihin pääse käsiksi ja tätä purkukoodia vastaan rikollinen vaatii lunnaita. Lunnaat halutaan maksuun usein virtuaalivaluuttana, esimerkiksi bitcoineina. Takuita tiedostojen palautumisesta tai siitä etteivät ne päädy yleiseen jakeluun ei kuitenkaan ole, vaikka lunnaat maksettaisiinkin. (Liikenne- ja viestintävirasto Traficom 2020, 8.)

3.3 Tietomurrot, tietovuodot ja väärän tiedon levittäminen

Tietomurrot ovat kyberrikollisten tahallisesti tekemiä hyökkäyksiä, joissa tunkeudutaan luvattomasti tietojärjestelmään, laitteeseen, sovellukseen tai palveluun. Tietomurrosta on kyse esimerkiksi silloin, kun hyökkääjä ottaa luvattomasti haltuun toisen henkilön sähköpostitilin saamiensa tunnusten avulla. Yleensä hyökkääjät tavoittelevat tietomurroissa, tietovuodoissa sekä tietojenkalastelussa luottamuksellisten tietojen luvatonta käyttöä tai paljastamista ja motiivina on useimmiten raha sekä joskus myös vakoilu. (Lehtonen 2021.)

Tietovuodoissa salaiseksi luokiteltavia tietoja, kuten esimerkiksi salasanoja ja henkilötunnuksia levitetään ulkopuolisille tietomurron seurauksena. Tietovuoto voi tapahtua myös tahattomasti ilman viitteitä rikollisesta toiminnasta. (Lehtonen 2021.) Henkilötietojen tietoturvaloukkauksesta on kyse silloin kun joku ulkopuolinen taho pääsee henkilötietoihin käsiksi, tietoja tuhoutuu tai ne muuttuvat kyberhyökkäyksen tai muun tapahtuman seurauksena (Tietosuojavaltuutetun toimisto 2023a).

Tarkoituksellisesti väärennettyjen tietojen levittäminen eli disinformaatio sekä väärien tai puutteellisten tietojen levittäminen vahingossa eli misinformaatio ovat lisääntyneet sosiaalisen median alustojen ja verkkomedian käytön yleistyttyä. Harhaanjohtavan tiedon levittämisen tavoitteena voi olla halu vaikuttaa mielipiteisiin tai aiheuttaa hämmennystä sekä pelkoa. (Euroopan parlamentti 2023.)

3.4 Tietojenkalastelu

Tietojenkalasteluviestit ovat usein naamioitu näyttämään tunnetun organisaation tai vastaanottajan tunteman henkilön lähettämältä viestiltä. Viestien tarkoituksena on saada urkittua vastaanottajalta tietoja, rahaa tai sisäänpääsy vastaanottajan käyttämään järjestelmään. Haitallisia linkkejä lähetetään usein sähköpostitse, tekstiviestillä tai pikaviestimillä, mutta niitä on myös sosiaalisessa mediassa sekä internetsivustoilla. (Liikenne- ja viestintävirasto Traficom 2020, 4.)

Kalasteluviestit voidaan jakaa kolmeen eri kategoriaan. Tietojenkalastelussa (Phishing) pyritään saamaan käyttäjältä luottamuksellista tietoa, kuten esimerkiksi pankkitunnukset. Kohdennetussa tietojenkalastelussa (Spear Phishing) on verkkourkinta kohdistettu tiettyyn henkilöön tai organisaatioon, jolloin esimerkiksi sähköposti näyttää tulevan esimieheltä, mutta vastausviesti meneekin huijarille. Toimitusjohtajahuijaus (CEO Fraud) on puolestaan sellainen, että viesti näyttää tulevan yrityksen johtajalta ja se on suunnattu yrityksen rahaliikennettä hoitavalle työntekijälle. (Liikenne- ja viestintävirasto Traficom 2020, 4.)

3.5 Palvelunestohyökkäykset

Palvelunestohyökkäyksillä pyritään estämään tietojen ja palveluiden käyttö kokonaan häiritsemällä toimintaa. Hyökkäys toteutetaan siten, että kohdepalvelua tai sen verkkoliikennettä joko kuormitetaan ylimääräisellä liikenteellä tai hyödynnetään haavoittuvuutta mikä on havaittu verkkolaitteessa tai palvelussa. Nykyään käytetään paljon hajautettua hyökkäystä, joissa hyödynnetään verkkoon kytkettyjä ja kaapattuja laitteita omistajien tietämättä. (Liikenne- ja viestintävirasto Traficom 2022a, 2.)

Palvelunestohyökkäyksiä voi ostaa palveluna pimeästä verkosta, joten hyökkäyksen toteuttaja saattaa olla eri taho kuin tilaaja. Motiivina hyökkäyksille voi olla kiusanteko, kiristäminen tai poliittinen häirintä. Palvelunestohyökkäykset ovat erittäin kriittisiä uhkia ja ne ovat kehittyneet monimutkaisiksi ja laajemmiksi.

Ne ovat käytettävyyteen liittyviä uhkia ja kohdistuvat internetin saatavuuteen. Mobiiliverkot sekä niihin liittyvät laitteet ovat koko ajan enemmän riskille alttiina. Hyökkäyksen kohteena on viime aikoina ollut paljon myös julkisten palvelujen verkkosivuja. (Euroopan parlamentti 2023.)

3.6 Toimitusketjuhyökkäykset

Jokainen yritys on koostaan tai toimialastaan riippumatta potentiaalinen kohde kyberrikokselle. Tämän lisäksi yritys voi myös toimia reittinä toiseen yritykseen. Kyberrikolliset valitsevat kohteet omien käyttötarkoitustensa sekä tavoitteidensa mukaan ja yritykset tarjoavat niille laajan hyökkäyspinta-alan. Mikä yritys tahansa saattaa vaarantaa yhteiskunnan kykyä kohdata häiriöitä olemalla ketjun heikoin lenkki. Luottamuksellista tietoa voidaan varastaa tai digitaalisia tuhotöitä valmistella yrityksen tietoverkossa tai sen kautta. (Helsingin seudun kauppakamari 2022, 1, 37.)

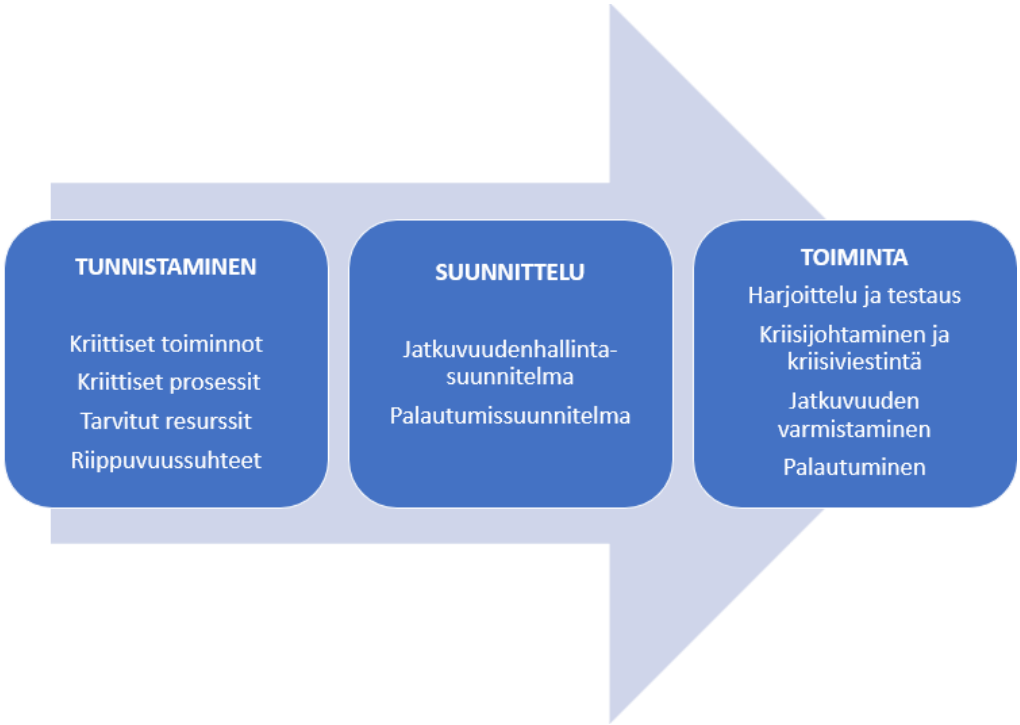
Toimitusketjuhyökkäyksissä käytetään hyväksi luottamusta organisaatioiden sekä toimittajien välillä ja uhrina ovat molemmat. Organisaation tietojärjestelmiin murtaudutaan käytössä olevien palveluiden, verkostojen avoimien lähdekoodin projektien tai tuotteiden kautta. Hyökkäyksen reittinä saattavat toimia yhteistyökumppanit, ohjelmistot, laitteet tai palveluntarjoajat. Hyökkäys etenee yleensä niin, että toimittajan järjestelmiin tunkeuduttuaan hyökkääjä saastuttaa haittakoodilla toimitusketjun osan, joka leviää toimittajan järjestelmistä normaaleja jakelukanavia pitkin asiakas- ja yhteistyöorganisaatioihin. Hyökkääjä pääsee sisälle toimitusketjun eri organisaatioihin ja voi tehdä haluamiinsa kohteisiin jatkohyökkäyksenä esimerkiksi kiristyshaittaohjelmahyökkäyksiä tai tietomurtoja. (Liikenne- ja viestintävirasto Traficom 2022b, 2.)

4 Kyberuhkiin varautuminen

4.1 Toiminnan jatkuvuuden varmistaminen

Kyberuhkiin varautumalla suojataan yrityksen henkilöstön ja asiakkaiden yksityisyyttä sekä yrityksen aineetonta omaisuutta. Varautumalla turvataan asiakkaita ja pystytään varmistamaan liiketoiminnan jatkuvuus kyberhyökkäyksen sattuessa omalle kohdalle. Kyberturvallisuuden varmistaminen on vastuunkantoa kansallisesta turvallisuudesta. (CGI Inc 2018, 5.)

Varautumisessa on tärkeää osata tunnistaa yrityksen toiminnan kannalta kriittiset prosessit sekä prosessien tarvitsemat resurssit ja kiinnittää suojautumisessa huomiota erityisesi niihin. Tietojärjestelmien ja palveluiden väliset riippuvuussuhteet tulisi huomioida ja yrityksen ulkopuoliset riippuvuussuhteet tulisi tunnistaa sekä varmistaa myös näiden varautumisen taso. (Mäkelä 2022.) Varautumisen prosessi on esitetty kuviossa 3.



Kuvio 3. Varautumisen prosessi (Mäkelä 2022).

Normaalitoiminnan palautumissuunnitelmassa tulisi huomioida toipumisen tavoiteaika. Mitä kriittisemmästä toiminnosta on kyse sitä nopeammin se tulisi saada palautettua. Myös menetetyn tiedon määrään sekä häiriön ajalliseen kestoon tulisi määritellä pisteet, milloin vaikutukset muuttuvat yrityksen kannalta sellaisiksi, että toimintaa uhkaa jopa sen loppuminen kokonaan. Varautumismekanismien tulisi vastata palautumissuunnitelman tavoitteita ja niiden avulla tulisi pystyä palautumaan normaalitoimintaan tavoiteajassa ilman suurempia vahinkoja. (Mäkelä 2022.)

Tietojen palauttamista varmuuskopioista olisi hyvä harjoitella ja testata ennakkoon mahdollisten kehityskohteiden havaitsemiseksi sekä laatia palauttamiseen riittävän kattava ohjeistus todellista tilannetta varten. Poikkeaman sattuessa tulee olla myös selkeä käsitys siitä, että kuka johtaa toimintaa, kenellä on valtuudet tehdä päätöksiä ja kuka vastaa viestinnästä. Kyberturvapoikkeama voi olla tahallisesti tai tahattomasti aiheutettu olotila tai tapahtuma, joka vaarantaa tietojen ja palvelujen eheyden, luottamuksellisuuden tai saatavuuden. (Mäkelä 2022.)

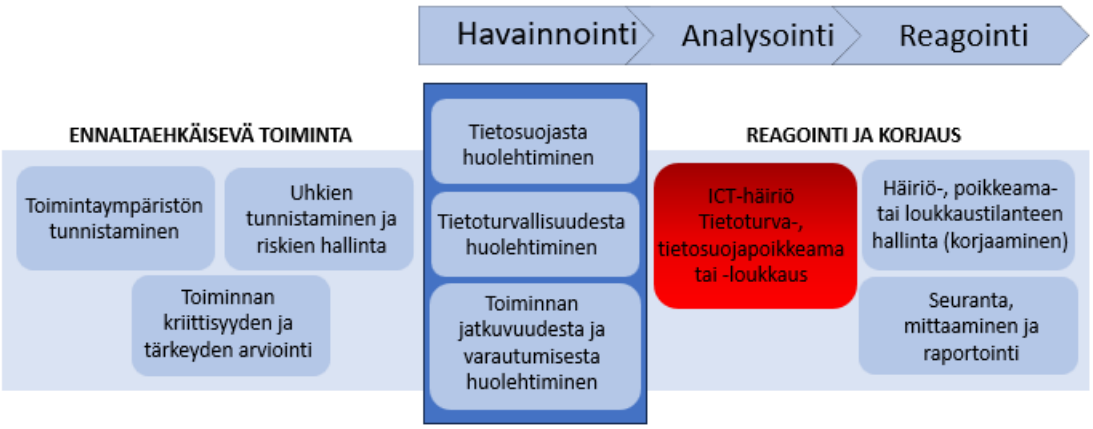
Häiriötilanne voi haitata palvelun toimintaa monin eri tavoin joko hidastamalla tai estämällä toiminnan kokonaan, mutta se voi olla myös huomaamaton tai ilmetä vain joitain erityisiä toimintoja tehdessä. Häiriö tulee kuitenkin poistaa ja toiminnan jatkuvuuden takaamiseksi on häiriötilanteisiin varauduttava. Etenkin tärkeillä ja kriittisillä toiminnoilla tulee olla kattava jatkuvuudenhallintasuunnitelma sekä toipumissuunnitelmat. (Rousku 2014, 60–61.)

Kyberturvallisuuden huomioiminen on erityisen tärkeää silloin kun organisaatiossa tapahtuu muutoksia. Muutokset voivat liittyä järjestelmiin, sovelluksiin, toimitiloihin, etätyöskentelyyn tai arvoketjussa tapahtuviin muutoksiin kuten lakimuutoksiin, yrityskauppoihin tai uusiin kumppaneihin. Teknologisista investoinneista erityisen kriittisiä ovat IoT-ympäristöön liittyvät muutokset, jossa jo jokin yksittäinen laite voi luoda mahdollisen uhan. Muutoksiin valmistautuessa kannattaa huomioida se, että suurin osa onnistuneista kyberhyökkäyksistä johtuu ihmisten tekemistä inhimillisistä virheistä ja tähän voidaan vaikuttaa koulutuksen avulla. (CGI Inc 2023, 6.)

4.2 Kyberriskien hallinta

Kyberturvallisuudesta huolehtimiseksi tulee kyetä arvioimaan kyberuhkien mahdolliset vaikutukset liiketoiminnalle ja laatia suunnitelmat näiden riskien hallitsemiseksi. Liiketoiminnan ytimessä tulee olla toimintamalli, jonka avulla voidaan puuttua uhkiin jo ennen kuin ne toteutuvat. Yksi tärkeä riskienhallintakeino on kehittää kykyä poikkeamien havaitsemiseen toimintaympäristössä. Lisäksi on hyvä omata toimintatavat ja varautumissuunnitelmat poikkeamien korjaamiseen mahdollisimman nopeasti sekä valmius oppia hyökkäykseen johtaneista virheistä. (Karinen 2020.)

Kyberriskien hallinta voidaan jakaa kahteen eri vaiheeseen eli proaktiiviseen, ennaltaehkäisevään toimintaan sekä reaktiiviseen, poikkeamiin reagoimiseen ja ongelmien korjaamiseen (kuvio 4). Proaktiivisessa ennaltaehkäisevässä toiminnassa ensin tunnistetaan ja priorisoidaan kohteet eli arvioidaan tiedon arvo ja sen käsittelyssä käytetyt järjestelmät. Seuraavaksi tunnistetaan kyberuhkien riskit sekä niiden todennäköisyydet ja vaikutukset. Tämän jälkeen tehdään hallinnollisia ja teknisiä toimenpiteitä kyberpoikkeamien ja riskien konkretisoitumisen ennaltaehkäisemiseksi. (Karinen 2020.)



Kuvio 4. Kyberriskin hallinta (mukaillen Väestörekisterikeskus 2019).

Reaktiivisessa ongelmien korjaamisessa on ensimmäisenä kyettävä havaitsemaan ja tunnistamaan normaalista poikkeavat tapahtumat, jotka liittyvät esimerkiksi käyttäjiin, laitteisiin, sovelluksiin ja verkkoihin. Seuraavaksi on pystyttävä

tutkimaan ja selvittämään tietoturvapoikkeamanhallinnan toimenpiteillä, että mitä on tapahtunut ja miksi. Lopuksi on tehtävä oikea-aikaiset ja laajuiset korjaustoimenpiteet, jotka tähtäävät ongelman korjaamiseen. Toiminnan palauttavia toimenpiteitä voi olla esimerkiksi tietoliikennemuutosten tekeminen, salasanan vaihtaminen sekä järjestelmän päivittäminen. (Karinen 2020.)

