LAPIN AMK
Lapland University of Applied Sciences

PIENYRITYKSEN TIETOTURVAN KEHITTÄMINEN – CASE: YRITYS X

Johansson Anne

Opinnäytetyö

Tietojenkäsittelyn koulutus
Tradenomi (AMK)

2024

LAPIN AMK
Lapland University of Applied Sciences

Opinnäytetyön tiivistelmä

Tietojenkäsittelyn koulutus
Tradenomi (AMK)

Tekijä	Anne Johansson	**Vuosi**	2024
Ohjaaja	Marko Leinonen		
Toimeksiantaja	Yritys X		
Työn nimi	Pienyrityksen tietoturvan kehittäminen – Case: Yritys X		
Sivumäärä	49 + 7		

Tämän opinnäytetyön tavoitteena oli kartoittaa, millaisia tietoturvakäytäntöjä Yritys X:llä on käytössä, sekä mitkä ovat keskeisimmät riskit yrityksessä. Lisäksi oli tavoitteena selvittää, mitä konkreettisia toimenpiteitä ja käytäntöjä Yritys X voisi ottaa käyttöönsä tietoturvan parantamiseksi. Yritys X:n tietoturvan nykytilan selvittämiseksi käytettiin sähköistä kyselylomaketta, joka lähetettiin koko henkilöstölle. Saatujen vastausten perusteella luotiin konkreettisia toimenpide-ehdotuksia ja suosituksia sisältävä kehityssuunnitelma.

Tietoperustassa tarkasteltiin tietoturvan keskeisiä käsitteitä, kuten CIA-mallia, sekä yleisimpiä tietoturvauhkia, joihin kuuluvat muun muassa tietojenkalastelu, haittaohjelmat ja palvelunestohyökkäykset. Lisäksi käsiteltiin tietoturvakäytäntöjä sekä erilaisia riskejä. Aineiston analysoinnissa hyödynnettiin laadullista lähestymistapaa.

Tutkimuksen tulokset osoittavat, että Yritys X:n tietoturvaan suhtaudutaan positiivisesti ja sen merkitys liiketoiminnalle ymmärretään, mutta käytännöissä on kehittämisen varaa. Tutkimuksessa havaittiin epäselvyyksiä tietoturvavastuissa, puutteita salasanojen hallinnassa sekä kriittisten tietojen sijaintia ei tunnettu kattavasti. Tulosten perusteella laadittiin kehityssuunnitelma, jossa toimenpide-ehdotuksina ovat muun muassa selkeän tietoturvapolitiikan luominen, henkilöstön koulutus sekä salasanojen hallinnan parantaminen. Tuloksia voidaan hyödyntää paitsi case-yrityksessä, myös muissa samankaltaisissa pienyrityksissä, joissa resurssit ovat rajalliset.

Avainsanat CIA-malli, haittaohjelmat, tietoturvakäytäntö, riskit, tietojenkalastelu, tietoturva

LAPIN AMK
Lapland University of Applied Sciences

Abstract of the thesis

Business Information Technology
Bachelor of Business Administration

Author	Anne Johansson	**Year**	2024
Supervisor	Marko Leinonen		
Commissioned by	Company X		
Title	Developing the information security in a small business - Case study: Company X		
Number of pages	49 + 7		

The objective of this thesis was to investigate the information security practices in use at Company X and identify the key risks within the organization. Additionally, the goal was to determine what concrete measures and practices Company X could implement to improve its information security. To assess the existing state of information security at Company X, an electronic questionnaire was distributed to the entire staff. A development plan was then created, based on the responses given. The plan includes concrete recommendations and proposals on how the company could improve its information security.

Key concepts of information security were covered in the knowledge base, such as the CIA model, as well as common threats like phishing, malware, and denial-of-service attacks. In addition, information security practices and various risks were discussed. A qualitative approach was utilized in the analysis of the data.

The results of the study indicate that Company X has a positive attitude toward information security and recognizes its significance for business operations. However, there is room for improvement in existing practices. The study identified uncertainties in information security responsibilities, shortcomings in password management, and the location of critical information was not fully known. Based on the findings, a development plan was created with recommendations, including the establishment of a clear information security policy, staff training, and improvements in password management. The results can be utilized not only in Company X but also in other similar small businesses where resources are limited.

Keywords CIA-model, information security, malware, phishing, practice, risks

SISÄLLYS

1 JOHDANTO

1.1 Tarkoitus ja tavoitteet

Tieto- ja viestintätekniikka on nykyään olennainen osa lähes kaikkia liiketoiminnan ja yhteiskunnan toimintoja. Vaikka tietokoneisiin luotetaan, ne ovat usein alttiita riskeille. Tietoturvan pääasiallinen tehtävä on löytää keinoja näiden riskien hallitsemiseksi ja minimoimiseksi. (Gupta & Goyal 2020, 17.) Traficomin (2020, 3) mukaan erilaiset tietoturvauhkat koskettavat kaiken kokoisia yrityksiä, ja tällaisen uhkan toteutuessa voi pienyrityksen toiminta seisahtua kokonaan. Tietoturva on tästä syystä yrityksille elintärkeää, koska se turvaa liiketoiminnan kannalta tärkeitä tietoja, kuten asiakas-, talous- ja liikesalaisuuksia. Tietomurrot ja vuotaneet tiedot voivat aiheuttaa huomattavia taloudellisia vahinkoja ja vahingoittaa yrityksen mainetta. (Konttoripiste 2024.)

Moni pienyrittäjä saattaa kuvitella, että heidän yrityksensä on liian pieni herättääkseen verkkorikollisten kiinnostuksen. Usein ajatellaan, ettei yrityksellä ole rahanarvoisia tietoja, joita voitaisiin varastaa. Jokaisella yrittäjällä on kuitenkin arvokasta tietoa, jonka menettäminen tai joutuminen vääriin käsiin voi aiheuttaa merkittävää vahinkoa. (Järvinen 2022, 33.) Tästä syystä suhtautumista tietoturvaa kohtaan on tärkeää pyrkiä edistämään. Traficom (2020, 3) painottaa, että tietoturvan ei tarvitse olla vaikeaa, vaan monille pienillä teoilla voi merkittävästi lisätä turvallisuutta ja välttyä erilaisilta uhilta.

Opinnäytetyössä tarkastellaan tietoturvaa sekä yleisellä tasolla että Yritys X:n näkökulmasta. Työssä käsitellään keskeisiä tietoturvan peruskäsitteitä kuten muun muassa CIA-mallia (Confidentiality, Integrity, Availability), joka muodostaa tietoturvan perustan korostaen tiedon luottamuksellisuutta, eheyttä ja saatavuutta (Andress 2014, 5). Lisäksi työssä käsitellään erilaisista uhkia, kuten tietojenkalastelua, haittaohjelmia ja palvelunestohyökkäyksiä.

Työ keskittyy tekniseen tietoturvaan, joka on monipuolinen ja laaja osa-alue. Sen ymmärtäminen ja käytännön toteuttaminen ovat ratkaisevia yrityksen turvallisuuden ja toiminnan jatkuvuuden varmistamisessa. Tekninen tietoturva on keskeinen osa yrityksen kokonaisvaltaista tietoturvaa, ja sen avulla pyritään ehkäisemään tietoturvauhkia, jotka ovat kasvaneet räjähdysmäisesti viime vuosina. (Jurvanen

2023b.) Valitsin teknisen tietoturvan, koska se on näkyvin osa Yritys X:n tietoturvaa ja tarjoaa konkreettisia keinoja suojautua uhkilta.

Opinnäytetyön tarkoituksena on kehittää Yritys X:n tietoturvaa siten, että sen tietoturvakäytännöt pyrkivät vastaamaan nykypäivän uhkiin ja vaatimuksiin. Työssä selvitetään nykyiset tietoturvariskit ja -heikkoudet sähköisellä kyselyllä, sekä laaditaan saatujen vastausten perusteella kehityssuunnitelma. Suunnitelmassa otetaan huomioon tapausyrityksen resurssit, jotta ehdotetut ratkaisut ovat realistisia ja toteuttamiskelpoisia yrityksen arjessa.

Opinnäytetyö toimii samalla yleisenä tietolähteenä, tarjoten suosituksia ja konkreettisia toimenpiteitä, joiden avulla tietoturvaa on mahdollista parantaa. Työssä esitetyt ratkaisut ovat helposti sovellettavissa muihin pienyrityksiin, jotka haluavat parantaa tietoturvaa vähäisillä resursseilla.

Yritys X:n tietoturvan nykytilan ja kehitystarpeiden arvioimiseksi opinnäytetyössä vastataan seuraaviin kysymyksiin:

1. Millaisia tietoturvakäytäntöjä Yritys X:llä on käytössä tällä hetkellä?
2. Mitkä ovat keskeisimmät tietoturvariskit Yritys X:ssä?
3. Mitä konkreettisia toimenpiteitä ja käytäntöjä Yritys X voi ottaa käyttöönsä tietoturvan parantamiseksi?

Ensimmäinen kysymys antaa lähtökohdan ymmärtää miten Yritys X on tällä hetkellä suojattu tietoturvauhkilta ja missä mahdolliset puutteet sijaitsevat. Arvioimalla nykytilan voidaan asettaa realistiset tavoitteet tietoturvan kehittämiselle. Toinen kysymys on hyvin tärkeä, koska tietoturvan parantaminen alkaa riskien tunnistamisesta. Ymmärtämällä mitkä ovat Yritys X:n suurimmat uhkat, voidaan kohdistaa toimenpiteet niihin riskeihin, jotka ovat todennäköisimpiä tai joilla on suurin vaikutus yrityksen toimintaan. Kolmannen kysymyksen avulla pyritään löytämään käytännön ratkaisuja yrityksen tietoturvan parantamiseen. On tärkeää määrittää konkreettiset askeleet, joilla Yritys X voi vahvistaa tietoturvaansa.