Riskienhallintaan kuuluu arvioida ja tunnistaa tietoturvallisuuteen sekä toiminnan jatkuvuuteen liittyvät riskit ja panostaa niihin toimintoihin, joissa uhkan toteutuminen on todennäköistä ja joissa sen vaikutukset ovat suuret. Varautumalla ja ennakkoon tehtyjen suunnitelmien avulla voidaan varmistaa, että häiriön sattuessa vahingot pysyvät mahdollisimman pieninä ja häiriön korjaamisen jälkeen palautuminen normaalitilanteeseen onnistuu. (Rousku 2014, 60–61.)

4.2.1 Laitteiden suojaukset

Laitteiden virusturvan sekä palomuurien tulee olla asennettuna ja ajan tasalla. Laitteiden päivittäminen heti uuden turvapäivityksen ilmestyessä on erittäin tärkeää ja tämän varmistamiseksi automaattisten päivitysten käyttö on suotavaa. Päivityksillä korjataan ilmenneitä turva-aukkoja ja ne ovat aiheellista pitää ajan tasalla. Ominaisuuspäivitysten avulla saadaan laitteet päivitettyä toimivuuden ja ominaisuuksien kannalta paremmiksi. (Järvinen 2022, 36, 40.)

Päätelaitetta ei tule jättää valvomatta ja lukitsematta tutussakaan työympäristössä. Virrat kannattaa katkaista kokonaan työskentelyn päätyttyä. Levynsalauksen käyttö on suositeltavaa sekä tietokoneella että mobiililaitteissa. Varmuuskopioinnin avulla voidaan välttää tietojen lopullinen menettäminen esimerkiksi laiterikon sattuessa. Tallentaminen on vaivatonta, kun se automatisoidaan esimerkiksi pilvipalveluun. (Järvinen 2022, 93, 42.)

Julkisten wifi- ja bluetooth-yhteyksien sijaan mobiilidatan käyttö on suositeltavampaa aina kun se on mahdollista. Mikäli avointa wifi-verkkoa käyttää, tulee se tehdä salatulla VPN-yhteydellä. Verkkoon liityttäessä verkon nimi kannattaa

tarkistaa huolella ja sitä ei kannata tallentaa koneelle, ettei oma laite liity siihen jatkossa automaattisesti. (Järvinen 2022, 223.)

4.2.2 Ohjelmistot ja käyttöjärjestelmät

Ohjelmistojen päivittäminen kannattaa tehdä myös automaattipäivityksiä hyödyntämällä. Ajantasaisilla päivityksillä saadaan tehokkaasti ehkäistyä hyökkäyksiä. Sovellusten asennus kannattaa tehdä vain luotettavalta taholta ja turhia sovelluksia kannattaa välttää, näin saadaan vähennettyä uhkien määrää. Sovelluksien käyttöoikeuksien hyväksymisen kanssa kannattaa myös olla huolellinen. Työkoneiden käyttöoikeuksien rajoittaminen on hyvä keino välttää turhia riskejä. Perusoikeuksilla saadaan karsittua tahattomia haittaohjelmien ja -sovellusten latauksia. (Järvinen 2022, 36, 41–44.)

Salasanojen kannattaa olla mahdollisimman pitkiä ja monimutkaisia, mikä hankaloittaa niiden hakkerointia. Jokaiseen palveluun tulee olla oma salasanansa ja niitä on vaihdettava säännöllisesti. Kaksivaiheinen todennus kannattaa ottaa käyttöön aina kun se on vaihtoehtona, näin salasanan vuotaminen ei vielä suoraan avaa pääsyä kohteeseen, vaan sisäänpääsy tulee vielä vahvistaa puhelimeen lähetetyllä kertakäyttöisellä koodilla. (Järvinen 2022, 94–9.)

Sähköpostin liitetiedostojen ja linkkien avaamisessa tulee olla varovainen ja epäilyttäviä tiedostoja ei tule avata tietokoneella laisinkaan, vaikka lähettäjä olisi tuttu. Mobiililaitteeseen tietokoneelle tehdyt haittaohjelmat eivät asennu, joten esimerkiksi älypuhelimella avattu liitetiedosto ei pysty aiheuttamaan vahinkoa. (Järvinen 2022, 170.)

4.2.3 Henkilöstö

Yritysten kyberturvallisuusteknologian murtamisen sijaan, helpoin ja nopein tapa päästä käsiksi yrityksen tietoihin on huijata käyttäjää. Tämän vuoksi henkilökunnan jatkuva kouluttaminen sekä ajankohtaisista riskeistä tiedottaminen

kuuluvat tehokkaimpiin keinoihin taistellessa kyberuhkia vastaan. (Mäkelä 2020.) Henkilökunnan tietoisuutta olisi hyvä lisätä koulutusten avulla myös siltä osin, että häiriötilanteen sattuessa osataan toimia oikein (Järvinen 2022, 235).

Tiedostojen turvaluokituksella selkeytetään tietojen käsittelyä. Luokittelussa voidaan määritellä tietoja esimerkiksi henkilökohtaiseksi, julkiseksi, sisäiseen käyttöön, luottamukselliseksi ja salaiseksi. Turvamerkinnät auttavat asiakirjojen käsittelijää ja ohjelmistot myös estävät tiedostojen lähettämisen ja jakamisen luokitusten mukaisesti. Hyvä turvatoimi on myös työntekijöiden oikeuksien rajoittaminen työtehtävien mukaan, jolloin järjestelmä sallii pääsyn vain työtehtävissä tarvittuihin tietoihin. (Järvinen 2022, 165–166; 233.)

Kulkulupien valvonta kuuluu kaikille työntekijöille. Työtiloissa ilman kulkulupaa liikkuvaan tuntemattomaan henkilöön tulee kiinnittää huomiota ja ilmoittaa poikkeamista. Kulkukorttia ei tule käyttää työpaikan ulkopuolella ja mikäli se häviää on siitä välittömästi ilmoitettava. Työpaikan ulkopuolella työskennellessä tulisi varmistaa, että työskentelee tilassa, jossa ei voida salakuunnella tai -katsella. Tietokoneella kannattaa olla julkisessa tilassa tai kulkuneuvossa työskennellessä näytönsuoja ja tärkeät puhelut kannattaa tehdä vain puheluihin tarkoitetuissa puhelinkopeissa. Tietokoneen ja tabletin kamera kannattaa peittää myös toimistolla työskennellessä. (Järvinen 2022, 84; 88.)

4.3 Kyberhyökkäyksen toteutuessa

Mikäli uhka toteutuu, ei kannata toimia liian hätäisesti, vaan tilanteesta pitäisi muodostaa selkeä tilannekuva ja pyrkiä rajaamaan vahingot mahdollisimman nopeasti. Tietokonetta ei tule sulkea ennekuin siihen on annettu lupa, mutta vahingon leviämisen voi estää irrottamalla saastunut kone sisäisestä verkosta. Hyökkäyksen selvittämiseksi tulisi tarkistaa kulunvalvonta, USB-tikut ja lokitiedot, ottaa kuvat tapahtumapaikalta sekä laittaa ylös kellonajat ja päivämäärät. (Järvinen 2022, 235–238.)

Tietoturvaloukkauksista kannattaa ilmoittaa Kyberturvallisuuskeskukseen, josta saa myös tarvittaessa toimintaohjeita. Vaikkei tietoturvarikosten tekijöitä useimmiten saada kiinni, kannattaa silti jättää rikosilmoitus poliisille. Rikosilmoitus ei ole julkinen ennen kuin syyllinen saadaan kiinni ja nostetaan syytteet. Henkilötietojen vaarantuessa yritys on kuitenkin velvollinen ilmoittamaan tapahtuneesta 72 tunnin kuluessa tietosuojavaltuutetun toimistoon. (Järvinen 2022, 239–240.)

Verkkohyökkäyksestä viestiminen on kriisiviestintää ja se tulee tehdä maltillisesti tilannetta liioittelematta tai vähättelemättä. Henkilökunnan informointi kannattaa toteuttaa joko kasvokkain suullisesti tai puhelimen välityksellä soittamalla tai tekstiviestillä. Sähköpostia ei kannata käyttää muuhun kuin yleisluonteiseen tiedottamiseen, silloin kun hyökkäys on vielä meneillään ja tutkina on kesken. Hyökkäävä taho saattaa aktivoitua tekemään lisävahinkoa, mikäli havaitsee että hyökkäys on huomattu. (Järvinen 2022, 238–239.)

4.4 Kyberhyökkäysten haittavaikutukset

Onnistunut kyberhyökkäys voi aiheuttaa merkittäviä haittavaikutuksia yritykselle. Tietovuotojen yhteydessä voivat asiakkaat kokea, että heidän tietonsa ja rahansa eivät ole enää yrityksessä turvassa. Maineen menetys ja imagotappiot saattavat näin ollen aiheuttaa asiakkuuksien menetyksiä ja markkinaosuuden pienenemistä asiakkaiden siirtyessä kilpailijoille. (CGI Inc 2018, 5.)

Henkilöstön ja asiakkaiden tietojen vuotaminen loukkaa yksityisyyden suojaa ja voi johtaa jopa mittavien vahingonkorvauksien maksuun. Asiantuntijayrityksessä aineettoman omaisuuden menettäminen voi puolestaan vaikuttaa merkittävästi tuotekehitykseen. Kyberhyökkäyksen vuoksi kaatuneet järjestelmät voivat lamaannuttaa yrityksen toiminnan jopa viikoiksi aiheuttaen suuria taloudellisia menetyksiä. Liiketoiminnan jatkuvuus häiriintyy ja pahimmillaan voi aiheuttaa yrityksen toiminnan lakkautumisen kokonaan. (CGI Inc 2018, 5.)

5 Kyberuhat digitaalisessa taloushallinnossa

5.1 Taloushallinnon tehtävät

Yrityksen taloushallinto koostuu monesta eri toiminnosta ja se on erittäin tärkeä osa liiketoimintaa. Taloushallinnon perustehtävä on rekisteröidä liiketapahtumat lain edellyttämällä tavalla siten, että yritys kykenee hoitamaan raportointivelvoitteensa sekä suorittamaan pakolliset päivittäiset liiketoimintaan liittyvät toiminnot. Raportointiin kuuluvat sekä lakisääteiset että sidosryhmille suuntautuva raportointi. (Kaarlejärvi & Salminen 2018, 31.)

Taloushallinnon päivittäisiin toimintoihin kuuluvat muun muassa yrityksen kirjanpidon hoitaminen, ostolaskujen maksaminen, myyntilaskujen tekeminen ja lähettäminen, palkanlaskenta ja maksatus sekä viranomaisilmoitusten tekeminen. Taloushallinnon tärkeisiin tehtäviin kuuluvat myös tilinpäätöksen tekeminen sekä liiketoiminnan tavoitteiden saavuttamisen kannalta oleellinen budjetointi. Yritys voi huolehtia kirjanpidosta itse tai se voi ulkoistaa sen joko osittain tai kokonaan tilitoimistolle, jolloin vastuu kirjanpidon oikeellisuudesta siirtyy sitä hoitavalle taholle. (Visma 2023a.)

Taloushallinnon prosesseista voidaan puhua siinä vaiheessa, kun on kyse yrityksen rahaliikenteestä. Prosesseja voidaan hoitaa joko manuaalisesti perinteisiä menetelmiä käyttäen kirjoittamalla, kopioimalla, arkistoimalla ja prosesseja seuraamalla tai sähköisiä taloushallinnon-ohjelmistoja hyödyntäen, jolloin järjestelmien avulla asiat hoituvat valmiita pohjia hyödyntäen nopeammin, vähemmillä virheillä ja niitä on myös helpompi seurata. Nykyään yrityksissä ensisijaisesti suositaan sähköistä ja digitalisoituvaa taloushallintoa. (Visma 2023a.)

5.2 Taloushallinnon digitalisoituminen

Suomessa taloushallinnon sähköistyminen alkoi jo vuonna 1997, kun lainsäädännön muutos mahdollisti siirtymisen paperisesta taloushallinnosta sähköiseen

taloushallintoon. Aiemmin kaikkien tositteiden ja aineistojen käsittely sekä arkistointi tapahtui lain vaatimusten mukaisesti pääosin paperisessa muodossa ja manuaalisesti. Suomi oli lakimuutoksellaan taloushallinnon sähköistymisessä edelläkävijämaa. Suomalaiset organisaatiot ovat osanneet hyödyntää aina uutta teknologiaa monia muita maita paremmin. Taloushallinnon tehokkuus onkin tällä hetkellä Suomessa maailmanlaajuisestikin verrattuna huippuluokkaa. (Kaarlejärvi & Salminen 2018, 11–12.)

Taloushallinnon digitaalinen kehitys on alkanut Suomessa 1990-luvulla paperittomasta kirjanpidosta. 2000-luvulla siirryttiin sähköiseen taloushallintoon, jota voidaan pitää digitaalisen taloushallinnon esiasteena. Teknologian kehittyessä on 2010-luvulla päästy digitaaliseen taloushallintoon, josta automaatioasteen kasvaessa olemme nyt 2020-luvulla siirtymässä älykkääseen taloushallintoon. (Kaarlejärvi & Salminen 2018, 15–16.)

Merkittävimpiä vaikuttajia nopeaan kehittymiseen ovat olleet sähköisen laskutuksen yleistyminen sekä pilvipalveluiden vakiintuminen yleisimmäksi hankintakanavaksi taloushallinto-ohjelmistoille sekä toiminnanohjausjärjestelmille. Taloushallinto-ohjelmistojen mobiilitoimintojen yleistyminen on vaikuttanut käyttäjäystävällisyyteen lisäten käytön helppoutta ja tehokkuutta sekä aika- ja paikkariippumattomuutta. (Kaarlejärvi & Salminen 2018, 29–30.)

Taloushallinnon ohjelmistoissa hyödynnetään koko ajan enemmän käyttöä tehostavaa ohjelmistorobotiikkaa sekä koneoppimista. Ohjelmistovalmistajat pyrkivät myös integroimaan taloushallinnon mukaan toiminnanohjausratkaisuihin luodakseen eri toimialoille toimivia kokonaisuuksia. Ohjelmistomarkkinoilla muodostetaan laajoja ekosysteemejä ja alustaratkaisuja. Kaikki tämä digitalisoituminen nostaa datan suureen merkitykseen. Ilman dataa ei voida tehdä automaatiota eikä hyödyntää tekoälyä. Digitaalisessa muodossa olevaa dataa tarvitaan myös liiketoimintapalveluiden ja tiedolla johtamisen mahdollisuuksien kehittämisessä. (Kaarlejärvi & Salminen 2018, 30.)

5.3 Muutosvaiheen riskit

Digitaalisen taloushallinnon käyttöönoton suunnittelussa on tärkeää huomioida riskeissä esimerkiksi käyttökatkot, tietokaappaukset sekä virukset ja pyrkiä vähentämään tai sulkemaan niiden mahdollisuus pois (Elisa Jämsén 2019). Taloushallinto-ohjelmiston tietoturvariskejä voi minimoida hankkimalla digitaalisen taloushallinnon ohjelmiston pitkään markkinoilla toimineelta toimittajalta, jolla on kokemusta ohjelmistojen kehittämisestä sekä ylläpidosta ja joka tuntee viranomaismääräykset. Alalla pitkään toimineet taloushallinto- ja kirjanpito-ohjelmistojen toimittajayritykset osaavat huolehtia tietoturvasta ja tietojen oikeanlaisesta digitaalisesta arkistoinnista. (Visma 2023b.)

Siirryttäessä digitaalisiin järjestelmiin tulee huomioida muutoshankkeen riskit ja valita tietoturvallinen, sekä kirjanpitoon ja talouden hallintaan liittyvät viranomaismääräykset täyttävä ohjelmisto. Tulee myös huolehtia, että työntekijät osaavat käyttää ohjelmistoa oikein. Tilitoimistojen työntekijöiden mielestä etenkin muutosten aikana suurimmat riskit liittyvät osaamiseen ja työn resursointiin. Muutokseen huolellisesti valmistautumalla sekä varmistamalla tarvittava tuki käyttöönottoprosessin aikana ja sen jälkeen, voidaan riskejä pienentää. (Visma 2023b.)

Muutostilanteissa pelkästään huonolla suunnittelulla ja omalla toiminnalla voidaan aiheuttaa tahaton kyberpoikkeama ja saada aikaan kriittisten toimintojen häiriintyminen. Hyvänä esimerkkinä uuden järjestelmän käyttöönottovaiheen haasteista on Helsingin kaupungin siirtyminen uuteen Sarastia -palkkajärjestelmään keväällä 2022. Puutteellisen johtamisen, tiukan aikataulun, käyttäjien osaamattomuuden sekä järjestelmän teknisten ongelmien vuoksi palkanmaksu ajautui totaaliseen kaaokseen. Palkanmaksussa on muutoksen jälkeen ollut tuhansia virheitä, ja osa työntekijöistä on jäänyt jopa kokonaan palkatta. Palkkasotkun selvittäminen on tullut maksamaan kaupungille miljoonia euroja ja kesällä 2023 selvitykset jatkuivat edelleen. (Karppi & Kulmanen 2023.)

5.4 Muita riskitekijöitä

Taloushallinnossa käsitellään päivittäin rikollisia kiinnostavaa aineistoa, kuten yrityksen maksuliikennettä, asiakastietoja, henkilökunnan henkilötietoja ja liikesalaisuuksia. Tietokoneilla on paljon niin sanottua kyberomaisuutta, jota rikolliset voivat käyttää kauppatavarana tai hyödyntää muutoin rikollisessa toiminnassa. Yrityksen kyberomaisuudeksi voidaan lukea muun muassa IPR-tiedot ja patenttitiedot, asiakastiedot, henkilökunnan tiedot, rahaliikenne, tarjoukset, yrityksen sähköposti, talousluvut, asiakassuunnitelmat, tuotekehitystiedot, tuotetiedot sekä yrityskauppoja koskevat tiedot. (Peltomäki & Norppa 2015, 61–63.)

Etenkin pienyrityksillä sekä yrittäjillä on paljon erilaisia sähköpostipalveluita ja -ohjelmia käytössä, joiden tiedonkulun sekä tiedon säilytyksen tietoturvallisuudesta ei ole täyttä varmuutta. Sähköpostien lähetyksessä tyypillisenä riskinä on sähköpostiosoitteen virheellinen kirjoitus, jolloin viesti menee väärälle henkilölle. Sähköposti toimii usein myös asiakkaiden tietojen kalastelun välineenä ja joku voi esimerkiksi kysellä tietoja esiintyen asiakkaana väärentämällä viestin lähettäjätiedot. Paljon tietojen välittämisessä käytettyä Dropboxia sekä muita vastaavia tiedostojen jakoon tarkoitettuja pilvitallennuspalveluja on käytetty myös tietojen kalasteluun. (Palkkaus.fi 2023.)

Sähköpostia ei kannata pitää luottamuksellisen tiedon arkistointipaikkana, koska sähköpostidata saatetaan varastaa, jolloin tieto päätyy vääriin käsiin. Kirjanpitodatan, työntekijöiden palkkatietojen tai muiden henkilökohtaisten tietojen lähetys sähköpostilla on tietoturvariski ja tietojen menetys voi aiheuttaa merkittävän mainehaitan. Sähköpostin avulla voidaan tehdä tietomurtoja, mutta haitallisia ohjelmistoja voi tulla tietokoneelle myös muistitikkujen tai siirrettävien massamuistien kautta. (Palkkaus.fi 2023.)

Luottamuksellisen tiedon tulisi kulkea aina tietoturvallisesti työntekijöiden, asiakasyrityksen ja tilitoimiston välillä. Viranomaisille tieto välitetään aina omien turvapostien kautta. Asiakasdataa kertyy tilitoimistojen säilytykseen todella paljon ja paperisen arkistoinnin sijaan tietoa siirretään sähköisiin järjestelmiin. Varmuuskopiointi on todella tärkeä osa asiakasdatan arkistointia. Mikäli yrityksen

tietojärjestelmät joutuvat esimerkiksi kiristysohjelman uhriksi, varmuuskopioiden avulla toiminnot saadaan nopeasti palautettua. (Palkkaus.fi 2023.)

Käytössä olevien tietokoneiden virustorjuntaohjelmistot tulee pitää päivitettyinä. Asiakkaiden dataa käsitellessä henkilötunnuksia kannattaa käyttää todella harkiten ja suosia jotain muuta tunnistetta esimerkiksi Exceliin tehtävissä listauksissa. Puhelimessakin tulee välttää luottamuksellisen tiedon välittämistä, jollei henkilökohtaisesti tunne soittajaa. Esimerkiksi identiteettivarkauksissa tyypillinen tietojen kalastelun keino on puhelimella soittaminen. (Palkkaus.fi 2023.)

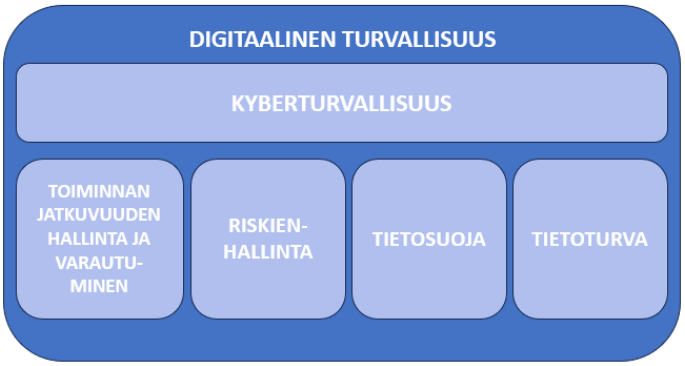
Paperisten sopimusten lisäksi, nykyään voidaan tehdä sopimuksia digitaalisesti vahvan sähköisen allekirjoituksen avulla, jossa tunnistautuminen tapahtuu verkkopankkitunnuksilla, mobiilivarmenteella tai henkilökortilla. Allekirjoitusprosessi nopeutuu, arkistointi on helpompaa ja allekirjoittajan tiedot ovat varmasti oikein, kun esimerkiksi kirjoitusvirheiden mahdollisuus poistuu. Tietoturvaan ja tietosuojaan kuuluu digitaalisen datan lisäksi myös fyysisiä asioita ja esimerkiksi arkistoidun asiakasdatan suojaaminen tulipalolta, ulkopuolisilta käyttäjiltä tai muulta uhkaavalta tekijältä tulisi ottaa huomioon. (Palkkaus.fi 2023.)

5.5 Varautuminen

Hanna Kangasniemen (2023) haastatteleman Taloushallintoliiton toimitusjohtajan Jari Sepän mukaan, tällä hetkellä taloushallinnon alaan kohdistuvat uhkat ovat tyypillisesti tietojen kalastelua, toimitusjohtajahuijauksia ja muita erilaisia tietoturvaloukkauksia sekä palvelunestohyökkäyksiä. Seppä kertoo, että tietoturvaosaaminen on taloushallinnon alalla hyvin vaihtelevaa, vaikka uhkien määrä on kasvanut. (Kangasniemi 2023.)

Yrityksen tietoturvasta sekä tietosuojasta tulisi huolehtia tarkasti. Taloushallintoliiton johtaja korostaa alalla työskentelevien tietoturvaosaamisen ja -tietoisuuden kasvattamisen tärkeyttä ja muistuttaa kuinka huolimattomuus ja tietoturvan laiminlyönti voi tulla yritykselle kalliiksi. Tietoturvan tulisi olla ajan tasalla ja hyökkäyksiin olisi varauduttava ennakkoon, etteivät tilitoimistojen keskeiset

toiminnot vaarannu. (Kangasniemi 2023.) Kuviossa 5 on esitettynä digitaalisen turvallisuuden osa-alueet.



Kuvio 5. Digitaalisen turvallisuuden osa-alueet (mukaillen Väestörekisterikeskus 2019, 15).

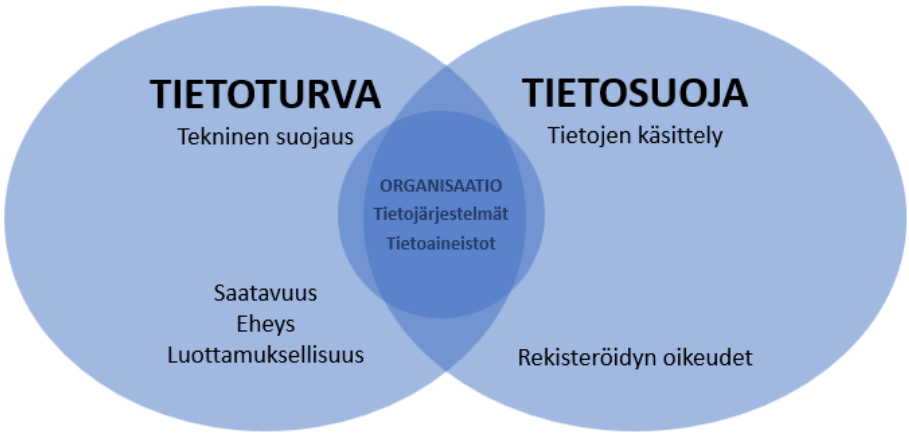
Taloushallintoliiton taloushallinnon johtava asiantuntija Janne Fredman (2022) muistuttaa artikkelissaan ”Venäjän kyberuhka ja tilitoimistot” tilitoimistojen kyberturvallisuuden korostuneesta merkityksestä. Hän suosittelee tilitoimistoja valmistautumaan häiriöihin ja miettimään jo ennakkoon mitä tehdä kriisitilanteissa. Tilitoimistoissa käsiteltävien tietojen arkaluonteisuus ja Venäjän suunnalta kasvanut uhka muun kyberrikollisuuden lisäksi, ovat painava syy siihen, että tietoturvaan liittyvien teknisten toimintojen ja sovittujen prosessien tulee olla ehdottomasti kunnossa. Ohjelmistojen toimivuuden, pilvipalvelujen tietoturvan sekä maksuliikenteen jatkuvuuden takaamiseksi, on yhteistyön merkityksellä eri palveluntarjoajien välillä suuri. Kriisitilanteissakin tulisi varmistaa toiminnan jatkuvuus. (Fredman 2022.)

Nixu Oy:n kyberturvallisuusjohtaja Antti Nuopponen (2018) korostaa artikkelissaan ”Huijarit horjuttavat taloushallinnon kyberturvaa” työntekijöiden valveutuneisuuden tärkeyttä. Pelkästään laitteiden suojauksien ja vahvojen tunnistautumisten avulla ei huijauksilta pystytä suojautumaan, vaan nämä tulisi ottaa huomioon myös taloushallinnon prosesseissa. Henkilökunnan tietoisuuden nostamisella sekä koulutuksilla on suuri merkitys kyberuhkien tunnistamisessa. Taloushallintoon kohdistuvista kyberrikoksista useimmat perustuvat erilaisiin huijauksiin, joiden tavoitteena on saada yritys maksamaan rikollisille rahaa. (Nuopponen 2018.)

5.6 Tietosuoja-asetus ja tietoturva

Tietosuoja-asetus eli GDPR tuli voimaan vuonna 2018 ja se velvoittaa myös taloushallinnonalan toimijoita käsittelemään asiakkaiden henkilötietoja aina tietosuojaperiaatteiden mukaisesti. Henkilötietojen turvalliseen käsittelyyn, rekisteröintiin, säilytykseen ja poistoon annetut ohjeistukset on määritelty laissa ja niiden noudattamista valvotaan. Tietoturvaloukkaus voi olla esimerkiksi hakkerointi, kyberhyökkäys, haittaohjelmatartunta, kadonnut USB tikku, varastettu tietokone tai tiliotteen toimittaminen väärälle henkilölle. Tietoturvaloukkauksista tulee ilmoittaa valvontaviranomaisille 72 tunnin kuluessa ja ilmoittamatta jättämisestä voi koitua rekisterinpitäjälle seuraamuksia. (Tietosuojavaltuutetun toimisto 2023a; Tietosuojavaltuutetun toimisto 2023b.)

Tietosuojan toteutuminen on mahdollista tietoturvan avulla, jonka tarkoituksena on suojata tietojärjestelmiä sekä tietoaineistoa ja varmistaa niiden luottamuksellisuus, eheys sekä järjestelmien käytettävyys eli tiedon saatavuus. Tietoturva kuuluu tietosuojan teknisiin toimenpiteisiin, jolla varmistetaan, että rekisteröidyn oikeudet toteutuvat (kuvio 6). (Tietosuojavaltuutetun toimisto 2023c.) Tietoturvaa koskevassa NIS-direktiivissä on säädetty huoltovarmuuskriittisiin sektoreihin kuuluvien toimijoiden tietoturvavelvollisuuksista ja tietoturvahäiriöistä ilmoittamisesta. Taloushallinnonala ei kuulu NIS-direktiivin velvoitteiden ja valvonnan piiriin. (Liikenne- ja viestintävirasto Traficom 2023c.)



Kuvio 6. Tietoturva varmistaa tietosuojan toteutumisen (Tietosuojavaltuutetun toimisto 2023c).

Taloushallintoliitossa on tehty havaintoja tilitoimistotarkastusten sekä jäsenneuvonnan yhteydessä, että tietoturvaan ja tietosuojaan liittyvässä toimialakohtaisessa ohjeistuksessa on puutteita (Manninen 2019). Taloushallintoliitto tekee jäsenyrityksilleen tilitoimistotarkastuksia noin viiden vuoden välein ja niissä käytetään tietoturvan ja tietosuojan tason selvitykseen itsearviointilomakkeita. Tilitoimistoalan yrityksiä on Suomessa tällä hetkellä noin 6 200 ja niistä Taloushallintoliiton auktorisoimia jäseniä on vajaat 600. Keskikoko alan yrityksillä on kaksi henkilöä. (Suomen Taloushallintoliitto ry 2023a, Suomen Taloushallintoliitto ry 2023b.)

5.7 Taloushallinnon tehtävien kriittisyys

Taloushallintoliiton toimitusjohtaja Jari Seppä, kertoo Hanna Kangasniemen (2023) tekemässä haastattelussa, kuinka kokonaisvaltaisesti taloushallintoalan palveluiden lamaantuminen vaikuttaisi yhteiskunnan rahaliikenteeseen. Taloushallinnon toiminnot koskettavat monia aloja ja toimintojen häiriintyessä esimerkiksi pankkien suorittamat maksut pysähtyisivät puutteellisten tietojen vuoksi. Huoltovarmuuden ja yhteiskunnan toimivuuden kannalta kriittisen maksuliikenteen, kuten palkkojen ja yritysten laskutuksen ja maksujen pysähtyminen lakkauttaisi yksitellen yhteiskunnan toiminnot. (Kangasniemi 2023.)

Tilitoimistoihin kohdistuva kyberhyökkäys voisi pahimmillaan pysäyttää avaintoimintoihin kuuluvien palkkalaskelmien teon ja pk-sektorin maksuliikenteen hoitamisen. Jos pankit eivät saisi tilitoimistoilta palkanmaksuaineistoja jäisi kuukausitasolla noin miljoona palkkalaskelmaa laskematta ja yli puolet pk-sektorin maksuista hoitamatta. Useiden viikkojen käyttökatko järjestelmissä olisi vaikutuksiltaan erittäin mittava ja koskettaisi suuria määriä ihmisiä. (Kangasniemi 2023.)

Maaliskuussa 2023 joutui kaksi suomalaista ohjelmistoyhtiötä kyberhyökkäyksen kohteeksi. Tämä on herättänyt huolta myös Taloushallintoliitossa. Kerrannaisvaikutukset nousevat nopeasti suuriksi maksuliikenteen osalta, jos ohjelmistotalo joutuu sulkemaan palvelimensa korjausten ajaksi taloushallinnonalan toimijoilta. (Kangasniemi 2023.)

Hyvänä esimerkkinä taloushallinnon toimintojen häiriintymisen laaja-alaisista vaikutuksista, on vuonna 2017 Ukrainaan kohdistunut kyberhyökkäys, joka tehtiin suositun ukrainalaisen taloushallinnon sovelluksen avulla. M.E.Doc on ohjelma, jolla voi tehdä yrityksen kirjanpidon sekä ilmoittaa tiedot verottajalle. Hyökkääjät murtautuivat ohjelmaa valmistavan yrityksen päivityspalvelimelle ja lisäsivät sinne oman koodinsa. Tätä kautta hyökkääjät laittoivat jakoon kiintolevyn tietoalueita tuhoavan NotPetya-kiristysohjelman. M.E.Doc -sovellusta käyttää noin 80 prosenttia ukrainalaisista yrityksistä, joten kun päivitykseksi naamioitu saastunut versio laitettiin liikkeelle, se levisi maan sisällä tehokkaasti. (Järvinen 2018, 49.)

Hyökkäys vaikutti erittäin rajusti eri alan toimijoihin. Toiminta häiriintyi muun muassa Kiovan lentokentällä, bensa-asemilla, metrojen maksukorteissa, valtion pankissa ja monissa pienemmissä yrityksissä. Hyökkäyksessä NotPetya levisi sisäverkon kautta myös lukuisiin kansainvälisiin yrityksiin, joilla oli tytäryhtiö Ukrainassa, mutta tietoturva ei ollut päivitettynä ajan tasalle. Usealle iskusta kärsineelle yritykselle tuli jopa satojen miljoonien dollareiden tappioita, joten taloudellinen vaikutus oli kokonaisuudessaan valtava. Jälkiselvityksessä selvisi, ettei M.C.Docin palvelinohjelmistoa ollut päivitetty kolmeen vuoteen. Ohjelmistoon murtautuminen oli näin ollen hyökkääjille helppoa ja he olivat olleet verkossa jo useiden viikkojen ajan ennen iskua. (Järvinen 2018, 49–50.)

6 Tutkimuksen menetelmät, tavoite ja toteutus

6.1 Tutkimusmenetelmät

Opinnäytetyössä on käytetty laadullista eli kvalitatiivista tutkimusta. Laadullisen tutkimuksen avulla saadaan kokonaisvaltaista ja yksityiskohtaista tutkimustietoa luotettavien lähdetietojen sekä asiantuntijoiden avulla. Lähdeaineiston avulla tutkimusilmiöön tutustutaan monipuolisesti eri katsantokannoilta ja näin tutkimukseen luodaan syvyyttä sekä laajuutta. Kvalitatiivinen tutkimus sisältää

useita erilaisia tapoja lähestymisessä, aineistonkeruussa sekä analysointimenetelmissä. (Saaranen-Kauppinen & Puusniekka 2006.)

Tutkimusmenetelminä opinnäytetyössä on käytetty rinnakkain narratiivista kirjallisuuskatsausta sekä asiantuntijahaastatteluja. Kirjallisuuskatsauksessa tutkimusaineiston avulla pyritään vastaamaan tutkimuskysymykseen. Kirjallisuuskatsaus jaetaan kolmeen päätyyppiin, jotka ovat systemaattinen kirjallisuuskatsaus, kuvaileva kirjallisuuskatsaus ja meta-analyysi. Narratiivinen kirjallisuuskatsaus on toinen kuvailevan kirjallisuuskatsauksen pääluokista ja siinä on pyrkimyksenä saada tutkittavasta ilmiöstä mahdollisimman laaja-alainen kokonaiskuva. (Mannila 2021.)