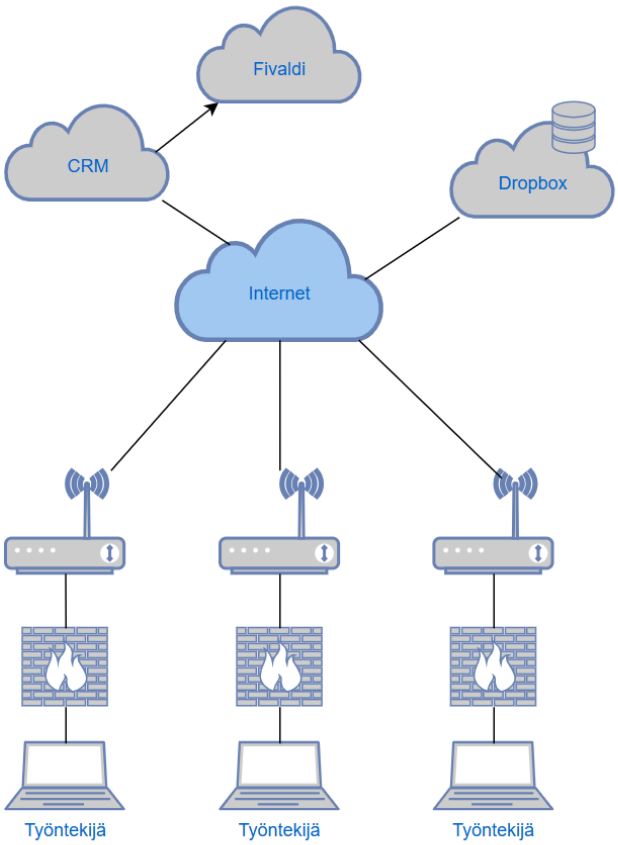
1.2 Toimeksiantajan kuvaus

Yritys X on kolmen hengen yritys, jossa yrittäjän lisäksi työskentelee säännöllisesti kaksi henkilöä. Satunnaisesti yrityksessä työskentelee myös esimerkiksi kesätyöntekijöitä edellä mainitun vakituisen henkilöstön lisäksi. Yritys X toimii jälleenmyyjänä palvellen kaiken kokoisia yrityksiä ja yhdistyksiä. Myytävät tuotteet hankitaan Suomesta ja EU:n alueelta, mutta jonkin verran on tuontia myös EU:n ulkopuolelta, lähinnä Aasiasta.

Yritys X:llä on oma verkkosivusto, jossa se esittelee jälleenmyytäviä tuotteitaan. Sivusto toimii eräänlaisena tuotekatalogina ja sisältää tuhansia tuotevaihtoehtoja ollen siten tärkeä työväline henkilöstölle. Asiakas voi jättää tarjouspyynnön tai tarjouskyselyn verkkosivuston kautta. Asiakkaiden, alihankkijoiden ja tavarantoimittajien kanssa viestitään pääasiassa sähköpostitse.

Tietoturvaan ei Yritys X:ssä ole aikaisemmin kiinnitetty erityistä huomiota. Tämän vuoksi tavoitteena on laatia selkeä ja käytännönläheinen kehityssuunnitelma, joka sisältää konkreettisia suosituksia tietoturvan parantamiseksi sekä yrityksen suojaamiseksi nykyisiltä ja tulevilta uhkilta.

Kuviossa 1 on esitetty Yritys X:n etätyöskentelyn verkkokaavio, jossa on havainnollistettu, miten käytössä oleviin järjestelmiin ollaan yhteydessä. Työntekijöiden laitteet on yhdistetty kunkin omaan kotona olevaan reitittimeen, joka puolestaan yhdistää heidät internetiin. Pilvipalvelut, joita työskentelyssä käytetään, ovat: CRM-järjestelmä (Customer Relationship Management), Fivaldi-laskutusjärjestelmä sekä Dropbox-pilvitallennustila. CRM-järjestelmästä on integraatio Fivaldiin, josta laskutus hoidetaan.



Kuvio 1. Yritys X:n etätyöskentelyn verkkokaavio

2 TIETOTURVA

2.1 Tietoturva ja sen tarkoitus

Tietoturvalla tarkoitetaan tietojen ja tietojärjestelmien suojaamista luvattomalta pääsyltä, käytöltä, paljastumiselta, häiriöiltä sekä muutoksilta tai tuhoutumiselta. Yksinkertaistettuna kyse on siitä, että tiedot halutaan turvata niiltä, jotka voivat käyttää niitä väärin. Laajemmin ajateltuna turvallisuus tarkoittaa omaisuuden suojaamista, mikä voi sisältää suojautumisen verkkohyökkäyksiltä, viruksilta, varkauksilta tai vahingonteolta. (Andress 2014, 3.)

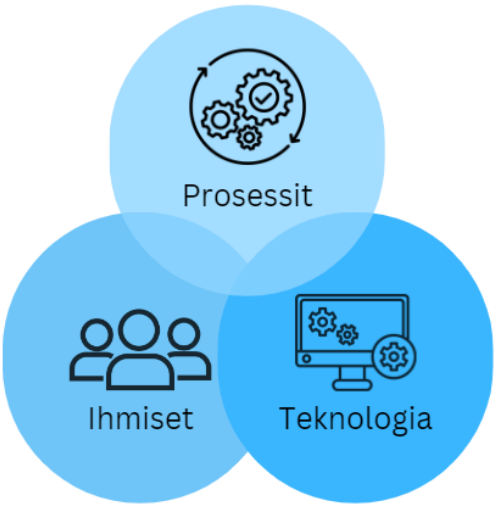
Tietoja pyritään suojaamaan järjestelyillä, joilla varmistetaan niiden luottamuksellisuus, eheys ja saatavuus. Tällaisia järjestelyitä voivat olla esimerkiksi virustorjuntaohjelman käyttö, palomuurin käyttö tai varmuuskopiointi. (Sanastokeskus ry 2024.) Kailan ja Nymanin (2018, 33) mukaan tietoturvassa on kyse tietoisuudesta ja nimenomaan siitä, että tietää mitä suojella ja miten sitä suojataan. Kyse on heidän mukaansa myös siitä, että osaa toimia oikein silloin kun asiat menevät vikaan.

2.2 Tietoturvan peruspilarit ja CIA-malli

Sussmanin (2022) mukaan ihmiset, prosessit ja teknologia ovat tehokkaan tietoturvan peruspilareita. Jotkut organisaatiot saattavat hänen mielestään panostaa huipputeknologiaan ilman riittävää osaamista sen käyttöönottoon, kun taas toiset palkkaavat alan parhaita osaajia, mutta yritykseltä puuttuu tarvittavat prosessit. Jotkut taas keskittyvät hyvin laadittuihin prosesseihin ilman tarvittavaa teknologiaa. Näissä tapauksissa tietoturva on epätasapainossa ja ei siten riitä kattamaan kaikkia turvallisuustarpeita. Siksi kolme peruspilaria, ihmiset, prosessit ja teknologia, ovat kattavan suojan perusta.

Kolmesta pilarista ihmisten rooli on keskeinen, koska he muodostavat ensimmäisen suojakerroksen uhkia vastaan. Koulutus ja tietoisuus auttavat työntekijöitä tunnistamaan ja välttämään vaaroja, kuten muun muassa tietojenkalastelua. Toinen pilari pitää sisällään prosessit, jotka muun muassa sisältävät asianmukaiset

politiikat. (Sussman 2022.) Kolmannessa pilarissa keskitytään siihen, miten teknologian toimivuus edellyttää, että käytössä on osaava henkilöstö, selkeät prosessit ja suunnitelma, joka varmistaa, että teknologiaa käytetään oikealla tavalla ja oikeisiin tarkoituksiin (XeneX 2023). Kuviossa 2 on havainnollistettu nämä kolme tietoturvan peruspilaria.



Kuvio 2. Tehokkaan tietoturvan peruspilarit (mukaillen XeneX 2023)

Näiden kolmen peruspilarin tasapainon löytäminen voi olla haastavaa. Monilta yrityksiltä puuttuu vahva perusta kaikilla kolmella osa-alueella, mikä tekee niistä alttiimpia tietoturvauhkille. Epätasapaino osa-alueiden välillä voi näkyä kaiken kokoisissa organisaatioissa, mikä heikentää niiden kykyä suojautua. Pienillä organisaatioilla on usein puutteita tietoturvaosaamisessa, koska niillä ei ole varaa palkata huippuosaajia. Tämän vuoksi ne eivät pysty hyödyntämään kaikkia käytössään olevia turvallisuustyökaluja resurssien puutteen vuoksi. Tämä johtaa usein siihen, että rikollisten silmissä pienet yritykset ovat kiinnostavampia kohteita, mikä voi houkutella rikollisia. (Sussman 2022.)

Organisaatioiden koosta riippumatta tietoturvan toteuttamisessa on usein haasteita. Monilla yrityksillä saattaa olla puutteellisia tai huonosti määriteltyjä tietoturvastrategioita, eikä heillä välttämättä ole yhtenäisiä prosesseja uhkien tutkimiseen, havaitsemiseen ja torjuntaan. Usein luotetaan pelkästään käytössä ole-

vaan teknologiaan suojana, mutta jos ihmisten ja prosessien pilarit eivät tue teknologiaa tasapainoisesti, se rajoittaa kykyä hyödyntää teknologian tuottamaa tietoa tehokkaasti. (Sussman 2022.)