Kirjallisuuskatsauksen aineistona opinnäytetyössä käytettiin ajankohtaisia artikkeleita, tietoturva- ja kyberturvallisuusoppaita sekä muuta alan kirjallisuutta. Kirjallisuuden lähteet koostuivat pitkään alalla toimineiden tietoturva- ja ICT-alan ammattilaisten teoksista, joissa on hyödynnetty kyberturvallisuusasiantuntijoiden ja viranomaistahojen lausuntoja sekä esitetty runsaasti esimerkkitapauksia. Tutkimuksessa olen käyttänyt viranomaislähteinä muun muassa Liikenne- ja viestintäviraston Traficomin Kyberturvallisuuskeskuksen, Ulko- ja Sisäministeriön, Työ- ja elinkeinoministeriön sekä Valtiovarainministeriön verkkosivuja sekä julkaisuja.

Kirjallisuuskatsauksen avulla sain kerättyä tarvittavaa pohjatietoa asiantuntijahaastattelujen tekoon. Tutkimuksen asiantuntijahaastattelut toteutettiin puolistrukturoituina teemahaastatteluina. Haastattelu on hyvä tutkimusmenetelmä, kun halutaan tuottaa aineistoa ja tietoa, jolla pystytään vastaamaan tiettyyn tutkimusongelmaan. Laadullista haastattelua tehdessä on hyvä, että haastateltava voi vastata kysymyksiin omin sanoin ja tarvittavalla laajuudella. (Hyvärinen, Suoninen & Vuori 2023.)

Teemahaastattelussa haastattelija kysyy valitsemansa teeman mukaisesti aiheesta, johon on perehtynyt kirjallisuuden avulla. Puolistrukturoituun haastatteluun valmistellaan kysymykset ennakkoon, mutta ne voidaan tarvittaessa esittää eri muodossa tai järjestyksessä ja vastaajalla on vapaus vastata haluamallaan

tavalla. Asiantuntijahaastattelussa tavoitteena on saada selville, kuinka esimerkiksi yritykset käsittelevät tutkittavaa asiaa omissa toimissaan. (Hyvärinen ym. 2023.)

Analysointimenetelmänä tutkimuksessa käytettiin teemoittelua. Teemoittelussa nostetaan aineistosta esille usein esiintyviä tutkimusongelman kannalta keskeisiä asiakokonaisuuksia ja aiheita eli teemoja. Teemoittelua voidaan havainnollistaa tutkimusraportissa aineistosta kerättyjen sitaattien avulla. Teema-analyysiä käytetään usein haastatteluaineiston analysoimisessa. Huomioitavaa on, että teemat eivät ole samoja kuin haastatteluun ennakkoon mietityt teemat, vaan ne ovat haastatteluaineiston analyysin tuloksena syntyneitä teemoja. (Juhila 2023.)

6.2 Tutkimuksen tavoite

Tutkimuksen tavoitteena oli saada opinnäytetyön tutkimuskysymykseen taloushallinnon alaa koskevaa ajantasaista tietoa mahdollisimman laaja-alaisesti ja monesta eri näkökulmasta. Asiantuntijahaastatteluissa tavoitteena oli saada selville taloushallinnon alaa uhkaavien kyberuhkien sekä yritysten varautumisen tason tilannetta taloushallinnon sekä kyberturvallisuusalan asiantuntijoiden näkökulmasta katsottuna. Haastattelututkimuksen asiantuntijat ovat lueteltuna taulukossa 1.

HAASTATTELUT	
Haastattelu 1	Yrittäjä, Tilitoimisto Tili-Satu Oy Satu Ryhänen
	Taloushallinnon asiantuntija KLT, Tilitoimisto Tili-Satu Oy Mika Ryhänen
Haastattelu 2	Tietoturvajohtaja, Elisa Oyj Teemu Mäkelä
Haastattelu 3	Taloushallinnon johtava asiantuntija, Suomen Taloushallintoliitto ry Janne Fredman

Taulukko 1. Asiantuntijahaastattelut

Ensimmäisessä haastattelussa haastateltavana oli joensuulaisen Tilitoimisto Tili-Satu Oy:n yrittäjä Satu Ryhänen, sekä yrityksessä taloushallinnon asiantuntijana (KLT) ja neuvonantajana toimivan Mika Ryhänen. Tilitoimisto Tili-Satu Oy on ollut toiminnassa jo 20 vuoden ajan ja sitä ennen yrittäjä Satu Ryhänen on työskennellyt taloushallinnon alalla noin kymmenen vuoden ajan.

Mika Ryhäsellä on myös yli 30 vuoden kokemus taloushallinnon alalta ja hän on aiemmin työskennellyt muun muassa yhdessä Suomen suurimmista taloushallinnon palveluja tarjoavista yrityksistä. Hän vastaa tällä hetkellä myös Tili-Satu Oy:n ohjelmistoihin ja tietoturvaan liittyvistä asioista. Tämän haastattelun tavoitteena oli saada pitkään työskennelleiden asiantuntijoiden näkökulmaa digitalisoitumisen vaikutuksista taloushallinnon alalla, sekä päivittäisessä työssä havaituista kyberuhkista ja arvioita tilitoimistojen varautumisen tasosta.

Toiseen haastatteluun sain haastateltavaksi Elisa Oyj:n tietoturvajohtajan Teemu Mäkelän, joka vastaa Elisalla kyberturvallisuuden johtamisesta ja kehittämisestä. Hän on työskennellyt tietoturva- ja tietoliikenne alalla sekä kansainvälisissä ICT-alan yrityksissä ansioituneesti jo lähes 20 vuoden ajan. Mäkelä on saanut myös Tietoturva ry:ltä Vuoden Tietoturvapäällikkö -tunnustuksen vuonna 2020. (Business Insight Group 2023.) Tällä haastattelulla tavoiteltiin vastauksia opinnäytetyön tutkimuskysymykseen tieto- ja kyberturvallisuusalan asiantuntijan sekä turvallisuuspalveluja tarjoavan yrityksen kannalta katsottuna.

Kolmanteen asiantuntijahaastatteluun sain haastateltavaksi Janne Fredmanin. Fredman toimii Taloushallintoliiton taloushallinnon johtavana asiantuntijana sekä Tilisanomien päätoimittajana. Tämän haastattelun tavoitteena oli saada tarkennusta aiemmista haastatteluista saamiini tietoihin. Tavoitteena oli myös saada tietoa alalla toimivien tilitoimistojen tilanteesta hieman laajemmin Taloushallintoliiton näkökulmasta katsottuna.

6.3 Tutkimuksen toteutus

Asiantuntijahaastattelut toteutettiin siten, että haastattelin kaikkia asiantuntijoita henkilökohtaisesti. Kaikkiin haastatteluihin laadin omat teeman mukaiset haastattelukysymykset (liite 1). Ensimmäinen haastattelu tehtiin kesäkuussa 2023 Tilitoimisto Tili-Satu Oy:n tiloissa ryhmähaastatteluna. Satu ja Mika Ryhänen eivät halunneet, että haastattelua nauhoitetaan, joten aineiston tallennus tapahtui käsin kirjoittamalla haastattelun lomassa. Tämän haastattelun osalta opinnäytetyössä käytetyt viittaukset perustuvat näihin muistiinpanoihin. Tietoturvajohtajana toimivanTeemu Mäkelän haastattelu toteutettiin elokuussa 2023 videopuheluna Microsoft Teamsin välityksellä ja haastatteluvideo tallennettiin Teamsiin.

Taloushallinnon johtavan asiantuntijan Janne Fredmanin haastattelu toteutettiin syyskuussa 2023 puhelimitse. Alkuperäinen suunnitelma oli toteuttaa haastattelu videopuheluna Teamsin välityksellä, mutta ääniteknisten ongelmien vuoksi teimme haastattelun puhelimitse siten, että kuva tuli Teamsin välityksellä. Tämän vuoksi en pystynyt hyödyntämään Teamsin äänitallennusta, joten tein tämänkin haastattelun aikana muistiinpanot käsin.

Heti haastattelujen jälkeen kirjoitin tekemäni muistiinpanot puhtaaksi tekstinkäsittelyohjelmalla. Mäkelän haastattelu on litteroitu tekstimuotoon tallenteelta tekstinkäsittelyohjelmaa hyödyntäen siten, että puheesta on karsittu toistot ja täytesanat. Litterointi tarkoittaa puheen muuttamista tekstimuotoon ja se voidaan tehdä eri tarkkuuksilla. Kun halutaan saada tietoa haastateltavan näkökulmista tiettyyn ilmiöön, litterointitarkkuudeksi riittää, että puheen sisältö ja haastateltavan asia tulevat ymmärretyksi, jolloin takeltelut, tauot ja muut asiaan kuulumattomat yksityiskohdat ovat merkityksettömiä. (Kallio 2023.)

Haastattelujen litterointi eli puhtaaksikirjoitusvaiheessa tein havaintoja kerätystä aineistosta ja kirjasin ylös tutkimusongelman kannalta olennaisia toistuvia aiheita teemoittelua varten. Haastatteluista saadun aineiston analysoinnissa teemoiksi nousivat muutos digitaaliseen taloushallintoon, palveluntarjoajat, ohjelmistot, pilvipalvelut, kyberuhka, varautuminen, varmuuskopiointi, riskienhallinta, tietoturva ja toimenpiteet. Teemoissa varautuminen, riskienhallinta, tietoturva ja

toimenpiteet oli lisäksi havaittavissa eroja pienien ja suurten tilitoimistojen välillä. Haastatteluissa esiin nousseet teemat sekä pienten ja suurten tilitoimistojen erot on esitetty koostetusti taulukossa (liite 2). Tutkimuksen tuloksien vertailussa hyödynsin aiempaa aiheeseen liittyvää opinnäytetyötä sekä tutkimusta.

7 Tulokset ja niiden analysointi

7.1 Muutos digitaaliseen taloushallintoon

Tutkimuksessa ilmeni, että taloushallinnon alalla tehdään vielä paljon töitä paperisessa muodossa. Monet alan toimijat eivät ole vielä siirtyneet digitaaliseen taloushallintoon omista tai asiakkaista johtuvista syistä. Tilitoimiston yrittäjän Satu Ryhäsen sekä tilitoimistossa kirjanpitäjänä ja tietoturvavastaavana toimivan Mika Ryhäsen haastattelussa selvisi, että asiakkaista etenkin pienemmät yritykset toimittavat usein materiaalinsa edelleen paperisena. Asiakkaat saattavat vastustaa ja kyseenalaistaa muutosta, mutta yleensä kuitenkin haluavat siirtyä digitaalisiin menetelmiin käytännön syistä viimeistään silloin kun yrityksen koko on suurempi.

Tutkimus osoittaa, että siirtymävaihetta paperisesta järjestelmästä digitaaliseen taloushallintoon tai jo käytössä olevan ohjelmiston vaihtoa uuteen voidaan pitää tilitoimistoissa riskialttiina vaiheena. Alussa uuden ohjelmiston käytön opettelu hidastaa työntekoa ja pitkään alalla olleista voi tuntua, että osaisi tehdä työt nopeammin vanhoilla totutuilla menetelmillä. Tämä voi aiheuttaa muutosvastarintaa työntekijöissä. Satu Ryhänen toteaa myös, että jos uusia ohjelmistoja ei osata käyttää, niin niistä ei saada kaikkea hyötyä irti ja osaamattomuuden vuoksi saattaa tulla myös virheitä. Niitä voi tulla esimerkiksi tietoja kirjatessa ja riskinä on, että voi mennä pitkäänkin ennen kuin virhe huomataan.

Riskialttiissa muutos- ja siirtymävaiheissa Elisan tietoturvajohtajana toimiva Teemu Mäkelä kehottaa miettimään tietoturvan kolmijalkaa, joka on tiedon luottamuksellisuus, saatavuus ja eheys. Hän muistuttaa, että muutostilanteissa

tulisi huolehtia, että käyttäjät osaavat käyttää järjestelmiä ennen käyttöönottoa. Yrityksen työntekijät voivat omalla virheellisellä toiminnallaan vaikuttaa esimerkiksi tiedon eheyteen. Vaikeita asioita lähdetään helposti kiertämää ja tietoja kirjoitellaan erinäisille muistilapuille tai voidaan jotenkin muutoin käsitellä epämääräisesti. Esimerkiksi kalasteluhyökkäyksissä rikolliset etsivät ihmisen psykologisia heikkouksia ja tällaiset muutostilanteet ovat juuri sellaisia potentiaalisia hetkiä, joita hyödynnetään.

7.2 Palveluntarjoajat, ohjelmistot ja pilvipalvelut

Tutkimuksen mukaan tilitoimistoissa luotetaan tieto- ja kyberturvallisuudessa ohjelmistojen sekä pilvipalveluiden palveluntarjoajiin. Pilvipalveluissa turvallisena pidetään kotimaisia palveluntarjoajia, joilla on myös serverit EU-alueella. Kehittyneet kirjautumismenetelmät, varmenteet ja kirjautumissovellukset koetaan turvallisiksi menetelmiksi. Toimintavarmuus on nykypäivänä ohjelmistoissa hyvä ja suurempia katkoksia tulee todella harvoin. Internetyhteyksien paraneminen on myös vaikuttanut omalta osaltaan positiivisesti toimivuuteen.

Mäkelä muistuttaa, että suojaukset kuten monivaiheinen tunnistautuminen suojaavat ohjelman käyttöliittymää ja sitä että käyttö on turvallista, mutta se ei välttämättä takaa tietojen säilymistä. Pilvipalvelun luotettavuutta arvioitaessa olisi Mäkelän mielestä hyvä olla jokin luotettava leima tai sertifiointi, ettei olla pelkästään palveluntarjoajan kertoman varassa.

> – – Kun on tämmöinen pieni toimija. Ne on käytännössä sen varassa mitä heille kerrotaan, ei ole mitään kyvykkyyttä tarkastaa mitään.– – Pitäs olla joku leima tai sertifiointi tai joku johon voi luottaa, muutenhan sä oot täysin sen varassa. (Mäkelä)

Mäkelän mukaan pilvipalvelun konesalin sijainti ei ole pelkästään tae luotettavuudesta vaan kannattaa myös selvittää mistä toimija on kotoisin eli minkä maan lainsäädännön velvoittamaa toiminta on. Amerikkalaisella toimijalla voi olla konesali Euroopassa, mutta sitä velvoittaa kuitenkin oman maan lait siirtämään tiedot Amerikkaan. Mäkelä muistuttaa, että esimerkiksi kiinalaisilla on

sellainen lainsäädäntö, että Kiinan valtio voi ryhtyä hoitamaan yritystä ja sanoa yrityksen hallitukselle ja toimitusjohtajalle, että kuinka toimitaan. Sama määräysvalta pätee myös yksittäiseen työntekijään, joka voisi vaikuttaa esimerkiksi pilvipalvelun toimintaan ja tietojen käsittelyyn.

7.3 Taloushallintoa uhkaavat kyberuhat

Tutkimuksessa selvisi, että taloushallinnon alan toimijoihin eniten kohdistuvia ja havaittuja uhkia ovat tietojen kalastelu, toimitusjohtajahuijaukset sekä Microsoft sähköpostitilien kaappaukset. Tilien kaappaukset ovat ilmenneet siten, että eri tileiltä on tullut kutsuja tiedostojen jakoon. Rikollisille rahallisesti kannattavat toimitusjohtajahuijaukset ovat hyvin yleisiä ja pitkälle kehittyneitä sekä entistä kohdennetumpia. Suurimpana motiivina hyökkäyksille pidettiin rahaa. Rahan menetystäkin suurempana haittana Fredman kuitenkin pitää henkilötietojen ja yritys-salaisuuksien joutumista vääriin käsiin.

Eniten toimintaa haittaavina uhkina pidettiin ohjelmistojen ja pilvipalveluiden palveluntarjoajiin kohdistuvia palvelunestohyökkäyksiä. Taloushallinnon ohjelmiston käytön estymisellä ja rahaliikenteen pysähtymisellä voisi olla merkittävän laajat vaikutukset. Fredman kertoo, että tällä hetkellä tietoturva asiantuntijoiden mukaan kyberuhkien määrä on taloushallinnon alalla kasvussa. Pilvipalveluihin kohdistuneet palvelunestohyökkäykset ovat aiheuttaneet joillekin toimijoille jopa muutaman päivän kestäneitä käyttökatkoja. Satu ja Mika Ryhäsen arvion mukaan heidän omassa toimistossaan ei olla huomattu mitään selkeää kasvua kyberhyökkäyksissä, ja esimerkiksi roskapostien määrät ovat ehkä jopa hieman vähentyneet.

Eniten käytetyksi hyökkäystavaksi nousi tutkimuksessa sähköposti. Mäkelä kertoo, että tietojen kalastelussa rikolliset hyödyntävät usein ihmisten uteliaisuutta. Saatetaan houkutella avaamaan haitallinen linkki esimerkiksi kertomalla, että se sisältää pikkujoulukuvia ja vastaanottaja avaa sen uteliaisuuttaan. Yleisimpiä syitä huijauksen onnistumiselle onkin Mäkelän mukaan uteliaisuus, pelko ja

kiire. Suojaamattomien IoT-laitteiden myötä sisäverkkoon tulevat kyberuhat tulisi Mäkelän mukaan huomioida sekä kotona että toimistossa.