Kun puhutaan tietoturvasta, vastaan tulee hyvin usein CIA-triadi, eli CIA-malli, joka koostuu kolmesta keskeisestä tietoturvaperiaatteesta; confidentiality, integrity ja availability (Andress 2014, 5). Suomennettuna nämä tarkoittavat tiedon luottamuksellisuutta, eheyttä ja saatavuutta (Bautomo 2024). Kuviossa 3 esitetyn CIA-mallin avulla voidaan paremmin hahmottaa, mitä tietoturva on ja onko se riittävällä tasolla yrityksessä (Forculus 2024).

Kuvio 3. Kolme keskeistä tietoturvaperiaatteetta (mukaillen Andress 2014, 5)

Luottamuksellisuus (confidentiality) on käsite, joka liittyy läheisesti yksityisyyteen, mutta ei ole täysin sama asia. Se on yksityisyyden olennainen osa ja tarkoittaa kykyä suojata tietoja niiltä, joilla ei ole lupaa päästä niihin käsiksi. (Andress 2014, 6.) Järvisen (2022, 13) mukaan tällaisia tietoja ovat mm. sähköpostien sisältö ja langaton verkkoliike, joita täytyy suojata siten, etteivät ulkopuoliset pääse niihin käsiksi. Luottamuksellisuus voi olla uhattuna, jos esimerkiksi tietoja sisältävä tietokone katoaa, joku tarkkailee salaa, kun kirjoitetaan salasanaa, sähköpostin liite päätyy vahingossa väärälle vastaanottajalle tai jos hyökkääjä pääsee murtautumaan järjestelmään (Anderss 2014, 6).

Eheydellä (integrity) viitataan kykyyn suojata tietoja luvattomilta ei-toivotuilta muutoksilta. Tämä voi myös tarkoittaa sitä, että tietoja tai niiden osia ei saa muuttaa tai poistaa ilman lupaa, mutta se voi myös käsittää valtuutetut muutokset, joita ei kuitenkaan ole tarkoitus toteuttaa. Turvatakseen eheyden, edellytetään, että luvattomat muutokset estetään ja valtuutettuja muutoksia voidaan tarvittaessa perua. Eheys on erityisen tärkeä silloin, kun kyseessä ovat tiedot, jotka toimivat muiden päätösten perustana (Anderss 2014, 6–7.) Tietoihin, joihin saa olla pääsy vain tietyillä henkilöillä, edellytetään käyttäjien tunnistamista ja todentamista. Tällaisia tietoja ovat esimerkiksi palkkatiedot. (Järvinen 2022, 14.)

CIA-mallin viimeinen osa-alue on saatavuus (availability). Saatavuus tarkoittaa sitä, että tiedot ovat käytettävissä silloin, kun niitä tarvitaan. Saatavuuden menetys voi johtua monenlaisista katkeamista missä tahansa tietojen käyttöön pääsyä mahdollistavassa ketjussa. Tällaisia ongelmia voivat aiheuttaa esimerkiksi sähkökatkot, käyttöjärjestelmän tai sovellusten viat, verkkohyökkäykset, järjestelmän haavoittuvuudet tai muut häiriöt. Jos ongelmat ovat ulkopuolisen aiheuttamia, kuten hyökkääjän, niitä kutsutaan yleisesti palvelunestohyökkäyksiksi (Denial of Service, DoS). (Anderss 2014, 7.) Saatavuus on enimmäkseen tekninen ongelma, kuten nettiyhteyden pätkiminen tai kun kone ei käynnisty, ja tällaisia ongelmia pyritään estämään teknisillä keinoilla. (Järvinen 2022, 14–15.)

2.3 Tietoturvan osa-alueet

Tietoturva koostuu kolmesta osa-alueesta: teknisestä, fyysisestä ja hallinnollisesta tietoturvasta. Teknisessä tietoturvassa keskitytään laitteiden, tietojärjestelmien ja tietoverkkojen suojaamiseen. Fyysinen tietoturva kattaa konkreettiset toimenpiteet ja varotoimenpiteet, joilla suojataan laitteet, tilat ja muut fyysiset resurssit. Hallinnollisen tietoturvan tehtävä taas on ohjata teknistä ja fyysistä tietoturvaa ja auttaa yritystä tunnistamaan ja hallitsemaan tietoturvauhkia ja -riskejä. Sen avulla varmistetaan, että tietoturvastrategia on kattava ja ajantasainen. Nämä kolme osa-aluetta täydentävät toisiaan ja niiden on oltava yhteensovitettuja saumattoman tietoturvan saavuttamiseksi. (Jurvanen 2023a.)

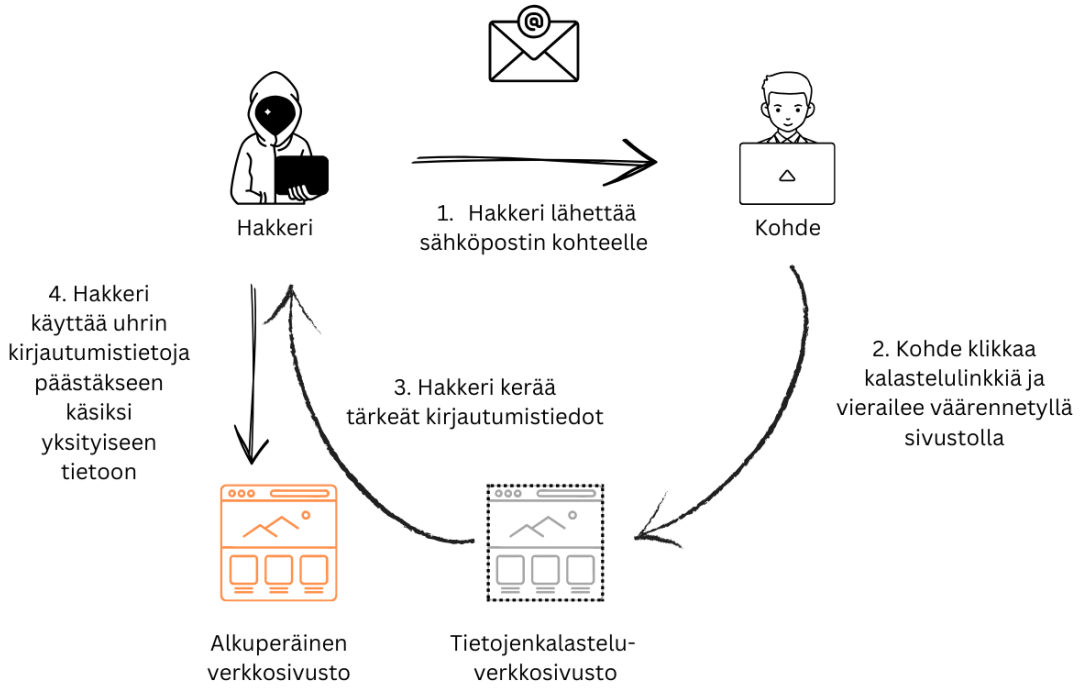
Tässä työssä keskitytään tekniseen tietoturvaan, joka on olennainen yritysten turvallisuuden ja toiminnan jatkuvuuden kannalta. Se on keskeinen osa kokonaisvaltaista tietoturvaa ja auttaa ehkäisemään nopeasti kasvaneita tietoturvauhkia. (Jurvanen 2023b.)

Tekninen tietoturva voidaan jakaa kolmeen pääkategoriaan: laitteisto, ohjelmisto sekä toimintapolitiikat. Laitteistot ovat fyysisiä laitteita, jotka suojaavat järjestelmää, kuten mm. palomuureja. Tähän voi kuulua myös salausalgoritmeja käyttäviä laitteita ja biometrisiä tunnistuslaitteita. Ohjelmistot sisältävät erilaisia sovelluksia ja järjestelmiä, joiden tarkoitus on suojata tietojärjestelmiä erilaisilta uhkilta. Näihin kuuluvat esimerkiksi virustentorjuntaohjelmistot, vakoiluohjelmien tunnistusohjelmat ja muut haittaohjelmien torjuntaan suunnitellut ohjelmistot. Hallinnollisella tietoturvalla, eli toimintapolitiikoilla viitataan ohjeisiin ja sääntöihin, jotka määrittelevät teknologian käytön periaatteet sekä tietoturvan ylläpidon. (Jurvanen 2023b.)

2.4 Hyökkäystyypit ja tavat

Erilaisia verkkohyökkäystyyppejä on monenlaisia, ja ne perustuvat jokainen omanlaiseen menetelmään, jonka tarkoitus on varastaa arkaluontoisia tietoja (Rouse 2024). Traficomin (2020, 4) mukaan pienetkin kyberturvallisuustapahtumat, kuten tietojenkalastelu, haittaohjelmat, ja kiristyshaittaohjelmat voivat aiheuttaa pienyrityksille merkittäviä ja ei-toivottuja vaikutuksia.

Tietojenkalastelun (phishing) tarkoituksena on huijata viestin vastaanottajaa antamaan tärkeitä tietoja tai saada pääsy johonkin järjestelmään. Kuka tahansa kelpaa uhriksi, ja tällaisen tietojenkalasteluviestin voi saada sähköpostin lisäksi mm. sosiaalisen median kautta. Tietojenkalastelu voi tapahtua esimerkiksi siten, että käyttäjältä pyydetään pankin nimissä luottokortin numero ja samalla myös kortin tunnusluku. (Traficom 2020, 4.) Tällaiset tietojenkalasteluviestit näyttävät usein tulevan luotettavasta lähteestä (Rouse 2024), joten niiden tunnistaminen voi olla vaikeaa. Kuviossa 4 havainnollistetaan esimerkin avulla, miten tietojenkalastelu voi tapahtua.