> Yleensä on helpoin tapa se, että hyödynnetään ihmisen tekemää virhettä jollain tavalla. Joko se on tää tämmöinen kalastelu tai joku muu huijaus. Tai sitten luodataan niitä laitteita mitä sinne verkkoon on jätetty kaikkien nähtäville ja katsotaan, että minkälaisia heikkouksia siellä on ja mennään niitten kautta. Ne on sitten näitä haavoittuvuuksia. Ihmisen virhe sekin on tietenkin, kun sinne on semmoinen jätetty. Ne on niitä mitä ehkä kuluttaja viljelee eniten tuonne verkkoon. (Mäkelä)

Etenkin suurempien tilitoimistojen uhkatekijöiksi nousivat tutkimuksessa myös sisäiset uhat, jossa henkilökuntaan kuuluva urkkii tai vuotaa tietoja esimerkiksi kilpailijalle tai rikollisille. Mäkelän mukaan rikolliset eivät enää jaksa aina taistella laitteiden ja kehittyneiden palomuurien kanssa, vaan saatetaan yrittää päästä tietoihin käsiksi yksittäisen työntekijän kautta lahjomalla tai kiristämällä. Tutkimuksessa uutena hyökkäystapana hän nostaa esiin myös toimitusketjuhyökkäyksen, jossa suurten yritysten järjestelmiin yritetään päästä pienempien yrityksien kautta.

> Rikolliset on keksinyt tämmöisen, kutsutaan toimitusketjuhyökkäykseksi, missä saattaa olla, että on iso pankki vaikka, joka on tehnyt tietoturvaa vuosia ja kohtuu hyvät kyvykkyydet siellä. Niin ei sen hyökkääjän kannata sitä koestaa ja yrittää päästä, vaan se menee sitten sieltä, kun siellä on joku kahden hengen alihankkija, joka tekee sille jotain pikku pätkää siellä. Jos on luottamusketju rakennettu ja ovet auki, niin menee sen kautta sinne pankkiin sitten. Nää on näitä uusimpia uhkia sitten mitä tuolla on.– – Se pieni taloushallinnon yritys voi olla pomppulauta sinne varsinaiseen kohteeseen ja sitten puhutaan siitä toimitusketjuhyökkäyksestä. (Mäkelä)

Hyökkäystapa ja -reitti riippuu Mäkelän mukaan hyökkääjän tavoitteesta. Isompaan taloushallinnon yritykseen voidaan tehdä esimerkiksi kohdistettu hyökkäys. On myös olemassa tuhansia rikollisia, jotka laittavat miljoonia kalasteluviestejä ympäriinsä ja odottelevat vain, että joku haksahtaa. Jos takana on suurempi toimija kuten esimerkiksi Venäjä, saattaisi se koittaa vaikuttaa jonkin taloushallinnon ohjelman, kuten esimerkiksi Visman kautta suomalaisen yhteiskunnan toimintaan. Se aiheuttaisi monille suomalaisille suuryrityksille ongelmia.

7.4 Varautumisen taso

Tutkimus osoittaa, että tilitoimistojen varautuminen kyberuhkiin on puutteellista etenkin pienillä toimijoilla, mutta myös isommissa tilitoimistoissa on havaittu paljon vaihtelua. Fredman kertoo, että tietoturva asiantuntijat ovat huolissaan tilitoimistojen tietoturvan tasosta. Puutteita on havaittu jäsenyritysten tarkastusten yhteydessä, joita on tehty tilitoimistoille tietoturvan itsearviointilomaketta hyödyntäen. Monilla yrityksillä ei ole käytössä esimerkiksi kaksivaiheista tunnistautumista eikä suojattuja VPN-yhteyksiä. Fredmanin arvio on, että tilitoimistoissa ollaan tietoturvan suhteen kuitenkin valveutuneimpia kuin keskimäärin muilla aloilla.

Tutkimuksessa selvisi, että pienimmillä tilitoimistoilla ei ole useinkaan erillistä IT-henkilöä, ellei henkilökunnassa ole tietoteknistä osaajaa. Kyberturvapalveluita ei myöskään pienissä tilitoimistoissa hyödynnetä. Pienissä yrityksissä on Mäkelän mielestä aivan ymmärrettävää, että keskitytään kiireen vuoksi tieto- ja kyberturvallisuusasioiden sijaan liiketoiminnan pyörittämiseen.

> Mä luulen et tavallaan se keskittyminen, jos puhutaan tämmösestä pienestä yrityksestä tai sit jos on joku start-upp tai joku tämmönen näin, ni sehän on luonnollista, ettei siellä mitään tietoturvapäällikköä oo, kun toimitusjohtajakin on kädet savessa siellä ja tekee hommia. (Mäkelä)

Suuremmissa tilitoimistoissa on tutkimuksen mukaan yleensä tiukemmat ohjeistukset ja paremmat suojautumisjärjestelmät käytössä kuin pienemmissä toimistoissa. Toimistoissa käytetään suojattuja VPN-yhteyksiä, tietokoneelle kirjautuminen on monivaiheinen, julkisissa tiloissa kamerat sekä mikrofonit tulee sulkea ja on käytettävä näytön suojakalvoja sekä muiden, kuin työnantajan tarkastamien USB-tikkujen käyttö on kielletty. Julkisissa tiloissa työskentely on sallittu vain työskentelyyn osoitetuissa tiloissa. Suuremmilla yrityksillä voi olla myös kyberturvapalveluita ja niihin liittyviä koulutuksia käytössä.

Tutkimuksen mukaan etätyöskentely on taloushallinnon alalla viime vuosina lisääntynyt, mutta esimerkiksi suojatut yhteydet eivät monilla yrityksillä ole kuitenkaan käytössä. Mäkelä on sitä mieltä, että yrityksellä tulisi olla käytössä

sellaiset järjestelmät, joissa niiden käyttäminen on turvallista sijainnista huolimatta. Työkoneen pitäisi pystyä toimimaan niin sanotussa epäluotettavassakin verkossa, jolloin siinä on niin vahva suojattu yhteys, ettei koneeseen pääse ulkopuoliset. Työskentely tulisi myös järjestää turvallisessa ympäristössä.

Mäkelän mukaan kyberturvapalvelut on suunnattu pääosin suuremmille asiakkaille ja ne ovat niin kalliita palveluita, että pienyrittäjät eivät ole niille potentiaalisia asiakkaita. Pienyrittäjille on tarjolla samoja tuotteita kuin kuluttaja asiakkaille kuten tietoturva ja mobiiliturva. Tarkoituksena on mahdollisesti kehittää palveluja myös pienyrittäjille. Palveluiden tulisi kuitenkin olla vaivattomasti päälle saatavia ja läpinäkyviä, ettei tarvitse asennella montaa tuntia, että saa palvelun päälle.

7.5 Varmuuskopiot

Tutkimuksen mukaan varmuuskopioita ei enää tehdä tilitoimistoissa itse, vaan ohjelmistojen ja pilvipalveluiden osalta luotetaan siihen, että palveluntarjoajat ovat huolehtineet palveluiden tieto- ja kyberturvallisuudesta sekä hoitavat varmuuskopioinnit. Mäkelä korostaa varmuuskopioiden tärkeyttä ja muistuttaa että jopa koko palvelu voi syystä tai toisesta kadota.

> – – Jos mä annan sille mun elintärkeät asiat, niin onks mulla joku varmuuskopio itellä jos tuo nyt hukkaa ne? Saanko mä ne sitten vielä jostain? Joku kyky palautua, jos kuvitellaan skenaario et pilvipalvelu yhtäkkiä, vaikka katoaa syystä tai toisesta. Voi olla et ne pistää vaikka lapun luukulle tai muuta vastaavaa. Mitä sulle käy sitten kun se lähtee alta, onko sulla kaikki rahan kiinni siinä? (Mäkelä)

Fredman uskoo, että tilitoimistoissa kaikki tieto tallennetaan pilvipalveluihin eikä sitä kahdenneta. Hänen arvionsa mukaan tilitoimistoilla ei olisi kykyä palautua, mikäli tiedot pilvipalveluista katoaisivat. Mäkelä näkee tässä mahdollisen riskin ja suosittelee, että kannattaa ottaa yrityksen ydintoiminnan kannalta kriittisistä tiedoista varmuuskopiot myös itse, toiminnan jatkuvuuden varmistamiseksi.

> Vähintäänkin pitäisi olla ne omat tiedot jossain kopioituna.– – Toimintahan ei jatku, jos ei ole mitään vaihtoehtoista tapaa jatkaa sitä liiketoimintaa ja sulla se palvelu häviää sieltä. Mutta jos kuitenkin olisi ne tiedot

> jossain tallessa. Jos vaikka käy semmoinen, että ne palaa ne tiedot ja seuraavan päivänä ne saa sen järjestelmän takaisin pystyyn, mutta se on tyhjä. Niin että sit sulla on semmoset tiedot, mitkä sä voit viedä takaisin sinne. Otat varmuuskopiot, se on yks juttu. (Mäkelä)

7.6 Tietoturva

Tutkimus osoittaa, että kukaan ei valvo millään tavalla kirjanpitotoimistojen ja tilitoimistojen toimintaa eikä tietoturvan tasoa. Periaatteessa kuka vain voi perustaa tilitoimiston. Fredman kertoo, että alan piirissä toimii tällä hetkellä yli 6000 yritystä, joista valtaosa on pieniä yhden-kahden hengen toimistoja. Hän pahoin pelkää, että kaikki tilitoimistot eivät ilmoita kaikista tietoturvaloukkauksista, vaikka tietosuoja-asetus velvoittaakin alan toimijoita. Syynä voi olla tietämättömyys, välinpitämättömyys tai huonon maineen leviämisen pelko.

Tutkimuksissa selvisi, että Taloushallintoliiton auktorisoimilla tilitoimistoilla on tehtynä itsearviointilomakkeella tietoturvasta selonteko auktorisoinnin yhteydessä. Käytännössä kaikille Taloushallintoliiton 600 jäsenelle, ihan muutamaa toimistoa lukuun ottamatta, on tehty itsearviointilomakkeen avulla tarkastus tietoturvan tasosta. Tarkastuksia voidaan toteuttaa vain jäsenyrityksille ja niitä tehdään viiden vuoden välein. Mikäli huomataan puutteita, niin niiden korjaamiseksi annetaan ohjeistukset ja jos niitä ei noudateta, voi seurauksena olla Taloushallintoliitosta erottaminen.

Tutkimuksen mukaan suuremmilla tilitoimistoilla voi olla asiakkaita, jotka velvoittavat korkeampaan tietoturvan tasoon, jolloin tilitoimistoille on tehty tietoturvaan liittyviä auditointeja eli ulkopuolisen tekemiä tarkastuksia. Satu Ryhänen kertoo, että pienillä ja keskisuurilla asiakasyrityksillä ei ole erityisiä erillisvaatimuksia tietoturvan suhteen, vaan luotetaan tilitoimistoon. Vain erittäin harvat asiakkaat ovat kiinnostuneita tilitoimiston tietoturvajärjestelyistä.

Mäkelä uskoo, että koska tällä hetkellä useimmilla aloilla ei ole tietoturvaan velvoittavaa lainsäädäntöä, ei kaikkia tietoturvapoikkeamia ilmoiteta. Muutos on jo käynnissä ja tietoturvan osalta on tulossa uusi direktiivi EU-tasolla,

tietoturvalainsäädäntö, jota sovelletaan paikalliseksi lainsäädännöksi täällä Suomessa. Tästä aiemmin teleoperaattoreita koskettanut NIS-direktiivistä on nyt tulossa NIS2, jossa laajenee toimialavelvoittavuus ja siinä on mukana uusia toimialoja, jotka eivät aikaisemmin olleet sen piirissä.

> – – Siihen laajenee tää toimialavelvoittavuus eli sinne tulee uusia toimialoja, jotka ei aikaisemmin ollut sen piirissä. – – Kun sä oot havainnut, että sulla on tietoturvapoikkeama, sun täytyy ilmoittaa viranomaiselle siitä, sä et voi enää piilotella sitä asiaa. Tällaisia juttuja, samoin kuin tietosuoja asetuksissa oli, mutta se on vaan henkilötiedoilla, niin tästä tulee ihan kaikelle sitten. Jos ei ole velvoittavaa lainsäädäntöä, niin se on vaan sellainen, että ”Voisitko nyt ilmoittaa”. Jos ei ilmoita ja sitten jos selviää myöhemmin, että sä et ole havainnut sitä, niin silloinhan sulla on ollut riittämätön havainnointikyky havainnoida uhkia. (Mäkelä)

7.7 Riskienhallinta

Tutkimus osoittaa, että pienemmillä tilitoimistoilla ei ole yleensä omaa riskienhallintasuunnitelmaa tai toimintasuunnitelmaa kyberuhkien varalle tehtynä. Pienillä tilitoimistoilla ei ole myöskään kyberturvapalveluita tai -koulutuksia käytössä. Satu Ryhänen epäilee, että pienet yritykset voivat kokea, etteivät kyberuhat kosketa heitä. Esteenä on myös ajan puute sekä resurssien rajallisuus. Tiedon käsittelyyn liittyviä ohjeistuksia on ja niitä kyllä noudatetaan, mutta esimerkiksi mitään käyttöoikeuksien rajoituksia ei ole, koska työntekijöiden täytyy pystyä hoitamaan kaikkia asioita.

Tutkimuksen mukaan suuremmilla tilitoimistoistoilla on useimmiten olemassa riskienhallintasuunnitelmat ja niillä voi mahdollisesti olla riskienhallinnassa huomioituna myös kyberuhat. Suuremmilla yrityksillä on yleensä myös tiukemmat säännöt ja valvonta pienempiin verrattuna, sekä omat IT-osastot, jotka huolehtivat tieto- ja kyberturvallisuusasioista. Mika Ryhäsen kokemuksen mukaan käytössä voi olla esimerkiksi toimiston ovien lukitukset, kulkuluvat sekä käyttöoikeuksien rajoituksia. Työntekijät eivät saa itse ladattua työkoneelle mitään ohjelmia ja kaikkiin järjestelmiin sekä laitteisiin on omat henkilökohtaiset käyttäjätunnukset käytönvalvontaa varten.

Mika Ryhänen kertoo, että suuremmissa tilitoimistoissa voi olla asiakkaana esimerkiksi pörssiyhtiöitä, joilla on tiukat riskienhallintasuunnitelmat, jolloin tilitoimistolta voidaan vaatia tarkempia selosteita tietoturvan varmistamiseksi. Joidenkin pörssiyhtiöiden vaatimuksesta tilitoimistolla tulee olla tietyt sertifikaatit täyttävät tietoturvajärjestelyt. Sertifikaattien toteutumista käy tarkastamassa ulkopuolinen auditoija. Esimerkiksi sitä, että tilitoimiston käyttämien pilvipalvelujen serverit sijaitsevat EU:n ulkopuolella, voidaan pitää tietoturva- ja kyberturvariskinä.

7.8 Toimenpiteet

Pienemmissä tilitoimistoissa ei tutkimuksen mukaan ole tiettävästi kyberturvallisuuteen liittyviä koulutuksia. Mika Ryhänen kertoo, että suuremmissa tilitoimistoissa tieto- ja kyberturvakoulutukset ovat usein omalla koneella töiden lomassa toteutettavia koulutuksia, joissa voi olla esimerkiksi lopuksi jokin pieni tentti ja suorituksista tulee merkintä, kun ne on läpäisty. Myös sähköpostitse saatetaan lähettää koulutusmielessä erilaisia huijausviestejä, joilla tarkistetaan työntekijöiden valppautta ja samalla opetetaan tunnistamaan muun muassa erilaisia kalasteluviestejä. Hänen havaintojensa mukaan työntekijät kyllä noudattavat annettuja ohjeita, mutta koulutuksiin ei hirveästi ole aikaa suuremmissakaan yrityksissä ja niitä tehdään usein omalla ajalla ja töiden lomassa.

Satu ja Mika Ryhänen kertovat, että ajankohtaista tietoturva- ja kyberuhkauutisointia kohdistetaan suoraan tilitoimistoille varoittamaan havaituista uhkista esimerkiksi Kauppakamarin, Taloushallintoliiton sekä Yrittäjät ry:n taholta. Muiden yritysten kanssa keskustellaan yleisessä tiedossa olevista uhkista ja niistä varoitetaan myös omia asiakkaita. He epäilevät, että yritykset eivät mielellään itselle tapahtuneista puhu eteenpäin mainehaitan vuoksi, mutta tiedonjako koetaan tärkeäksi ja muiden varoittaminen kuuluu asiaan.

Taloushallintoliitto on ryhtynyt toimenpiteisiin tilitoimistojen tietoturvan tason parantamiseksi ja on järjestämässä koulutushanketta, jota Huoltovarmuuskeskus on rahoittamassa. Fredmanin mukaan koulutukset olisi tarkoitus toteuttaa siten,

että tilitoimistojen työntekijät voivat suorittaa koulutuksen netin välityksellä omalla koneella ja suorituksesta saa merkinnän, jolla voi todentaa omaa tietoturvaosaamistaan. Ajallisesti koulutukset eivät vaadi työntekijöiltä paljon, mutta näin saadaan tietoturvaan liittyvää tietämystä kasvatettua ja osaamista pidettyä yllä. Koulutusten tarkoitus on myös madaltaa kynnystä tietoturvan auditointeihin ja sertifikaattien suorittamiseen.

Tutkimuksen mukaan kyberturvallisuudesta ollaan yleensä kiinnostuneita, mutta siihen liittyvät toimenpiteet jäävät usein melko vähäisiksi. Mäkelän mukaan isossa skaalassa kyberturvallisuus huolestuttaa ja kiinnostaa kaiken kokoisissa yrityksissä, mutta sitten kun on kyse toimenpiteisiin ryhtymisestä, niin vaihtelu on todella suurta. Toimenpiteitä ei välttämättä tehdä ja tämä koskee myös isoja yrityksiä. Mäkelä arvioi, että kyberturvallisuuspalveluiden puolella todennäköisesti kiinnostuksen tilanne ei tule muuttumaan ennen kuin lainsäädäntöä muutetaan. Yritykset ottavat usein yhteyttä vasta sitten, kun on sattunut jo jotain tai kun se tuodaan pakolliseksi.

Toimenpiteisiin ryhtymisestä Mäkelä nostaa esimerkkinä esiin Vastaamon tietomurto tapauksen, joka toi Suomessa tietoturva asian isommin esille. Valtiotasollakaan ei olla kuitenkaan puheista huolimatta nimetty tahoa, joka kantaisi kyberturvallisuus asioista vastuuta, jos jotain sattuisi. Mäkelän mukaan usein yrityksissä voi olla harhaluulo, että tietoturvajohtajan ja tietoturvapäällikön palkkaaminen pelkästään riittää toimenpiteeksi. Tietoturvajohtajan rooli on toimia yrityksessä neuvonantajana, mutta mikäli yritys ei anna tietoturvajohtajalle henkilökuntaa eikä rahaa suojaaviin toimenpiteisiin, ei pelkkä tietoturvajohtajan olemassaolo riitä. Mäkelä sanookin, että organisaatio ei ole kypsä tietoturvaan, mikäli ei olla valmiita toteuttamaan näitä annettuja ohjeistuksia.

8 Yhteenveto ja pohdinta

8.1 Tavoitteiden saavuttaminen

Kirjallisuuskatsauksen ja haastattelututkimuksen avulla pystyttiin vastaamaan tässä opinnäytetyössä esitettyyn tutkimuskysymykseen: Mitkä ovat tällä hetkellä digitaalista taloushallintoa uhkaavat kyberuhat ja onko niihin osattu alan toimijoiden keskuudessa varautua riittävästi? Varautumisen tasossa oli havaittavissa paljon eroja pienten ja suurten toimijoiden välillä. Tulokset on esitetty tiivistetysti taulukossa 2.

DIGITAALISTA TALOUSHALLINTOA UHKAAVAT KYBERUHAT	TALOUSHALLINNON ALAN TOIMIJOIDEN VARAUTUMISEN TASO
Eniten havaittuja: ▪ Kohdennetut toimitusjohtajahuijaukset ▪ Tietojenkalastelu ▪ Microsoft-tilien kaappaukset Muita mahdollisia uhkia: ▪ Kiristyshaittaohjelmat ▪ Palvelunestohyökkäykset ▪ Sisäinen uhka ▪ Toimitusketjuhyökkäykset ▪ Valtiollinen toimija	**Pienet tilitoimistot** (Valtaosa toimijoista 1-2 henkilöä) • Varautuminen puutteellista • Esteenä osaaminen, ajan puute sekä resurssien rajallisuus ja ei ehkä koeta, että ollaan itse kohteena. • Ei ole erillistä IT-henkilöä. • Tietoturvan tasossa puutteita, ei käytössä VPN-yhteyksiä tai monivaiheista kirjautumista, puutteita palomuurissa. • Luotetaan että palveluntarjoaja hoitaa varmuuskopioinnit. • Ei kyvykkyyttä varmistaa palveluntarjoajan luotettavuutta. • Ei riski- tai toimintasuunnitelmaa kyberuhkien varalle. • Kyberturvakoulutuksia tai -palveluita ei käytössä. **Isommat tilitoimistot** • Varautumisen taso vaihtelee suuresti. • Esteenä usein riittämättömät toimenpiteet sekä ajan puute. • Usein omat IT-osastot. • Tiukemmat ohjeistukset ja paremmat suojautumisjärjestelmät kuin pienillä toimijoilla. • Käytössä VPN-yhteydet, monivaiheinen kirjautuminen, käyttöoikeuksien rajoituksia, kulkuluvat sekä henkilökunnalle koulutuksia ja harjoituksia. • Asiakkaat saattavat vaatia tiukempia tietoturvajärjestelyjä. • Riskienhallinnassa voi olla huomioituna myös kyberuhat. • Kyberturvakoulutuksia tai -palveluita voi olla käytössä.

Taulukko 2. Digitaalista taloushallintoa uhkaavat kyberuhat ja taloushallinnon alan toimijoiden varautumisen taso.

Tutkimuksen avulla haluttiin myös selvittää hyökkääjien mahdollisia motiiveja, mitä hyökkäystapoja on käytössä ja hyökkäysten aiheuttamia haittavaikutuksia

sekä suositeltavia varautumiskeinoja kyberuhkien varalle. Nämä tulokset on esitetty koostetusti taulukossa 3.

HYÖKKÄÄJIEN MOTIIVIT	HYÖKKÄYSTEN HAITTAVAIKUTUKSET
• Raha • Henkilötiedot • Liikesalaisuudet • Suomen yhteiskunnan toimintaan vaikuttaminen lamauttavasti.	• Henkilötietojen, liikesalaisuuksien ja rahan menetykset. • Mainehaitta • Liiketoiminnan jatkuvuuden vaarantuminen. • Yritysten ja yksityishenkilöiden rahaliikenteen pysähtyminen, hyökkäys taloushallinnon ohjelmistoon.
HYÖKKÄYSTAVAT	**KYBERUHKIIN VARAUTUMINEN**
• Hyökkäyksiä eniten sähköpostin välityksellä. • Hyödynnetään usein ihmisen tekemää virhettä. • Muutostilanteiden hyödyntäminen. • Verkkoon jätettyjen laitteiden haavoittuvuuksien hyödyntäminen. • Käytetään pienempää yritystä reittinä varsinaiseen kohteeseen.	• Tietoturvan kolmijalka: tiedon saatavuus, luottamuksellisuus ja eheys. • Laitteiden ja yhteyksien asianmukaiset suojaukset sekä päivitykset, esim. VPN-yhteydet, monivaiheinen tunnistautuminen. • Tunnistaa kriittiset toiminnot, uhkat sekä riskit. • Riskienhallinta • Luotettavien ohjelmistojen ja pilvipalveluiden käyttö. • Muutostilanteissa henkilökunnan riittävä koulutus. • Varmuuskopioiden teko on tärkeää, että yrityksellä on kyky palautua. • Henkilökunnan tieto- ja kyberturvakoulutukset.

Taulukko 3. Hyökkääjien motiivit, hyökkäystavat, haittavaikutukset ja kyberuhkiin varautuminen.

Tämän lisäksi tutkimuksessa selvisi, että taloushallinnon alaa ei velvoita tällä hetkellä tietoturvaa koskeva lainsäädäntö, mikä voi omalta osaltaan aiheuttaa puutteita tietoturvan tasossa sekä tietoturvapoikkeamien ilmoittamisessa. Tietosuoja-asetus velvoittaa tilitoimistoja tietojen turvalliseen käsittelyyn. Tietosuojan toteutumisen edellytyksenä kuitenkin on, että tietoturva on kunnossa. Muutoinkaan tilitoimistojen toimintaa ei valvota millään tavalla eli käytännössä kuka tahansa voisi perustaa tilitoimiston.

8.2 Tulosten tarkastelu

Vertailtaessa tämän tutkimuksen tuloksia Martinmaan (2017) tekemään opinnäytetyön ”Taloushallinnon sähköistymisen ja digitalisoitumisen tuomat riskit ja niiden hallinta taloushallinnon työntekijän näkökulmasta” kyselytutkimuksen tuloksiin, voidaan havaita paljon yhtäläisyyksiä. Suurimpana erona aiempaan tutkimukseen nähden on pilvipalveluiden ja järjestelmien luotettavuuden ja

tietoturvallisuuden arvioimisessa. Martinmaan (2017) tutkimuksen mukaan taloushallinnon alan työntekijät pitivät digitaalista taloushallintoa riskialttiimpana kuin paperista. Palveluntarjoajien luotettavuutta sekä pilvipalveluiden, järjestelmien ja yhteyksien toimivuutta sekä tietoturvallisuutta kyseenalaistettiin. Tietojen varastointia pilvipalveluihin sekä tallennusmuotojen vanhenemista pidettiin riskinä ja tiedostoista tehtiin varmuuskopioita. (Martinmaa 2017, 44–46.)

Pilvipalveluiden luotettavuuden osalta tämän opinnäytetyön tutkimuksen tuloksia voidaan pitää päinvastaisina aiempiin tuloksiin nähden. Tämän tutkimuksen tuloksien mukaan pilvipalveluihin ja järjestelmiin luotetaan, yhteydet ovat toimintavarmoja ja varmuuskopioita ei enää tehdä erikseen palveluiden ulkopuolelle. Tutkimustulosten ero voi selittyä digitaalisen taloushallinnon järjestelmien ja palvelujen kehittymisellä. Aiempi tutkimus on toteutettu vuonna 2017 ja vuosien saatossa ohjelmistot ovat kehittyneet sekä nettiyhteydet parantuneet. Aiemmin on osattu suhtautua uuteen teknologiaan hieman varovaisemmin ja on vielä huomioitu varmuuskopioinnin tärkeys, kun ohjelmistot eivät ole olleet yhtä toimintavarmoja kuin nykypäivänä.

Helsingin seudun kauppakamarin (2022) teettämän selvityksen ”Yrityksiin kohdistuvat kyberuhat” tuloksiin verratessa, voidaan myös havaita hyvin samansuuntaisia tuloksia suurelta osin. Eroavaisuuksista merkittävin tutkimusten välillä oli tiedon saatavuuden sekä työntekijöiden asennoitumisen arvioinnissa. Kauppakamarin teettämässä tutkimuksessa on saatu tulokseksi, että tieto- ja kyberturvallisuuteen liittyvää informaatiota on hankalasti saatavilla ja työntekijät suhtautuvat tietoturvaan välinpitämättömästi (Helsingin seudun kauppakamari 2022, 37–39).

Tämän opinnäytetyön tutkimuksen mukaan taloushallinnon alalla tieto- ja kyberturvallisuuteen liittyvää tietoa on saatavilla ja työntekijät pääsääntöisesti noudattavat annettuja ohjeistuksia. Näin selkeä ero tutkimusten tulosten välillä voi mahdollisesti selittyä toimialakohtaisilla eroilla, sillä Kauppakamarin teettämään tutkimukseen kuului useiden eri alojen yrityksiä. Taloushallinnon alalla on totuttu käsittelemään arkaluontoisia tietoja tietosuoja-asetuksen velvoittamalla tavalla.

Etenkin pienissä yrityksissä tietoturvan toteutumisen esteenä on välinpitämättömyyden sijaan puutteellinen osaaminen sekä aikataululliset ongelmat.

Tutkimuksen tuloksista voidaan päätellä, että taloushallinnon alalle olisi tarpeellinen myös tietoturvaa koskeva lakivelvoite, joka määrittelee noudatettavat vähimmäiskriteerit tietoturvan osalta. Tuloksien perusteella voidaan todeta, että tietoturvan tasoon, laitteiden ja yhteyksien suojaamiseen, kyberturvallisuuden huomioimiseen riskienhallinnassa sekä henkilökunnan tieto- ja kyberturvallisuus koulutuksiin tulisi kiinnittää taloushallinnon alalla enemmän huomiota. Saatavilla olevan tiedon sekä tarjolla olevien suojausmenetelmien tulisi olla niin helposti omaksuttavia ja nopeasti asennettavia, että tiedon käsittelyyn ja suojauksien käyttöönottoon ei kuluisi suuria määriä aikaa.

8.3 Tutkimusmenetelmät ja oma oppiminen

Käytetyt tutkimusmenetelmät sopivat opinnäytetyön tutkimuskysymyksen tutkimiseen mielestäni hyvin. Kirjallisuuskatsauksessa sain kerättyä paljon kyberturvallisuutta koskevaa aineistoa, joissa käsiteltiin aihetta myös taloushallinnon alaa koskien. Opinnäytetyöni aiheeseen sopivia aiempia tutkimuksia on tehty vähän, mutta onnistuin kuitenkin löytämään opinnäytetyön sekä tutkimuksen, joita pystyin hyödyntämään omassa työssäni vertailukohteena.

Asiantuntijahaastattelujen avulla sain täsmällistä ja ajantasaista tietoa tutkimukseeni. Hyödynsin kirjallisuuskatsauksesta saamiani tietoja asiantuntijoiden puolistrukturoitujen teemahaastattelujen kysymysten laatimiseen. Vertailemalla kirjallisuuskatsauksen aineistoa, aiempien tutkimusten tuloksia ja haastatteluista saamiani tietoja, pystyin arvioimaan tutkimukseni tuloksien luotettavuutta ja yleistettävyyttä.

Vaihtoehtoisena tutkimusmenetelmänä mietin taloushallinnon alan yrityksille kohdistettua kyselytutkimusta, mutta ajattelin sen olevan hieman epävarma menetelmä aiheen arkaluonteisuuden vuoksi. Yritykset eivät välttämättä mielellään kerro tietoturvaongelmista tai kohdatuista kyberhyökkäyksistä mahdollisen

mainehaitan vuoksi. Hyvänä esimerkkinä tästä on Barakkaan ja Kärpän vuonna 2022 opinnäytetyössään tekemä kyselytutkimus yritysten kyberturvallisuudesta. Tutkimus oli toteutettu sähköpostitse kyselytutkimuksena ja sen kohteena olivat tilitoimistot, asianajotoimistot sekä mainostoimistot. Kyselyitä oli lähetetty noin 200 yritykselle, joista vastasi 14 eli vastausprosentti oli vain 6%. (Barakas & Kärppä 2022 17.)

Opinnäytetyötä tehdessäni havaitsin, että tutkimuksellisen opinnäytetyön tekeminen vaatii todella paljon erilaisten aineistojen läpikäymistä sekä tietojen vertailua. Aiheena kyberturvallisuus on hyvin laaja ja nopeasti kehittyvä, joten aineiston rajaamista opinnäytetyön aiheeseen sopivaksi sekä aineiston ajantasaisuutta oli huomioitava. Lähteiden luotettavuuden arviointiin kiinnitin myös paljon huomiota ja työssä on käytetty paljon esimerkiksi viranomaislähteitä sekä ajankohtaisia artikkeleita.

Haastattelututkimuksen haastateltavien etsintä ja haastattelut sujuivat suhteellisen helposti muutamia ääniteknisiä ongelmia lukuun ottamatta. Haastattelujen litterointi ja purkaminen kirjoitettuun muotoon puolestaan vei yllättävän paljon aikaa. Kahden ensimmäisen haastattelun jälkeen nousi esiin kysymyksiä, joihin halusin tarkennusta, joten pyysin haastattelua vielä Taloushallintoliiton taloushallinnon johtavalta neuvonantajalta. Jälkeenpäin ajateltuna Taloushallintoliiton edustajan haastattelu olisi ehkä ollut järkevää tehdä jo aivan heti tutkimuksen alussa. Toisaalta tarkennusta vaativat asiat tulivat esiin vasta tutkimuksen loppupuolella.

8.4 Luotettavuus ja eettisyys

Hyvän tieteellisen käytännön perusperiaatteisiin sekä tutkimuseettisiin ohjeistuksiin kuuluvat arvostus, vastuunkanto, luotettavuus sekä rehellisyys. Tieteellisessä toiminnassa hyvän käytännön vastaista toimintaa ovat vilppi tieteellisessä toiminnassa sekä piittaamattomuus hyvästä tieteellisestä käytännöstä. Vilpiksi luokiteltavia toimintoja ovat sepittäminen, vääristely ja plagiointi.

Piittaamattomuudella viitataan muuhun kuin vilpiksi luokiteltavaan hyvän tieteellisen käytännön vastaiseen toimintaan. (Tutkimuseettinen neuvottelukunta 2023, 11,16–17.)

Tämä opinnäytetyö on tehty hyvän tieteellisen käytännön perusperiaatteita sekä tutkimuseettistä ohjeistusta noudattaen. Opinnäytetyössä on käytetty aiheittain useita eri lähteitä, joiden luotettavuutta on arvioitu toisiinsa vertailemalla sekä käytetyn aineiston kirjoittajien ja julkaisevien tahojen taustoja tutkimalla. Opinnäytetyössä tehdyn tutkimuksen tulosten arvioinnissa ja vertailussa on hyödynnetty aiempien tutkimusten tuloksia.

Asiantuntijahaastattelujen kysymykset oli laadittu siten, että sain tutkimukseeni tarkentavaa digitaalista taloushallintoa sekä kyberturvallisuutta koskevaa ajantasaista tietoa. Haastateltavat saivat vastata kysymyksiin avoimin vastauksin, oman kokemuksensa sekä tietämyksensä mukaisesti. Haastattelun riskinä voi olla kysymysten liika johdattelevuus, mutta ottaen huomioon kaikkien haastateltavien useiden vuosien kokemuksen omilla aloillaan, uskoisin että heidän kertomansa perustuu omaan kokemukseen ja tietämykseen kysymyksen asettelusta riippumatta. Haastateltavien vastauksia ei ole muunneltu eikä mitään tutkimuksen kannalta olennaista tietoa ole jätetty pois.

8.5 Tulevaisuuden näkymät ja jatkotutkimusaiheet

Taloushallintoliitto on ollut huolestunut tilitoimistojen tietoturvan tasosta ja haluaa nostaa taloushallinnon alan toimijoiden tietoturva- ja tietosuojaosaamista sekä varautumista tietoturva- ja kyberuhkien aiheuttamiin kriisitilanteisiin toteuttamalla koulutuskokonaisuuden vuosien 2023–2025 aikana. Suomen Huoltovarmuuskeskus on lähtenyt rahoittamaan Taloushallintoliiton järjestämää koulutushanketta, jolla pyritään saamaan myös pienemmät toimijat mukaan nostamaan tietoturvan tasoa. (Suomen Taloushallintoliitto ry 2023c.)