Kuvio 4. Esimerkki tietojenkalastelusta (mukaillen Valimail 2024)

Microsoftin (2024) mukaan paras tapa suojautua tietojenkalastelulta, on oppia tunnistamaan erilaiset viestit. Heidän mukaansa kiireellinen kehotus toimia on yleinen temppu, jolloin viestin saaja ei ajattelisi asiaa liikaa. Lisäksi oikeinkirjoitukseen ja kielioppiin on hyvä kiinnittää huomiota. Yleiset tervehdykset, kuten ”Hyvä herra” tai ”Hyvä rouva” ovat myös asioita, joiden pitäisi soittaa hälytyskelloja. Jos viesti sisältää epäilyttäviä linkkejä tai odottamattomia liitteitä, niitä ei saisi koskaan avata, ellei voi olla varma, että kyseessä ei ole huijaus.

Haittaohjelman (malware) tarkoitus on aiheuttaa ei-toivottuja tapahtumia tietojärjestelmässä tai sen osassa. Erilaisia haittaohjelmatyyppejä ovat esimerkiksi virus, vakoiluohjelma (spyware), troijalainen tai mato. Haittaohjelman asentamisella tavoitellaan usein taloudellista hyötyä, ja se voidaan asentaa varastamaan tärkeitä tietoja tai esimerkiksi seuraamaan tietokoneen käyttäjän toimintaa. Haittaohjelman avulla rikollinen voi varastaa tietoa, salata tiedostoja, vakoilla tai tehdä muuta rikollista toimintaa. (Traficom 2020, 7.) Haittaohjelmat voivat levitä monin eri tavoin, kuten sähköpostin, huolimattoman selailun seurauksena tai muiden ohjelmistojen mukana. Esimerkiksi mainoksen tai ponnahdusikkunan klikkaaminen voi johtaa siihen, että laitteelle latautuu huomaamatta haittaohjelma, kuten näppäilyntallennin tai troijalainen. (NordVPN 2024b.)

IBM:n (2024) mukaan haittaohjelmien vaikutukset voivat vaihdella suuresti verkkorikollisten tavoitteiden mukaan. Vaikutukset voivat heidän mukaansa olla erittäin tuhoisia ja kalliita, kuten kiristyshaittaohjelmat, tai vain lievästi häiritseviä, kuten ärsyttävät mainosohjelmat. Haittaohjelmilta voi suojautua yksinkertaisilla keinoilla; mm. käyttämällä hyvämaineista tietoturvaohjelmistoa, olemalla varovainen internetin käyttäjä sekä pitämällä ohjelmistot ajan tasalla, koska uusimman päivitykset paikkaavat usein juuri löydettyjä tietoturvahaavoittuvuuksia (NordVPN 2024b).

Traficomin (2020, 8–9) mukaan kiristyshaittaohjelma (ransomware) leviää usein aidolta näyttävän sähköpostin kautta, joka sisältää linkin tai liitetiedoston. Kun liite avataan tai linkkiä klikataan, haittaohjelma pääsee tietokoneelle ja salaa sen tiedostot, estäen niiden käytön ilman oikeaa salauksenpurkuavainta. Rikolliset vaativat yleensä lunnaita virtuaalivaluuttana, kuten bitcoinina, luvaten poistaa salauksen maksun jälkeen. Tiedostojen palauttamisesta ei kuitenkaan ole takuita, ja tiedot voidaan jakaa myöhemmin, vaikka lunnaat olisi maksettu. Traficom neuvoo, ettei lunnaita maksettaisi, koska ei ole lainkaan selvää, että ongelma ratkeaa maksun jälkeen.

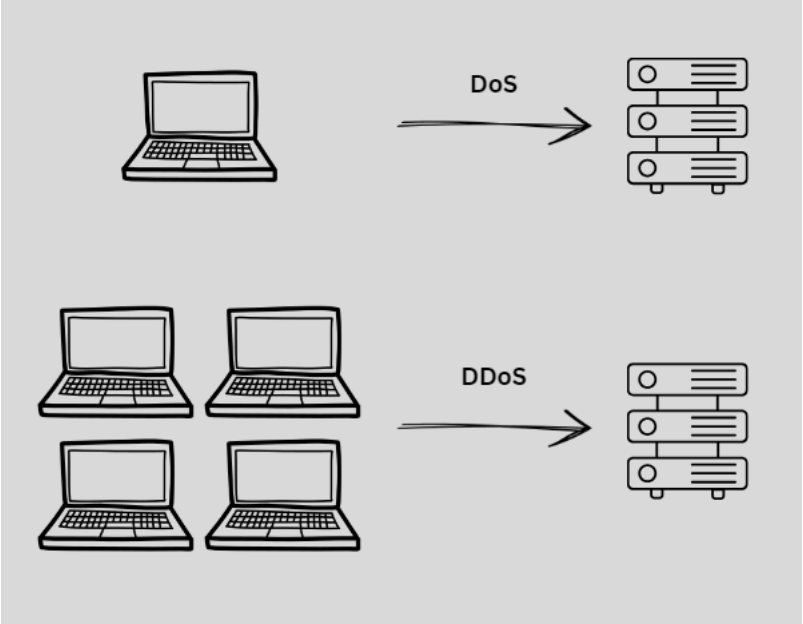
Kiristyshaittaohjelmia on olemassa myös erilaisia. Yleisin tyyppi on Kosinskin (2024) mukaan salaava kiristysohjelma, mutta vähemmän tunnettu on ohjelmatyyppi, joka lukitsee koko laitteen estämällä pääsyn käyttöjärjestelmään, jolloin laitetta käynnistettäessä näyttöön ilmestyy lunnasvaatimus. Kiristyshaittaohjelmat ovat yksi yleisimmistä haittaohjelmista, ja niiden aiheuttamat hyökkäykset voivat aiheuttaa kohdeorganisaatiolle suuria kustannuksia.

Kiristyshaittaohjelmilta voi suojautua samalla tavoin kuin haittaohjelmilta, josta kerrottiin aiemmin. Kiristyshaittaohjelmilta voi suojautua mm. pitämällä ohjelmistopäivitykset sekä tietoturvaohjelmisto ajan tasalla, ja huolehtia tiedostojen ja järjestelmän säännöllisesti varmuuskopioinnista (Selviytymisopas kiristyshaittaohjelmia vastaan 2016, 2).

Palvelunestohyökkäys (Denial of Service - DoS) on hyökkäysmenetelmä, jossa hyökkääjä pyrkii lamauttamaan verkkosivuston tai palvelun toiminnan häiritsemällä sen normaalikäyttöä, esimerkiksi kuormittamalla järjestelmää liiallisilla

pyynnöillä tai hyödyntämällä haavoittuvuutta palvelussa tai verkkolaitteessa. Palvelunestohyökkäys havaitaan yleensä palveluiden toimintakatkoksista tai niiden hidastumisesta. (Traficom 2022, 2–5.) F-Securen (2024b) mukaan DoS-hyökkäys toteutetaan yhdestä internetiin kytketystä laitteesta.

DDoS-hyökkäys (Distributed Denial of Service) tarkoittaa F-Securen (2024b) mukaan sellaista palvelunestohyökkäystä, johon osallistuu monia laitteita, ja joiden yhteistyö mahdollistaa huomattavasti suuremman liikennemäärän tuottamisen kuin mitä yksi hyökkääjä yksin pystyisi saamaan aikaan. Tällaista hyökkäystä kutsutaan hajautetuksi palvelunestohyökkäykseksi, jonka taustalla voi olla esimerkiksi tavallisten käyttäjien tietokoneita, jotka lähettävät pyyntöjä jatkuvasti kohteena olevalle verkkosivustolle palvelunestohyökkäyksen aikana. Kuviossa 5 esitetään yksinkertaistettuna DoS- sekä DDoS-hyökkäystavat.



Kuvio 5. DoS ja DDoS-hyökkäyksen toimintaperiaate (mukaillen Cloudflare 2024)

Palvelunestohyökkäyksiltä suojautuminen voi vaatia sellaista asiantuntijuutta ja laitteistoa, jota ei normaalisti ole käytössä. On kuitenkin hyvä tunnistaa varautumistarve ja vähintäänkin tiedettävä, mistä ja millä aikataululla asiantuntija-apua on mahdollista saada. (Palvelunestohyökkäysten ehkäisy ja torjunta 2016, 5.)

2.5 Tietoturvahyökkäykset Suomessa

Palvelunestohyökkäykset ovat F-Securen (2024b) mukaan maailmanlaajuinen ilmiö, joka aiheuttaa haittaa myös Suomessa. Heikkilän (2024) Ylelle toimittaman uutisen mukaan Nordea on syksyn 2024 aikana ollut usean palvelunestohyökkäyksen kohteena. Tällainen palvelunestohyökkäys vaikeuttaa verkkopankkiin pääsyä sekä hankaloittaa palveluihin kirjautumista, joissa käytetään vahvaa tunnistautumista (Jäärni 2024).