Digitaalinen turvallisuus 2030-ohjelman puitteissa toteutuva maksuton koulutus on suunnattu kaikille taloushallinnon alalla työskenteleville työntekijöille sekä

yrityksen johdolle. Uuden tietoturvaan ja tietosuojaan keskittyvän koulutuskokonaisuuden lisäksi on myös kehitteillä tilitoimistoille ja muille taloushallintopalvelualan yrityksille kohdistettu tietoturva-auditointimalli. (Suomen Taloushallintoliitto ry 2023c.) Koulutushankkeen päätyttyä, hyvä jatkotutkimuksen aihe olisi tutkia hankkeen vaikutuksia tietoturva ja kyberturva osaamiseen sekä varautumisen tasoon taloushallinnon alalla.

Valtaosa taloushallinnon yrityksistä on pieniä yhden-kahden hengen yrityksiä, joiden suurimpana ongelmana tietoturva- ja kyberturvallisuusuhkiin varautumisessa on tietoturvaosaamisen sekä ajan ja resurssien puute. Tämän vuoksi olisi mielestäni hyvä, jos taloushallinnon alan koulutuksissa voitaisiin jakaa tietoutta taloushallintoon kohdistuvista tietoturva- ja kyberuhista sekä niihin varautumisesta. Näin valmistuvilla opiskelijoilla olisi jo valmius turvalliseen työntekoon digitaalisessa ympäristössä.

Digitaalisen taloushallinnon jälkeen seuraava askel kehityksessä on ohjelmistorobotiikkaa sekä tekoälyä hyödyntävä älykäs taloushallinto. Automaatioaste nousee koko ajan, jonka ansiosta taloushallinnossa saadaan tuotettua liiketoiminnalle sekä viranomaisille tarpeellista dataa laadukkaammin ja nopeammin kuin ennen. (Kaarlejärvi & Salminen 2018, 12–13.) Digitaalisen kehityksen ja tekoälyn myötä muuttavat varmasti muotoaan myös taloushallinnon alaan kohdistuvat kyberuhat, joten epäilemättä tulevaisuudessa saadaan sitä kautta uusia mielenkiintoisia jatkotutkimusaiheita myös tältä saralta.

Lähteet

Barakas, S. & Kärppä, A. 2022. Kyberturvallisuus yrityksissä. Liiketalouden koulutusohjelma. Opinnäytetyö. Centria-ammattikorkeakoulu. https://www.theseus.fi/bitstream/handle/10024/788390/Barakas_K%c3%a4rpp%c3%a4.pdf?sequence=2&isAllowed=y. 19.8.2023.

Bogdanov, J. 2023. Venäläinen hakkeriryhmä voi olla eduskuntaan kohdistuneen palvelunestohyökkäyksen takana. Yle Uutiset 4.4.2023. https://yle.fi/a/74-20025816. 24.5.2023.

Business Insight Group. 2023. Positiivinen kyberturvallisuuskulttuuri. https://www.bignordic.com/positiivinen-kyberturvallisuuskulttuuri. 11.8.2023.

CGI Inc. 2018. Bitit, bisnes ja kyberturva. Kyberturvallisuudesta vastaavan opas puolustuksen rakentamiseen. bitit-bisnes-ja-kyberturva-opas.pdf. 5.6.2023.

Euroopan parlamentti. 2023. Kyberturvallisuus: nykyiset ja tulevat uhat. https://www.europarl.europa.eu/news/fi/headlines/society/20220120STO21428/kyberturvallisuus-nykyiset-ja-tulevat-uhat. 24.5.2023.

Euroopan tilintarkastustuomioistuin. 2022. EU:n toimielinten, elinten ja virastojen kyberturvallisuus: valmiustaso ei kokonaisuutena ole oikeassa suhteessa uhkiin. Erityiskertomus. Erityiskertomus: EU:n toimielinten, elinten ja virastojen kyberturvallisuus (europa.eu). 12.11.2023.

Fredman, J. 2022. Venäjän kyberuhka ja tilitoimistot. Tilisanomat 19.5.2022. Venäjän kyberuhka ja tilitoimistot | Suomen Taloushallintoliitto ry. 5.6.2023.

Fredman, J. 2023. Tietoturva kuntoon tilitoimistoissa. Tilisanomat 11.5.2023. https://tilisanomat.fi/kolumnit/paakirjoitus/tietoturva-kuntoon-tilitoimistoissa. 6.6.2023.

Finanssiala ry. 2023. Varo, varmista, varoita -kampanja: Digihuijausten määrä kasvoi selvästi vuoden 2022 jälkipuoliskolla. Varo, varmista, varoita -kampanja: Digihuijausten määrä kasvoi selvästi vuoden 2022 jälkipuoliskolla - Finanssiala. 18.9.2023.

Helsingin seudun kauppakamari. 2022. Yrityksiin kohdistuvat kyberuhat. https://view.24mags.com/helsinki.chamber/yrityksiin-kohdistuvat-kyberuhat--selvitys-2022#/page=6. 24.5.2023.

Huoltovarmuuskeskus. 2023. Vuosikatsaus 2022. https://www.huoltovarmuuskeskus.fi/files/edbeeb7ceb93f4ca6eddfccad2003615d72fe673/hvk-vuosikatsaus-2022.pdf. 24.5.2023.

Hyvärinen, M., Suoninen, E. & Vuori, J. 2023. Haastattelut. Teoksessa Jaana Vuori (toim.) Laadullisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/. 11.8.2023.

Juhila, K. 2023. Teemoittelu. Teoksessa Jaana Vuori (toim.) Laadullisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/. 10.9.2023.

Jämsen, E. 2019. Kannattaako digitaalinen taloushallinto?. Priima Yrityslaskennan blogi. 28.1.2019. Blogi. https://www.priimalaskenta.fi/laskenta-blog/kannattaako-digitaalinen-taloushallinto. 14.10.2023.

Järvinen, P. 2018. Kyberuhkia ja somesotaa. Digiaikana sinäkin olet etulinjassa. Jyväskylä: Docendo Oy.

Järvinen, P. 2022. Yrityksen tietoturvaopas. Helsinki: Helsingin seudun kauppakamari.

Kaarlejärvi, S. & Salminen, T. 2018. Älykäs taloushallinto. Automaation aika. Helsinki: Alma Talent Oy.

Kallio, A. 2023. Litterointi. Laadullisen tutkimuksen verkkokäsikirja. Tietoarkisto. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/laadullisen-tutkimuksen-prosessi/litterointi/. 10.9.2023.

Kangasniemi, H. 2023. Taloushallinnon on kestettävä tietoturvahyökkäykset, jotta yhteiskunnan toiminnot eivät vaarannu. Varmuuden vuoksi 20.6.2023. https://www.varmuudenvuoksi.fi/artikkeli/taloushallinnon-on-kestettava-tietoturvahyokkaykset-jotta-yhteiskunnan-toiminnot-eivat-vaarannu. 16.8.2023.

Karinen, I. 2020. Kyberriskit haltuun yhteistyöllä. 27.10.2020. Blogi. Elisa Oyj verkkosivut. https://yrityksille.elisa.fi/ideat/kyberriskit-haltuun-yhteistyolla/. 6.9.2023.

Karppi, T & Kulmanen, K. 2023. Puutteellinen johtaminen aiheutti kaaoksen Helsingin palkanmaksussa. Yle 12.4.2023. Puutteellinen johtaminen aiheutti kaaoksen Helsingin palkanmaksussa | Yle Uutiset. 16.8.2023.

Liikenne- ja viestintävirasto Traficom. 2020. Pienyritysten kyberturvallisuusopas. Traficomin julkaisuja 228/2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf. 24.5.2023.

Liikenne- ja viestintävirasto Traficom. 2022a. Toimintaohje - Palvelunestohyökkäys. Traficom julkaisuja 25/2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Palvelunestohy%C3%B6kk%C3%A4ysToimintaohje.pdf. 1.10.2023.

Liikenne- ja viestintävirasto Traficom. 2022b. Toimintaohje - Toimitusketjuhyökkäys. Traficomin julkaisuja 21/2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Toimitusketjuhy%C3%B6kk%C3%A4ysToimintaohje.pdf. 1.10.2023.

Liikenne- ja viestintävirasto Traficom. 2023a. Kybersää syyskuu 2023. Liikenne- ja viestintävirasto Traficom. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%20syyskuu%202023.pdf. 9.11.2023.

Liikenne- ja viestintävirasto Traficom. 2023b. NIS-koordinointi ja viranomaisyhteistyö. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/nis-koordinointi-ja-viranomaisyhteistyo. 8.9.2023.

Liikenne- ja viestintävirasto Traficom. 2023c. Kyberturvallisuuden uhkataso pysynyt kohonneena – kohdistettujen hyökkäysten määrä noussut. Liikenne- ja viestintävirasto Traficom. Kyberturvallisuuden uhkataso pysynyt kohonneena - kohdistettujen hyökkäysten määrä noussut | Traficom (kyberturvallisuuskeskus.fi). 24.5.2023.

Lehtonen, S. 2021. Tunnistatko tietomurron ja tietovuodon, entä muut verkkorikokset?. Rikosuhripäivystys.

https://www.riku.fi/rikosuhripaivystys/rikuteema/rikuteema-2-2021/tunnistatko-tietomurron-ja-tietovuodon-enta-muut-verkkorikokset-2/. 15.10.2023.
Limnéll, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Jyväskylä: Docendo Oy.
Manninen, O. 2019. Tietoturvan sertifiointi lisää luottamusta tilitoimistoalaan. Tilitoimistossa 2.4.2019. Tilitoimistossa (taloushallintoliitto.fi). 9.9.2023.
Mannila, M. 2021. Kirjallisuuskatsaus opinnäytetyön muotona. 11.2.2021. Blogi. Energiaa-verkkolehti. https://energiaa.vamk.fi/osaaminen/kirjallisuuskatsaus-opinnaytetyon-muotona/. 11.8.2023.
Martinmaa, P. 2017. Taloushallinnon sähköistymisen ja digitalisoitumisen tuomat riskit ja niiden hallinta taloushallinnon työntekijän näkökulmasta. Haaga-Helia ammattikorkeakoulu. Liiketalouden koulutusohjelma. Opinnäytetyö. https://www.theseus.fi/bitstream/handle/10024/131067/Martinmaa_Pauli.pdf?sequence=1&isAllowed=y. 19.8.2023.
Mulari, H. 2023. Kosto Suomen rajapäätöksestä – Venäläinen hakkeriryhmä pimensi verkkosivuja ja vinkkaa silmää. Iltalehti 19.9.2023. https://www.iltalehti.fi/digiuutiset/a/b1a6d06a-402d-4849-a184-52c4a7de7768. 14.10.2023.
MTV Uutiset. 2022. Wärtsilään kohdistunut hakkeri-isku – jäljet viittaavat Venäjälle. https://www.mtvuutiset.fi/artikkeli/wartsilaan-kohdistunut-hakkeri-isku-jaljet-viittaavat-venajalle/8476686#gs.w63acs. 24.5.2023.
Mäkelä, T. 2020. Henkilöstön kouluttaminen on yksi tehokkaimmista keinoista taistella kyberuhkia vastaan. 21.10.2020. Blogi. Elisa Oyj verkkosivut. Henkilöstön kouluttaminen on yksi tehokkaimmista keinoista taistella kyberuhkia vastaan | Elisa Ideat Yrityksille. 5.9.2023.
Mäkelä, T. 2022. Varaudu kyberhyökkäykseen – kyse ei ole jos, vaan milloin. Elisa Oyj Blogit. 30.3.2022. Blogi. Varaudu kyberhyökkäykseen | Elisa Ideat Yrityksille. 5.9.2023.
Nuopponen, A. 2018. Huijarit horjuttavat taloushallinnon kyberturvaa. Tilisanomat 22.3.2018. https://tilisanomat.fi/kolumnit/vieraskyna/huijarit-horjuttavat-taloushallinnon-kyberturvaa. 24.4.2023
Palkkaus.fi. 2023. Tilitoimisto: onko tietosuoja varmasti kunnossa?. Tilitoimisto: onko tietosuoja varmasti kunnossa? – Palkkaus.fi. 13.11.2023.
Peltomäki, J. & Norppa, K. 2015. Rikos meni verkkoon. Näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen. Helsinki: Talentum Media Oy.
Rousku, K. 2014. Kyberturvaopas. Tietoturvaa kotona ja työpaikalla. Helsinki: Talentum Media Oy.
Saaranen-Kauppinen, A. & Puusniekka, A. 2006. 1.2.Mitä laadullinen tutkimus on : lyhyt oppimäärä. KvaliMOTV – Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. KvaliMOTV - 1.2 Mitä laadullinen tutkimus on: lyhyt oppimäärä (tuni.fi). 1.10.2023.
Sisäministeriö. 2023. Kyberturvallisuus osana kansallista turvallisuutta. https://intermin.fi/kansallinen-turvallisuus/kyberturvallisuus. 24.5.2023
Suomen Taloushallintoliitto ry. 2023a. Taloushallintoliitto ja Huoltovarmuuskeskus kehittämään taloushallintoalan tietoturvaa, tietosuojaa ja kriisivalmiuksia. https://taloushallintoliitto.fi/taloushallintoliitto-ja-huoltovarmuuskeskus-kehittamaan-taloushallintoalan-tietoturvaa-tietosuojaa-ja-kriisivalmiuksia/. 8.9.2021.

Suomen Taloushallintoliitto ry. 2023b. Tilitoimistotarkastus. https://taloushallintoliitto.fi/palvelut/tilitoimistotarkastus/. 9.9.2023.
Suomen Taloushallintoliitto ry. 2023c. Taloushallintoala Suomessa. https://taloushallintoliitto.fi/tietopankki/taloushallintoala-suomessa/. 9.9.2023.
Suupohjan tietosuojatyöryhmä. 2021. Tietoturva- ja tietosuojaopas henkilöstölle. Karvian kunta. Henkiloston-tietoturvaopas-2021.pdf (karvia.fi). 12.11.2023.
Tietosuojavaltuutetun toimisto. 2023a. Tietoturvaloukkaukset. Tietoturvaloukkaukset | Tietosuojavaltuutetun toimisto. 8.9.2023.
Tietosuojavaltuutetun toimisto. 2023b. Usein kysyttyä EU:n tietosuoja-asetuksesta. https://tietosuoja.fi/gdpr. 8.9.2023.
Tietosuojavaltuutetun toimisto. 2023c. Tietosuoja. https://tietosuoja.fi/tietosuoja. 8.9.2023.
Turvallisuuskomitea. 2023. Ennakointi ja varautuminen. Ennakointi ja varautuminen – Turvallisuuskomitea. 12.11.2023.
Turvallisuuskomitean sihteeristö. 2013. Suomen kyberturvallisuusstrategia. https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf. 9.11.2023.
Tutkimuseettinen neuvottelukunta. 2023. Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa. https://tenk.fi/sites/default/files/2023-03/HTK-ohje_2023.pdf. 30.9.2023.
Työ- ja elinkeinoministeriö. 2021. Uusi hanke edistää yritysten taloushallinnon digitalisoitumista. Uusi hanke edistää yritysten taloushallinnon digitalisoitumista - Työ- ja elinkeinoministeriön verkkopalvelu (tem.fi). 2.6.2023.
Ulkoministeriö. 2023. Kyberturvallisuus ja kybertoimintaympäristö. https://um.fi/kyberturvallisuus-ja-kybertoimintaymparisto. 24.5.2023.
Valtiovarainministeriö. 2016. EU-tietosuojan kokonaisuudistus. VAHTI-raportti-1/2016. Raportti-luonnos (suomidigi.fi). 12.11.2023.
Valtiovarainministeriö. 2023. Kyberturvallisuusstrategia. https://vm.fi/kyberturvallisuusstrategia. 24.5.2023.
Visma. 2023a. Yrityksen taloushallinto ja sen tehtävät - opas taloushallinnon tehokkaaseen järjestämiseen. https://www.visma.fi/visma-fivaldi/yrityksen-taloushallinto/. 15.4.2023.
Visma. 2023b. Sähköinen taloushallinto 2023 – ohjelmistojen tuomat mahdollisuudet, riskit, hyödyt ja hinnat. https://www.visma.fi/visma-fivaldi/sahkoinen-taloushallinto/#mahdollisuudet. 4.6.2023.
Väestörekisterikeskus. 2019. Digiturvaopas – Judo-hanke sekä digitaalinen turvallisuus toiminnan mahdollistajana. digiturvaopas – JUDO-hanke sekä digitaalinen turvallisuus toiminnan mahdollistajana (dvv.fi). 12.11.2023.

Ryhmähaastattelu 9.6.2023
Haastateltavat:
Satu Ryhänen, Tilitoimisto Tili-satu Oy, yrittäjä
Mika Ryhänen, Tilitoimisto Tili-satu Oy, taloushallinnon asiantuntija KLT, neuvonantaja

1. Mitä vaikutuksia taloushallinnon sähköistymisellä ja digitalisoitumisella on ollut taloushallinnon alaan? Mitä hyötyjä ja riskejä on havaittu?

2. Kuinka laajalti on uutta teknologiaa otettu hyötykäyttöön? Kuinka digitalisoituminen ja tekoäly on otettu vastaan?

3. Mitkä ovat suosituimmat ohjelmistot ja sovellukset? Onko ohjelmistoissa toimivuusongelmia ja ovatko ne luotettavia? Mitä laitteitta pystytään hyödyntämään työnteossa?

4. Kiinnitetäänkö tietoturva ja kyberturvallisuus asioihin huomiota mielestänne tilitoimistoissa tarpeeksi uusien ohjelmistojen ja laitteiden käyttöönoton yhteydessä?

5. Kiinnostaako asiakkaita, että kuinka esimerkiksi tilitoimiston tietoturva ja kyberturvallisuus on hoidettu?

6. Onko alan yrityksillä kyberturvallisuudesta tietoa ja jos on niin mitä kautta sitä on tullut vai pitääkö ottaa itse selvää?