Traficomin (2024b) mukaan Dropbox-teemainen M365-tunnusten kalastelu on ollut aktiivista alkusyksystä 2024 ja Kyberturvallisuuskeskukselle on ilmoitettu monista M365-tilien tietomurroista näiden Dropbox-kalastelujen seurauksena. Tässä kalastelutavassa vastaanottaja saa sähköpostiinsa Dropbox-palvelun kautta pdf-tiedoston, joka sisältää linkin sivustolle, jossa kysytään M365-tunnuksia. Kun tunnukset syötetään sivustolle, päätyvät ne rikollisten haltuun. M365-tilille päästyään rikolliset kaappaavat käyttäjän mahdollisesti jo voimassa olevan Dropbox-tilin tai tekevät uuden tilin käyttäjän nimissä. M365-tilin palauttaminen on kohtuullisen helppoa, mutta Dropbox-tilin hallintaan organisaatiolla ei ole pääsyä, joten sen palauttaminen on miltei mahdotonta. Tietojenkalastelua vastaan voi suojautua muun muassa monivaiheisella tunnistautumisella.

2.6 Tietoturvan kehittäminen ja kontrollikeinot

Nykypäivänä tietoturvan jatkuva parantaminen ei ole vain vapaaehtoinen osa tietoturvaa, vaan se on elintärkeää, jotta yritys voi selviytyä ja kehittyä. Tietoturvan merkitys on kasvanut valtavasti nykypäivän digitaalisessa liiketoimintaympäristössä. Asiakassuhteiden ylläpitäminen, liiketoiminnan jatkuvuuden varmistaminen sekä kilpailukyvyn säilyttäminen ovat asioita, jotka korostavat tietoturvan merkitystä kyberuhkien lisääntyessä. Kiinnittämällä huomiota tietoturvan jatkuvaan kehittämiseen yritys voi suojautua paremmin riskeiltä ja edistää siten menetystä. (Integral 2024.)

Näkemykseni mukaan yrityksen tietoturvan kehittämisen lähtökohtana on tunnistaa, millaisia riskejä yrityksellä on, ja mitkä kohteet ja tiedot halutaan suojata.

Kailan ja Nymanin (2018, 34) mukaan yritysten omaisuuksien ja riskien tunnistaminen oli aiemmin yksinkertaisempaa kuin nykypäivänä. Monet yritykset käsittelevät heidän mukaansa nykyään tietoa fyysisten resurssien sijasta, minkä takia ns. näkymättömien tietovarantojen ja niihin liittyvien riskien listaaminen on hankalampaa. Omaisuuksiin voi kuulua esim. asiakkaille tarjottavat palvelut tai järjestelmät ja henkilöt, jotka tekevät palvelun tarjoamisen mahdolliseksi.

Kehittämisen ensimmäisessä vaiheessa on tärkeää tunnistaa omaisuudet ja riskit. Tavoitteena ei ole käydä läpi kaikkia mahdollisia riskejä, vaan keskittyä tunnistamaan tärkeimmät uhat, jotka kohdistuvat suojausta tarvitseviin keskeisiin resursseihin. (Kaila & Nyman 2018, 34.)

Esimerkkejä erilaisista IT:hen liittyvistä riskeistä ovat Kailan ja Nymanin (2018, 35) mukaan:

1) Tili on vaarantunut: tärkeät käyttäjätunnukset joutuvat vääriin käsiin esim. tietojenkalastelun vuoksi.

2) Palvelu ei ole käytettävissä: esim. pääsy yrityksen CRM-järjestelmään on estynyt.

3) Tietoja menetetään: keskeisiä tietoja häviää satunnaisesti, joko puutteellisen ylläpidon tai pahantahtoisen tarkoituksen takia.

4) Järjestelmä on saastunut viruksista tai muista haittaohjelmista.

Toisessa vaiheessa on Kailan ja Nymanin (2018, 35–36) mukaan tärkeää suojata tilit, kriittiset järjestelmät ja pilvet sekä data. Suojaamisen tavoitteena on vähentää riskejä. Edellä mainitun CIA-mallin lisäksi riskienhallinnassa hyödynnetään ns. kontrollikeinoja, jotka voidaan jakaa kolmeen tyyppiin: ennaltaehkäisevät, havaitsevat ja korjaavat. Ennaltaehkäisevät kontrollit pyrkivät estämään ei-toivottuja tapahtumia, havaitsevat kontrollit tunnistavat haitalliset tapahtumat niiden sattuessa, ja korjaavat kontrollit pyrkivät lievittämään vahinkoa tapahtuman jälkeen. Näiden kontrollikeinojen käytössä on usein löydettävä tasapaino turvallisuuden ja käytettävyyden välillä; esim. monivaiheinen tunnistautuminen lisää turvallisuutta, mutta tekee kirjautumisesta aavistuksen hitaampaa.

Kaila ja Nyman (2018, 36–38) ehdottavat, että yrityksessä käytetään seuraavia kontrollikeinoja suojaamiseen:

Tilit on hyvä suojata vahvoilla salasanoilla. Lisäksi on hyvä oppia tunnistamaan kalasteluyritykset ja ottaa käyttöön monivaiheinen tunnistautuminen. Nämä ovat keskeisiä toimenpiteitä, joilla varmistetaan tilien turvallisuus. Jos hyökkääjä pääsee käsiksi käyttäjätiliin, erityisesti hallintaoikeuksia sisältävään tiliin, voi organisaatio altistua merkittäville riskeille.

Salasanojen vahvuutta on perinteisesti parannettu käyttämällä erikoismerkkejä, numeroita sekä sekoittamalla isoja ja pieniä kirjaimia, mutta salasanan pituus on erittäin tärkeää. Vähintään 12-merkkinen, helposti muistettava, mutta vaikeasti arvatta ns. salalause on suositeltavampi vaihtoehto monimutkaisen ja lyhyen salasanan sijaan. Saman salasanan käyttö eri tileillä altistaa myös suurille riskeille, jos jokin tili joutuu tietomurron kohteeksi. Tästä syystä salasanojen tulisi olla yksilöllisiä.

On tärkeää, että henkilöstö osaa tunnistaa tietojenkalasteluyritykset. Tietojenkalastelun tavoitteena on harhauttaa käyttäjä paljastamaan kirjautumistietonsa tai muuta arkaluontoista tietoa. Tällaiset sivustot voivat näyttää uskottavilta, mutta niiden tarkoitus on houkutella käyttäjiä antamaan rikollisille kirjautumistietoja, maksukorttitietoja tai muuta arvokasta tietoa.

Monivaiheinen tunnistautuminen (2FA – Two-Factor Authentication) on tehokas keino tilien suojaamiseen, jossa pelkän salasanan lisäksi tarvitaan toinen todennuskeino, kuten esim. puhelimeen lähetettävä koodi. Vaikka rikollinen pääsisi käsiksi salasanaan, pysyy tili turvassa, jos hänellä ei ole pääsyä toiseen tunnistautumistapaan.

On tärkeää suojata kriittiset järjestelmät sekä erottaa järjestelmät, data ja palvelut toisistaan. Esimerkiksi tietokone, tiedostot ja asiakastilausten hallintajärjestelmä ovat itsenäisiä kokonaisuuksia. Tietokone itsessään ei välttämättä ole kriittinen, mutta jos tärkeä data on tallennettu vain yhdelle laitteelle, syntyy tietoturvariski. Useimmille yrityksille keskeisiä IT-järjestelmiä ovat laskutus-, myynti-, logistiikka-

ja asiakashallintajärjestelmät sekä niihin liittyvä data. On myös tärkeää huomioida mahdolliset vanhentuneet (ns. legacy) järjestelmät ja se, jos vain harva työntekijä tuntee niiden toiminnan, mikä voi vaarantaa toiminnan jatkuvuuden.

Pilvipalvelut on syytä suojata huolellisesti, sillä yritykset käyttävät yhä enemmän pilvipalveluja tietojen tallennukseen. On tärkeää ymmärtää, kuinka palveluntarjoajat suojaavat tietoja ja mitä tapahtuu, jos tietoja menetetään. Palvelun saatavuuden tarkistaminen on myös oleellista, eli kuinka luotettavasti palvelu on käytettävissä. Saatavuus ilmoitetaan usein prosentteina; esim. 99 % vastaa noin 3,65 päivän käyttökatkoa vuodessa.

Tärkeät tiedot on syytä suojata ja lisäksi on hyvä tunnistaa, mitkä tiedot ovat tärkeitä ja suojelun arvoisia. Olipa tiedot tallennettu pilvipalveluun tai omalle kiintolevylle, varmuuskopioiden tärkeyttä ei voi liioitella. On myös tärkeää testata varmuuskopioiden toimivuus säännöllisesti, ja tietoturvaa voidaan vahvistaa salaamalla tiedot ennen niiden tallentamista pilveen.

2.7 Muut suojauskeinot

Edellä mainittujen kontrollikeinojen lisäksi yrityksen on hyvä huomioida myös virustorjunta yrityksen laitteissa. Varovaisuus ja ajan tasalla pysyminen ei F-Securen (2024a) mukaan aina riitä, vaan siksi virustentorjuntaohjelmistoa kannattaa käyttää suojaamaan laitteet. Virustentorjunta ohjelma tarjoaa suojaa myös kiristysohjelmia, troijalaisia ja mainosohjelmia sekä tietojenkalasteluhyökkäyksiä vastaan. Antivirusohjelmisto valvoo reaaliaikaisesti laitetta epäilyttävän ja haitallisen toiminnan varalta, ja jos se havaitsee jotain, se ilmoittaa käyttäjälle ja pysäyttää uhkan ennen kuin se ehtii saamaan vahinkoa aikaiseksi.

Ilmainen virustorjuntaohjelma voi suojata laitetta perustasoisesti sekä joitain yksinkertaisia toimintoja mahdollisesti haitallisten ohjelmien tunnistamiseen. Maksullisen virustorjunnan etuna on luotettavuus. Kun ohjelmisto on ostettu tunnetulta palveluntarjoajalta, voit tietää saavasi turvallisen tuotteen. Etuna maksullisessa ohjelmistossa on myös se, että se pysyy ajan tasalla viimeisimpien päivitysten avulla, kun taas yksinkertaisemmat ohjelmat saattavat jäädä jälkeen uusimmista haittaohjelmista ja haavoittuvuuksista. (F-Secure 2024a.)