7. Mikä on haastavinta yrityksen kyberturvallisuuden kehittämisessä?

8. Mitä riskejä liittyy mielestänne pilvipalveluihin? Tehdäänkö varmuuskopioita muualle?

9. Työskennelläänkö alalla etänä paljon? Mitä riskejä liittyy mielestänne etätyöskentelyyn?

10. Mitkä ovat mielestänne taloushallinnon alalla suurimpia kyberuhkia?

11. Mitä hyökkääjät voisivat mahdollisesti haluta taloushallinnon yrityksestä?

12. Keskustellaanko kyberhyökkäyksistä ja jaetaanko tietoa yrittäjien kesken?

13. Onko koronapandemian tai Ukrainan sodan vaikutuksia ollut havaittavissa kyberhyökkäysten lisääntymisenä tai muutoin?

14. Onko yrityksillä yleensä ohjeistusta ja suunnitelmat kyberuhkien varalle? Noudatetaanko turvaohjeistuksia?

15. Ostetaanko kyberturvapalveluita palveluntarjoajilta vai huolehditaanko suojauksista ja suunnitelmien teosta itse? Mitä suojautumiskeinoja käytössä?

16. Järjestetäänkö työntekijöille kyberturvallisuuteen liittyviä koulutuksia?

Teams-haastattelu 4.8.2023
Haastateltava:
Teemu Mäkelä, Elisa Oyj, tietoturvajohtaja

1. Mitä tietoturvajohtajan työhön kuuluu?

2. Kuinka kyberturvallisuuteen suhtaudutaan tällä hetkellä yrityksissä?

3. Taloushallinnon alalla on paljon pieniä yrityksiä, minkälaisena näet pienten toimijoiden suhtautumisen kyberturvallisuuteen?

4. Voidaanko taloushallinnon alan toimintoja pitää mielestäsi kriittisinä yhteiskunnan toiminnan kannalta?

5. Tilitoimistojen asiakkaat harvoin tarkistavat kuinka tilitoimistojen tietoturva asiat on hoidettu. Tilitoimistot puolestaan luottavat ohjelmistojen palveluntarjoajiin, että ohjelmistot ovat kyberturvallisia käyttää. Voiko vaarana olla tällainen ”tietoturvailluusio”, jossa kaikki osapuolet luulevat, että tietoturva on kunnossa, mutta sitä ei olekaan huomioitu tarpeeksi tai laisinkaan?

6. Voiko mielestäsi luottaa vain siihen, että ohjelmiston valmistaja huolehtii käytön turvallisuudesta vai tulisiko lisäksi ottaa varmuuskopioita vielä muuallekin?

7. Mihin seikkoihin tulisi kiinnittää huomiota uusien ohjelmistojen ja laitteiden käyttöönoton yhteydessä ja siirtymävaiheessa? Mitä riskejä?

8. Mitä riskejä liittyy pilvipalveluihin? Miten erottaa luotettava pilvipalvelu?

9. Mitä ovat suurimmat riskit liittyen etätyöskentelyyn?

10. Mitä riskejä voi liittyä IoT-laitteisiin?

11. Mitkä ovat taloushallinnon alalla yleisimpiä kyberuhkia?

12. Mikä voisi olla todennäköisin reitti kyberhyökkäykselle taloushallinnon alan yrityksessä? Vai onko ihminen se heikoin lenkki?

13. Onko hyökkäysten määrässä eroa pienten ja suurten toimijoiden välillä?

14. Ovatko taloushallinnon alan yritykset kiinnostuneita kyberturvapalveluista? Ottaako asiakkaat itse yhteyttä vai tavoitellaanko asiakkaita?

15. Onko kyberturvallisuuspalveluissa kaiken kokoisille yrityksille soveltuvia kyberturvaratkaisuja?

16. Tulevaisuuden näkymät?

Puhelinhaastattelu 22.9.2023
Haastateltava:
Janne Fredman, Suomen Taloushallintoliitto ry, taloushallinnon johtava asiantuntija

1. Onko Taloushallintoliitto tehnyt jäsenilleen tietoturvan tasoon liittyvää tutkimusta vai perustuuko havainto tilitoimistojen puutteellisesta tietoturvan tasosta tilitoimistoille tehtyihin tarkistuksiin ja jäsenneuvontaan?

2. Minkälaisia tietoturva puutteita alan toimijoilla on havaittu?

3. Kuuluuko taloushallinnonala tietoturvaa koskevan uudistetun NIS-direktiivin velvoitteiden ja valvonnan piiriin? Ja jos ei kuulu niin onko tietoa siitä, että nouseeko taloushallinnon ala NIS-direktiivin alaisuuteen eli huoltovarmuuskriittisiin toimijoihin?

4. Valvotaanko tilitoimistojen tietoturvan tasoa millään tavalla?

5. Tapahtuuko Taloushallintoliiton toteuttama tietoturvan tason valvonta vain jäsenyritysten tarkastusten sekä neuvonnan yhteydessä?

6. Kuuluuko tietoturvan itsearviointilomakkeen täyttö kaikille jäsenyrityksille vai pelkästään niille, jotka hakevat auktorisointia?

7. Tarkistetaanko itsearviointilomakkeen tietojen ajantasaisuutta minkälaisilla aikaväleillä?

8. Tilitoimistojen tietoturvatason nostamiseksi on toimialalle kehitetty vuonna 2019 myös omaa kolmetasoista tietoturvallisuuden sertifiointiohjelmaa, onko tällainen sertifiointiohjelma käytössä?

9. Toimenpiteenä on Taloushallintoliitto nyt järjestämässä Huoltovarmuuskeskuksen rahoittamana koulutushanketta edistämään alan tietoturvaa ja kyberuhkiin varautumista. Kuinka koulutushanke etenee?

10. Mitkä ovat mielestäsi suurimmat kyberuhat mitä kohdistuu tilitoimistoihin?

11. Ilmoittavatko tilitoimistot tietoturvapoikkeamista?

12. Huomioidaanko kyberuhat tilitoimistojen riskienhallinnassa?

13. Käyttävätkö tilitoimistot kyberturvapalveluita tai kouluttavatko henkilökuntaa?

14. Otetaanko tilitoimistoissa edelleen varmuuskopioita?

Haastatteluista nousseet teemat

Teemat	Tilitoimiston haastattelu	Taloushallinnon neuvonantajan haastattelu	Tietoturvajohtajan haastattelu
Muutos digitaaliseen taloushallintoon	Työntekijöissä ja asiakkaissa havaittavissa muutosvastarintaa. Jos järjestelmiä ei osata käyttää, saattaa tulla virheitä → Virheiden havaitsemiseen voi mennä pitkään.	Paperisessa muodossa tehdään vielä paljon töitä → Muutos vasta tulossa.	Muutostilanteissa riskit kasvavat. Tietoturvan kolmijalka: tiedon saatavuus, luottamuksellisuus ja eheys. → Ennen käyttöönottoa tulisi varmistaa, että järjestelmiä osataan käyttää. Rikolliset etsivät ja hyödyntävät heikkouksia.
Palveluntarjoajat	Luotetaan, että palveluntarjoaja on huolehtinut tieto- ja kyberturvallisuudesta. Toimintavarmuus nykyisin hyvä ja parantuneet internetyhteydet vaikuttaneet toimivuuteen positiivisesti.	Tilitoimistoissa luotetaan tieto- ja kyberturvallisuudessa ohjelmistojen sekä pilvipalveluiden palveluntarjoajiin.	Etenkin pienillä toimijoilla ei ole kykyä vaatia toimittajalta mitään, on vain luotettava toimittajan kertomaan. Olisi hyvä olla jokin leima tai sertifiointi mihin voi luottaa → Toimijoilla ei kyvykkyyttä auditointiin ja tietoturvatietojen tarkistukseen.
Ohjelmistot	Ohjelmistoja pidetään luotettavina ja turvallisina käyttää. → Kirjautumismenetelmiä on kehitetty, käytössä varmenteet ja kirjautumissovellukset.	Tilitoimistoissa luotetaan ohjelmistojen turvallisuuteen.	Vahvoilla kirjautumismenetelmillä käyttö on turvallista, mutta se ei vielä takaa tietojen säilymistä.
Pilvipalvelut	Pilvipalveluissa turvallisina pidetään kotimaisia palveluntarjoajia. Luotettavana voidaan pitää, jos serverit ovat EU-alueella.	Pilvipalvelujen käyttö on lisännyt tietoturvan tasoa. → Tiedot omien koneiden ja arkistojen sijaan paremmin suojatuilla palvelimilla.	Pelkkä serverin sijainti EU-alueella ei kerro kaikkea → Tarkistettava minkä maan lainsäädäntöä toimija noudattaa. Palvelu voi hävitä tai sen käyttö voi estyä, tiedot voivat kadota.
Kyberuhat	**Havaittuja uhkia** → Sähköpostitse roskapostit, tietojenkalasteluviestit sekä kohdennettu toimitusjohtajahuijaus.	**Havaittuja uhkia** → Microsoft sähköpostitilien kaappauksia, pilvipalveluihin kohdistuneet palvelunestohyökkäykset	**Havaittuja uhkia** →Sähköpostitse yleisenä ilmiönä kohdennetut toimitusjohtajahuijaukset sekä tietojenkalastelut ja muut huijaukset.

	Mahdollisia uhkia → Palveluntarjoajaan kohdistuvat palvelunestohyökkäykset, sisäinen uhka, pienen yrityksen käyttö reittinä toiseen yritykseen. Rikollisten motiivina voi olla raha ja liikesalaisuudet.	**Mahdollisia uhkia** → Mikäli pilvipalvelun palveluntarjoaja menettää tiedot, tilitoimistot eivät saa niitä palautettua. Suurimpana uhkana on, että henkilötiedot ja yrityssalaisuudet joutuvat vääriin käsiin.	**Mahdollisia uhkia** → Verkkoon jätettyjen laitteiden haavoittuvuudet, toimitusketjuhyökkäykset, joissa käytetään pienempää yritystä reittinä varsinaiseen kohteeseen, yritysten sisäiset uhat. → Suomen yhteiskunnan toimintaan voisi joku suuri valtiollinen toimija vaikuttaa lamauttavasti esimerkiksi taloushallinnon ohjelmiston kautta. Motiivina rikollisilla yleensä raha.
Varautuminen	**Pienimmillä toimistoilla** ei ole useinkaan erillistä IT-henkilöä. Etänä työskennellessä käytetään työnantajan laitteita, joissa suojaukset. Pienillä toimistoilla ei välttämättä muita erityistoimia. → Kyberturvapalveluita ei käytössä. **Isommilla tilitoimistoilla** usein omat IT-osastot, jotka huolehtivat tieto- ja kyberturva asioista. → Tiukemmat ohjeistukset ja paremmat suojautumisjärjestelmät. Käytössä VPN-yhteydet, monivaiheinen kirjautuminen, näytönsuojakalvot, vain työnantajan USB-tikut sallittuja, kamerat ja mikrofonit kiinni → Suuremmilla tilitoimistoilla mahdollisesti kyberturvapalvelutkin ostettuna.	Tietoturvan tasossa on havaittu puutteita etenkin **pienemmillä toimistoilla** jäsenyritysten tarkastusten yhteydessä. →Tilitoimistoilla ei ole useinkaan omaa IT-osaamista laisinkaan, puutteita palomuureissa, suurella osalla ei ole käytössä kaksivaiheista tunnistautumista eikä VPN-yhteyksiä. → Pienillä tilitoimistoilla ei ole kyberturvapalveluita käytössä. **Suuremmilla tilitoimistoilla**, joilla asiakkaat velvoittavat korkeampaan tietoturvan tasoon, voi olla myös kyberturvapalveluita ja niihin liittyviä koulutuksia käytössä.	**Pienten yritysten** osalta on aivan ymmärrettävää, ettei siellä ole omaa tietoturva- ja kyberturvallisuusosaamista, kun kaikki keskittyminen menee liiketoiminnan pyörittämiseen → Pienille yhdenkahden hengen yrityksille ei ole tarjota muuta kuin samoja tietoturvapalveluita mitä kuluttajillekin. **Suurempienkin yritysten** varautumisen tasossa voi olla suurta vaihtelua → Kyberturvapalvelut ovat suunnattu suuremmille yrityksille. Yrityksellä tulisi olla käytössä sellaiset järjestelmät, joissa niiden käyttäminen on turvallista sijainnista tai verkon epäluotettavuudesta huolimatta.
Varmuuskopiointi	Luotetaan, että palveluntarjoaja hoitaa varmuuskopioinnit.	Kaikki tallennetaan pilvipalveluihin ja tietoa ei kahdenneta.	Varmuuskopioiden teko on tärkeää, että yrityksellä on kyky palautua. → Liiketoiminta ei jatku, jos tietoja ei pystytä palauttamaan.

Riskienhallinta	**Pienemmillä yrityksillä** ei ole oletettavasti omaa riski- tai toimintasuunnitelmaa kyberuhkien varalle. Voidaan kokea, että kyberuhat ei koske heitä. Esteenä on myös ajan puute sekä resurssien rajallisuus. → Tiedon käsittelyyn liittyviä ohjeistuksia noudatetaan, käyttöoikeuksien rajoituksia ei ole käytännön syistä. **Isommilla yrityksillä** olemassa riskisuunnitelmat, osalla huomioituna myös kyberuhat. Asiakas voi vaatia tiukempia tietoturvajärjestelyjä. → Yleensä tiukempi valvonta, ovien lukitukset, kulkuluvat sekä käyttöoikeuksien rajoituksia.	**Pienemmillä toimistoilla** ei välttämättä ole riskienhallintasuunnitelmia laisinkaan. **Suuremmilla toimistoilla** voi mahdollisesti olla huomioituna riskienhallinnassa myös kyberuhat.	**Pienemmillä yrityksillä** ei ole oletettavasti tarvittavaa kiinnostusta ja ymmärrystä asiasta. **Suuremmissa yrityksissä** huomioidaan kyberuhat usein vastuuasioiden ja taloudellisten menetysten pelon vuoksi.
Tietoturva	**Pienissä toimistoissa** erittäin harvat asiakkaat ovat kiinnostuneita tilitoimiston tietoturvajärjestelyistä → Taloushallintoliiton auktorisoimalla tilitoimistolla on tehtynä tietoturvasta selonteko Taloushallintoliitolle. **Suuremmissa tilitoimistoissa**, joissa on asiakkaana esimerkiksi pörssiyhtiöitä voidaan vaatia tarkempia selosteita tietoturvan varmistamiseksi. Joidenkin pörssiyhtiöiden vaatimuksesta tilitoimistolla tulee olla tietyt sertifikaatit täyttävät tietoturvajärjestelyt. Sertifikaattien toteutumista käy tarkistamassa ulkopuolinen auditoija.	Kukaan ei valvo kirjanpitotoimistojen eikä tilitoimistojen toimintaa. → Alan piirissä yli 6000 yritystä, joista valtaosa pieniä 1–2 hengen yrityksiä. → Taloushallintoliiton 600 jäsenelle on tehty itsearviointilomakkeen avulla tarkastus tietoturvan tasosta. Arvio on, että tilitoimistoissa ollaan tietoturvan suhteen valveutuneimpia kuin keskimäärin muilla aloilla → Taloushallinnon alaa velvoittaa tietosuoja-asetus. Pelko siitä, että tilitoimistot eivät ilmoita kaikista tietoturvapoikkeamista → Tietämättömyys, pelätään mainehaittaa.	Tietoturvasta tulisi olla alaa velvoittava lainsäädäntö, jolloin tietoturvapoikkeamista tulee ilmoittaa viranomaisille. → Muutoin tietoturva ei välttämättä ole riittävällä tasolla ja ilmoituksia poikkeamista ei hyvin suurella todennäköisyydellä tehdä. Tietoturvan lainsäädäntöä koskeva NIS-direktiivi on uudistumassa, jolloin toimialavelvoittavuus laajenee koskemaan useampaa toimialaa. → Ei tule koskemaan vielä taloushallinnon alaa.

Toimenpiteet	**Pienissä toimistoissa** ei kyberturvallisuuteen liittyviä erillisiä koulutuksia työntekijöille oletettavasti järjestetä. → Tietoa saadaan mm. Taloushallintoliiton, Yrittäjät ry:n ja Kauppakamarin kautta **Suuremmissa yrityksissä** on tietoturva- ja kyberkoulutuksia enemmän. → Koulutukset usein omalla koneella töiden lomassa toteutettavia koulutuksia. Työntekijät noudattavat ohjeita, mutta koulutuksiin ei jää hirveästi aikaa.	Huoltovarmuuskeskukselta on saatu rahoitus koulutushankkeeseen, jonka tarkoituksena on edistää taloushallinnon alan toimijoiden tietoturvaosaamista. → Koulutukset olisi tarkoitus toteuttaa siten, että tilitoimistojen työntekijät voivat suorittaa koulutuksen netin välityksellä omalla koneella ja suorituksesta saa merkinnän, jolla voi todentaa omaa tietoturvaosaamistaan.	Kyberturvallisuus yleisesti ottaen kiinnostaa, mutta toimenpiteisiin ryhtymisessä on erittäin suurta vaihtelua myös isommilla yrityksillä. → Usein otetaan yhteyttä vasta kun on sattunut jotain. Pelkkä tietoturvajohtajan palkkaaminen ei riitä, vaan yrityksen tulee myös noudattaa niitä neuvoja mitä tietoturvajohtaja antaa ja tehdä tarvittavia toimenpiteitä. → Tarvittavaa kiinnostusta ja ymmärrystä tieto- ja kyberturvallisuusasioihin tuskin tulee, ennekuin viranomainen vaatii niitä.