Palomuuri on työkalu, joka valvoo ja säätelee laitteiden välistä tietoliikennettä. Se toimii suodattimena, joka tarkistaa, millaista liikennettä verkkoon pääsee tai sieltä lähtee, ja estää haitallisen sisällön pääsyn laitteisiin. Palomuurin avulla pyritään estämään esim. virusten, haittaohjelmien tai hakkereiden pääsy verkkoon ja sen kautta laitteisiin. Palomuurin päätavoite on suojata vaaralliset hyökkäykset avoimesta internet-verkosta paikalliseen lähiverkkoon. Palomuurin tehtävänä on myös kontrolloida internetistä lähiverkkoon tulevaa liikennettä sallien sen vain määrättyjen porttien kautta. Se toimii suodattimena, joka joko sallii liikenteen kulkea sen läpi tai estää sen. Se noudattaa ennalta määriteltyjä sääntöjä ja torjuu tietyt yhteydenottopyynnöt, jotka eivät täytä asetettuja ehtoja. Joskus palomuuri saattaa pyytää käyttäjää vahvistamaan, voiko tietyn pyynnön päästää läpi. (NordVPN 2024a.)

Langaton lähiverkko, eli WLAN (Wireless Local Area Network), tai kuten puhekielessä usein puhutaan Wi-Fi, on suosittu ja halpa tapa päästä tietokoneella tai puhelimella internetiin. Yksinkertaisimmillaan WLAN-tukiasema tarvitsee vain kytkeä sähkövirtaan ja yhdistää internetiin langallisen lähiverkon avulla. Langattoman lähiverkon käyttäminen kuulostaa helpolta, ei se välttämättä ole turvallista, ellei tukiaseman asetuksissa ole estetty siihen pääsyä ulkopuolisilta käyttäjiltä. Jos käyttäjän tunnistautuminen verkkoon on toteutettu huonosti, voi hakkeri päästä sitä kautta lähiverkkoon. (Viestintävirasto 2014.)

Kotona työskennellessä on syytä kiinnittää huomiota kotiverkon ja reitittimen tietoturvaan. Traficom (2024a) kertoo, että modeemi tai reititin – jotka voivat usein olla sama laite tai toimia erillään – on portti kotiverkkoon ja siksi niistä kannattaa ymmärtää perusasiat tärkeiden tietojen suojaamiseksi. Seuraavat tietoturva-asetukset suositellaan tarkistettavan:

1) Verkkokaapelit on kytketty oikein.

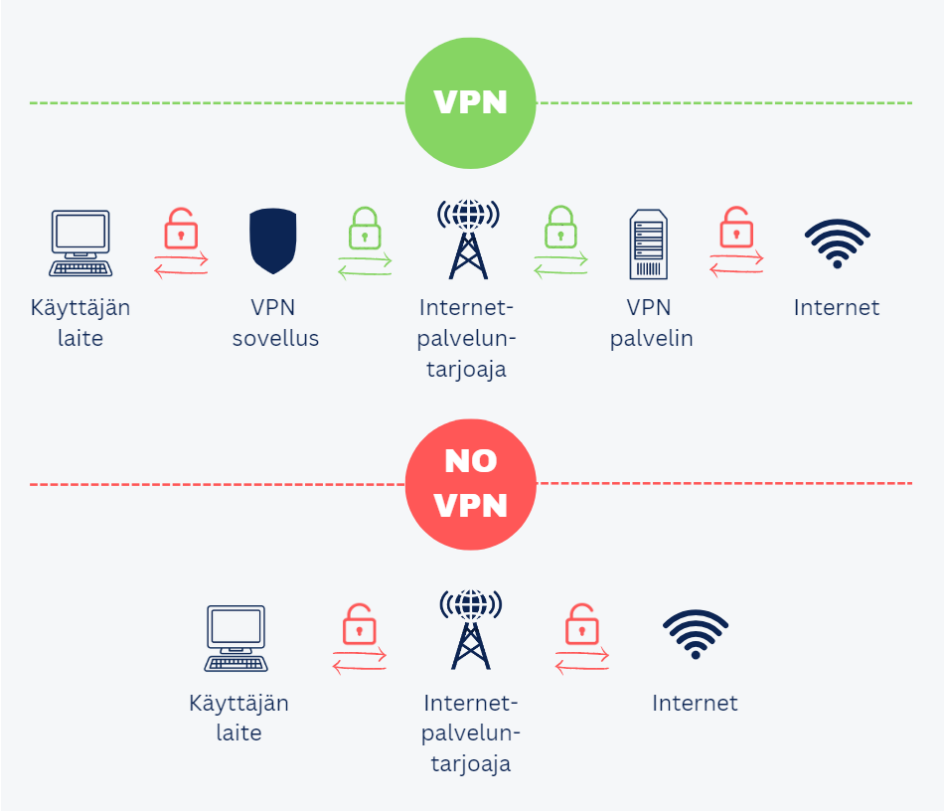
2) Reitittimestä on poistettu etähallinnan mahdollisuus oman verkon ulkopuolelta tai sen turvallisuuden varmistaminen.

3) Oletussalasana on vaihdettu.

Reititintä hallitaan hallintaportaalin kautta, johon pääsee kirjoittamalla tietokoneen selaimen osoiteriville IP-osoitteen (Internet Protocol) ja kirjautumalla sisään ADMIN-tunnuksilla, joka on merkitty reitittimeen. Kirjautuminen saattaa vaatia, että tietokone on kytkettynä juuri tämän reitittimen verkkoon. IP-osoitteen löytää esim. laitteen ohjekirjasta tai laitteessa olevasta tarrasta.

4) Laite on päivitetty ja siihen on asennettu viimeisimmät päivitykset.

Julkisen Wi-Fi-verkon käyttämiseen liittyy suuria tietoturvariskejä. Laitteet ovat erityisen haavoittuvaisia, kun ne yhdistetään julkiseen Wi-Fi-verkkoon, kuten kahvilassa tai lentokentällä. Tällöin ns. hotspotin omistaja ja muut verkon käyttäjät voivat nähdä käyttämäsi sivustot ja salaamattomat tiedot. Vaikka julkisen Wi-Fi-verkko olisi suojattu salasanalla, se ei ole turvallinen, jos salasana on vapaasti saatavilla. Lisäksi kaikki uhat eivät edes vaadi hakkerin liittymistä verkkoon, vaan he voivat luoda aidon näköisiä, turvalliselta kuulostavia Wi-Fi-verkkoja, joihin liittyminen altistaa laitteen ja tiedot varkauksille. Siitä syystä on aina tärkeää varmistua siitä, että käytetty verkko on luotettava. Julkisissa Wi-Fi-verkoissa kannattaa välttää arkaluonteisia toimia ja käyttää vain https-sivustoja, jotta tiedot ovat suojattuja. Laitteesta kannattaa poistaa sen automaattinen yhdistäminen Wi-Fi-verkkoihin, kun sitä ei tarvita. VPN-yhteyden käyttäminen on järkevää, mikäli halutaan suojata yhteys täysin julkisessa Wi-Fi-verkossa. (F-Secure 2024c.) VPN-yhteyden toimintaperiaate esitellään kuviossa 6.



Kuvio 6. VPN-yhteyden toimintaperiaate (mukaillen dela Luna 2024)

VPN-yhteyden (Virtual Private Network) käyttäminen mahdollistaa arkaluonteisten tietojen lähettämisen turvattomissa verkoissa. VPN-yhteys, jotka kutsutaan usein tunneliksi, on salattu yhteys kahden pisteen välillä. Yhteys muodostetaan yleensä VPN-asiakassovelluksella, joka yhdistyy VPN-keskittimeen internetin kautta. Kun yhteys on luotu, kaikki tietoliikenne siirtyy VPN-tunnelin kautta. (Andress 2014, 159.)

2.8 Jatkuvuussuunnitelma, seuranta ja arviointi

Vaikka riskien vähentämiseksi olisi tehty paljon erilaisia toimenpiteitä, on silti tärkeää varautua etukäteen laatimalla jatkuvuussuunnitelman tilanteita varten, joissa jokin menee pieleen kaikista varotoimista huolimatta. Tämä vaihe liittyy omaisuuden suojaamiseen, mutta painottaa toimia siinä tapauksessa, että suojaustoimet eivät ole riittäviä. Jatkuvuussuunnitelman voi toteuttaa eri tavoin, mutta perusajatuksena on turvata liiketoiminnan jatkuvuus erilaisten häiriöiden tai onnettomuuksien kohdatessa. (Kaila & Nyman 2018, 38–39.)

Jos jokin kriittinen toiminto keskeytyy, varasuunnitelma auttaa takaamaan toiminnan jatkumisen. Palautumissuunnitelma voi esim. kuvata, miten edetään, jos tietoja menetetään tai kriittinen palvelu on pois käytöstä. Suunnitelma voi olla yleisluontoinen ja sen olisi hyvä sisältää tarkat palvelut ja vastuuhenkilöiden nimet. Jos jokin kriittinen toiminta esimerkiksi häiriintyy, käytössä olisi varasuunnitelma tämän toiminnon takaamiseksi. Palautussuunnitelma voi kuvata esimerkiksi, miten toimitaan, jos dataa katoaa tai kriittinen palvelu on pois käytöstä. (Kaila & Nyman 2018, 38–39.)

Vaikka käytössä olisi parhaat mahdolliset suunnitelmat ja työkalut järjestelmien suojaamiseen, on tärkeää jatkuvasti seurata ja arvioida tilannetta. Pienyrityksille seurannan toteuttaminen voi olla haastavaa, mutta esim. havaittujen haittaohjelmien määrä ja tietoturvapoikkeamat kannattaa kirjata ylös, jotta pysytään perillä tilanteesta. Näiden kerättyjen tietojen perusteella voidaan tehdä tarvittavia päätöksiä ja ryhtyä toimenpiteisiin tilanteen hallitsemiseksi. Seurantatiedot voivat auttaa tunnistamaan kehityssuuntia, jotka voivat viitata uhkiin tai suojausten heikkouksiin. (Kaila & Nyman 2018, 39.)

Kailan ja Nymanin (2018, 39) mukaan on monia muitakin asioita, joita olisi tarpeen seurata ja tarkastella, mutta niiden toteuttaminen voi vaatia enemmän tietoturvaosaamista kuin yrityksellä on käytössään. Mikäli yritykseltä puuttuu omaa asiantuntemusta, heidän mukaansa on suositeltavaa kutsua ulkopuolinen asiantuntija arvioimaan tietoturvan tilaa. Asiantuntija voi opastaa esim. järjestelmien suojaamisessa.

3 MENETELMÄLLINEN TOTEUTUS

3.1 Opinnäytetyön lähestymistapa

Tässä opinnäytetyössä keskitytään Yritys X:n tietoturvan nykytilan kartoittamiseen ja sen pohjalta kehityssuunnitelman laatimiseen. Työn tarkoituksena on selvittää Yritys X:n tietoturvakäytännöt hyödyntäen kyselytutkimusta. Saatujen vastausten perusteella laaditaan konkreettinen kehityssuunnitelma, jolla pyritään parantamaan yrityksen tietoturvaa vastaamaan paremmin sen tarpeita ja riskejä. Kehityssuunnitelmasta tehdään realistinen ja sellainen, että se soveltuu yrityksen resursseihin ja toimintaympäristöön.

Kyselytutkimuksella pyritään myös selvittämään henkilöiden suhtautumista tietoturvaa kohtaan. Tavoitteena on saada käsitys siitä, miten tietoturvaan ylipäätään suhtaudutaan sekä minkä tasoista tietämystä työntekijöillä on tietoturvasta.

3.2 Tutkimusmenetelmä

Tutkimusmenetelmänä käytetään laadullista eli kvantitatiivista tutkimusta, joka käsittelee merkityksiä (Hirsjärvi, Remes & Sajavaara 2007, 133). Laadullisen tutkimuksen prosessi sisältää yleensä aiheen valinnan, tutkimuksen tavoitteiden määrittämisen, tutkimuskysymysten laatimisen, rajauksien esittelyn, teoriapohjan rakentamisen kirjallisuuden avulla, tutkimusmenetelmien ja aineiston valinnan, aineiston keräämisen, analysoinnin ja tulkinnan sekä tulosten raportoinnin. (Juuti & Puusa 2020, luku ”Johdanto”.)

Laadullista tutkimusmenetelmää käytetään, kun halutaan mm. ymmärtää tutkimuskohteena olevien henkilöiden ajatuksia (Juuti & Puusa 2020, luku ”Johdanto”). Laadullisessa tutkimuksessa keskitytään ihmisten omien kokemusten ja näkemysten tutkimiseen (Juuti & Puusa 2020, luku 2 ”Laadullisen tutkimuksen ominaispiirteet”). Vaikka osa tutkimuksen kysymyksistä on monivalintakysymyksiä, tutkimuksen tavoitteena ei ole tuottaa määrällistä eli numeerista tietoa vastauksista. Sen sijaan tutkimus pyrkii valottamaan vastaajien toimintatapoja ja käyttäytymistä.

Tutkimuksessa käytetään osittain myös määrällistä analyysiä, eli joitakin laadullisia vastauksia muutetaan numeeriseen muotoon, jotta niistä voidaan tehdä parempia päätelmiä, eivätkä tulokset perustu vain tuntumaan (Saaranen-Kauppinen & Puusniekka 2006). Tavoitteena on tunnistaa vastaajien käyttäytymiseen ja tietoturvatietoisuuteen vaikuttavat tekijät sekä löytää kehityskohteita, joiden avulla yrityksen tietoturvaa voidaan parantaa ja vahvistaa tulevaisuudessa.

3.3 Kyselytutkimuksen toteuttaminen

Tutkimus toteutetaan anonyymin sähköisen kyselylomakkeen avulla, joka luodaan käyttäen Webpropol-sovellusta ja lähetetään koko yrityksen henkilöstölle, eli kolmelle työntekijälle. Kyseisen tiedonkeruumenetelmän etuna on, että lomake voidaan täyttää silloin kuin se vastaajalle itselleen sopii, eikä siihen tarvitse varata tiettyä aikaa hektisen työn keskellä. Verkkokyselyn etuna on myös pienempi työvaiheiden määrä, koska vastaukset saadaan valmiiksi sähköisessä muodossa, eikä aikaa kulu niiden litteroimiseen (Valli & Perkkilä 2018, 118).

Kyselytutkimus on hyvä tapa tiedon keräämiseen ja tarkasteluun, kun halutaan tutkia mm. ihmisten toimintaa ja asenteita (Vehkalahti 2014, 11). Webpropolissa kysymykset esitetään yhdellä avoimella lomakkeella, jolloin useampi kysymys on nähtävissä samanaikaisesti. Tämän ansiosta vastaaja voi vertailla vastauksiaan helposti, mikä mahdollistaa sen, että yksi kysymys voi vaikuttaa seuraavaan. Tämä lähestymistapa parantaa vastauksien johdonmukaisuutta saman aihepiirin sisällä ja auttaa vastaajaa hahmottamaan aihekokonaisuuden paremmin. (Valli & Perkkilä 2018, 122–123.)

Kysymysten laadinta edellyttää huolellista suunnittelua, sillä ne ovat keskeinen tekijä tutkimuksen onnistumisessa. On tärkeää varmistaa, että kysymykset muotoillaan niin, että vastaajat tulkitsevat ne samalla tavalla kuin tutkija. Kysymysten tulee olla mahdollisimman selkeitä, jotta vältetään virheet ja väärinkäsitykset. Lisäksi kysymyksissä on vältettävä johdattelevuutta, jotta vastaukset olisivat mahdollisimman totuudenmukaisia. (Valli 2018, 93.)

Liitteessä 1 on esitelty tutkimuksen kysymykset, jotka sisältävät monivalintakysymyksiä ja avoimia kysymyksiä. Vastaajat saavat kirjoittaa avoimiin kysymyksiin

omia näkemyksiään ja toimintatapojaan. Lomakkeella on myös muutamia kysymyksiä, joiden avulla pyritään selvittämään henkilöiden suhtautumista tietoturvaan.

Kyselytutkimuksen vastausten analysointiin käytettiin mm. koodaamista ja teemoittelua. Koodaamisessa on kyse aineiston ryhmittelystä, luokittelusta tai merkitsemisestä. Teemoittelussa taas tutkimusaineistosta hahmotetaan keskeisiä aihekokonaisuuksia (Hakala 2024, 102–108). Analyysiprosessi eteni niin, että koodatut vastaukset ryhmiteltiin laajemmiksi teemoiksi, jonka jälkeen pystyttiin ymmärtämään paremmin vastauksista esiin nousseita merkityksiä. Esimerkiksi kysymyksen ”Onko yrityksessä olemassa selkeät tietoturvakäytännöt- tai ohjeet?” vastaus ”En tiedä”, merkittiin koodilla Tietoturvan epäselvyys, jonka jälkeen se ryhmiteltiin teemaan ”Tietoturvavastuiden ja ohjeiden epäselvyys”.

3.4 Opinnäytetytön eteneminen vaiheittain

Opinnäytetyö aloitettiin suunnittelulla elokuussa 2024, joka loi perustan koko prosessille. Työn aihe oli melko helppo päättää, sillä tietoturva on kiinnostava aihe ja arvelin siitä löytyvän materiaalia helposti. Lisäksi halusin syventää osaamistani, josta on varmasti hyötyä nykyisessä työssäni. Ensimmäisenä laadin opinnäytetyösuunnitelman, jossa määriteltiin aiheen lisäksi tutkimuskysymykset ja tutkimusmenetelmä. Samalla perehdyin tietoperustaan ja etsin sopivia lähteitä käytettäväksi. Materiaalia löytyi helposti ja todella paljon, ja välillä oli vaikea päättää mitä kaikkea työssä haluaa hyödyntää ja tuoda esille. Toimeksiantajayritys oli valmiina jo suunnitteluvaiheessa ja ennen varsinaista tutkimuksen aloitusta solmittiin opinnäytetyösopimus.

Toteutusvaihe alkoi lokakuussa 2024 syventymällä tietoperustaan ja opinnäytetyöraportin kirjoittamisella. Raportin kirjoittamisen aluksi laadin alustavan sisällysluettelon, joka helpotti työn etenemistä ja piti sen johdonmukaisena.

Yritys X:n tietoturvan nykytilannetta lähdin selvittämään kyselytutkimuksen avulla. Ennen lomakkeen lähettämistä mietin huolellisesti kyselyn kysymykset, jotta saisin mahdollisimman yksityiskohtaisesti selville käytännöt ja toimintatavat sekä suhtautumisen tietoturvaan. Tässä vaiheessa etsin tietoa sopivasta alus-

tasta lomaketta varten ja päädyin melko pian Webpropoliin, koska se tuntui helpolta käyttää. Vastaukset kyselyyn saatiin alle viikon kuluessa. Tämän jälkeen lähdin kuvaamaan yrityksen tietoturvan nykytilaa.

Kyselyvastausten pohjalta tehtiin johtopäätökset ja esitettiin konkreettisia suosituksia Yritys X:n tietoturvan parantamiseksi. Lisäksi tässä vaiheessa aloitin tuotoksen tekemisen ja loin kehityssuunnitelman, joka sisältää käytännön toimenpiteitä tietoturvan parantamiseksi.

3.5 Eettiset lähtökohdat ja luotettavuuden tarkastelu

3.5.1 Opinnäytetyön eettisyys

Opinnäytetyön eettisyys on keskeinen osa opinnäytetyöprosessia (Ammattikorkeakoulujen rehtorineuvosto Arene ry 2020, 14). Kaikkea kerättyä aineistoa, kuten kyselyvastauksia käsitellään luottamuksellisesti. Henkilöiden anonymiteetti varmistetaan, jotta yksittäisiä vastaajia tai heidän antamiaan tietoja ei voida tunnistaa tutkimuksen tuloksista. Nämä edellä mainitut asiat täytyy huomioida mm. kyselylomaketta suunnitellessa. Koska opinnäytetyö käsittelee tietoturvaa yrityksessä, on tärkeää ottaa huomioon toimeksiantajan anonymiteetti ja se, ettei opinnäytetyöraportissa paljasteta sellaisia asioita yrityksestä, joista sen voisi helposti tunnistaa. Yritys X:lle ilmoitetaan, että opinnäytetyö on julkinen asiakirja, mutta raportointi toteutetaan siten, ettei sitä voida tunnistaa raportista.

Ennen tutkimukseen osallistumista kaikille osallistujille on tärkeää tiedottaa tutkimuksen tarkoituksesta, tavoitteista ja siitä miten heidän antamiaan tietoja käytetään. Henkilöstölle ilmoitetaan myös, että tutkimukseen osallistuminen on täysin vapaaehtoista. Tutkimuksen toteuttamisessa noudatetaan rehellisyyttä ja avoimuutta; saatuja tuloksia ei manipuloida tai muokata harhaanjohtavasti, vaan ne esitetään totuudenmukaisesti ja objektiivisesti. Tutkimuksesta saatua aineistoa säilytetään turvallisesti ja pääsyä siihen rajoitetaan vain tutkijalle. Aineisto hävitetään asianmukaisesti tutkimuksen valmistuttua.

Opinnäytetyöprosessin aluksi on huolehdittu opinnäytetyösopimuksen tekemisestä. Aineistojen säilyttämisestä ja omistajuudesta on myös sovittu kaikkien osapuolten kanssa. Eettisten ohjeiden mukaan opinnäytetyö on myös tarkastettu

plagiaatintunnistusjärjestelmällä. (Ammattikorkeakoulujen rehtorineuvosto Arene ry 2020, 14.)

3.5.2 Opinnäytetyön luotettavuuteen vaikuttavat tekijät

Opinnäytetyössä käytettävä tieto kerätään tarkoituksenmukaisilla menetelmillä, jotka tarjoavat tarkkaa ja luotettavaa tietoa tutkittavasta aiheesta. Opinnäytetyön luotettavuuteen vaikuttavat merkittävästi sekä tutkimusaineiston määrä että sen laatu. Tutkimusmenetelmän huolellinen valinta ja perustelu ovat keskeisiä luotettavuuden kannalta. Kyselylomake, jonka kysymykset on esitetty liitteessä 1, on valittu aineistonhankintamenetelmäksi, koska se sopi aikataulullisesti parhaiten tutkimusongelman ratkaisemiseen. Kyselylomakkeen kysymykset täytyy muotoilla selkeästi ja ilman johdattelevuutta, jotta vastaajat ymmärtävät ne samalla tavalla. Luotettavuuden arvioiminen voi kuitenkin olla haastavaa, jos kaikki suunnitellut henkilöt eivät osallistu kyselyyn. Kyselyn tuloksia analysoitaessa niitä täytyy käsitellä ilman ennakko-oletuksia tai omia mielipiteitä. Tutkimustulokset perustuvat puhtaasti kerättyihin tietoihin, eikä tutkijan henkilökohtaisiin näkemyksiin. Tavoitteena on tarjota luotettava ja rehellinen kuvaus tutkimuksessa saaduista havainnoista.

Laadullisen tutkimuksen vaiheiden, menetelmien ja tulosten tarkka raportointi on tärkeää, jotta tutkimusprosessi on läpinäkyvä. Raportointi varmistaa, että lukijat ymmärtävät tutkimuksen kulun ja voivat arvioida sen luotettavuutta. (Hirsjärvi, Remes & Sajavaara 2007, 227.)

4 CASE-YRITYKSEN TIETOTURVAN NYKYTILA

4.1 Yleiset toimintatavat

Koko yritys X:n henkilöstö vastasi kyselyyn ja kun kysyttiin, onko yrityksellä käytössään omat vai yrityksen omistamat laitteet, saatiin vastaus, että koko henkilöstöllä on käytössään yritykset omistamat puhelimet, mutta yksi työntekijä ilmoittaa käyttävänsä omaa tietokonetta työtehtävien hoitoon. Kahdella muulla on vastausten perusteella yrityksen omistama tietokone käytössään.

Kun kysyttiin etätyöskentelystä, kävi ilmi, että koko henkilöstö hyödyntää tätä mahdollisuutta, koska vain yksi työntekijä työskentelee myös toimistolla etätyön lisäksi. Etätyöskentelyä suositaan, koska henkilöstö asuu kaukana toisistaan. Henkilöstö kertoo etätyön olevan kotona työskentelyä, eivätkä siten työskentele julkisissa tiloissa, kuten esim. kahviloissa. Kun kysyttiin VPN:n käytöstä, selvisi, että etätyötä tehdessään henkilöstö käyttää omia kotiverkkojaan, eikä käytössä ole VPN-yhteyttä. Etätyö on mahdollista myös sikäli, että Yritys X:ssä käytetään pilvipohjaisia sovelluksia, kuten CRM-järjestelmää ja Fivaldi-laskutusohjelmaa, joten niihin pääsee käsiksi mistä tahansa internet-yhteyden avulla.

Kysyttäessä julkisen Wi-Fi-verkon käytöstä, saatiin vastaus, että sitä käyttää vain yksi henkilöstön jäsen hyvin harvoin, muut kaksi eivät koskaan. Julkisen Wi-Fi-verkon käytön vähäisyys on hyvä, koska niissä on omat riskinsä, kuten F-Secure (2024c) kertoo; laitteet ovat haavoittuvaisia, koska muut verkon käyttäjät voivat nähdä käyttämäsi sivustot ja salaamattomat tiedot. Henkilö, joka käyttää hyvin harvoin julkista WiFi-verkkoa, ilmoittaa ettei käytä silloin VPN-yhteyttä. VPN-yhteys toisi julkisissa verkoissa turvaa, koska se salaa yhteyden (Andress 2014, 159), joten sitä kannattaisi ehdottomasti käyttää.

Pientä epäselvyyttä havaittiin tietoturvakäytäntöjen ja -ohjeiden suhteen. Kun kysyttiin, onko Yritys X:llä olemassa selkeää tietoturvaohjetta- tai käytäntöä, kaksi vastasi ”en osaa sanoa” ja yksi totesi suoraan, ettei tietoturvaohjeita ole. Tämä viittaa siihen, että työntekijöillä ei ole yhtenäistä käsitystä siitä, millaisia tietoturvakäytäntöjä heidän tulisi noudattaa tai onko sellaisia edes olemassa.

Vastausten mukaan yrityksen henkilöstö tunnistaa tietoturvauhkia, kuten tietojenkalastelun (phishing) tai haittaohjelmat, kohtuullisen hyvin, mikä auttaa Kailan ja Nymanin (2018, 36) mukaan suojaamaan mm. tilejä. Kyselyn perusteella yksi vastaajista tuntee nämä uhkat jonkin verran, mutta hän ei ymmärrä niiden tarkempaa toimintatapaa. Kaksi muuta vastaajaa arvioivat tuntevansa nämä uhkat paremmin, ja toinen heistä kuvaa osaamisensa olevan erittäin hyvää.

4.2 Laitteiden tietoturva

Tutkimuksessa selvisi, että työssä käytettävien laitteiden, kuten puhelimien ja tietokoneiden tietoturvavastuu näyttää olevan jossain määrin epäselvää henkilöstölle. Kun kysyttiin kuka vastaa laitteiden tietoturvasta, kävi ilmi, että kaksi työntekijää kokee vastaavansa siitä itse, kun taas yksi vastaaja katsoo sen olevan Yritys X:n vastuulla. Tämä epäselvyys vastuista voi vaarantaa tietojen luottamuksellisuuden, mikäli tietoja heikon suojauksen vuoksi pääsee vuotamaan ulkopuolisille.

Vastauksien perusteella, niillä vastaajilla, jotka kokevat olevansa itse vastuussa työssä käytettävien laitteidensa tietoturvasta, näyttää olevan perusasiat kunnossa: he ovat asettaneet tietokoneen ja ohjelmistojen päivitykset automaattisiksi, ja lisäksi käyttävät virustentorjuntaohjelmaa ja varmistavat, että palomuuri on päällä. Tämä on hyvä, sillä mm. palomuurin avulla pyritään estämään ulkopuolisten pääsy käytettyyn verkkoon ja sitä kautta laitteeseen (NordVPN 2024a).

Kysyttäessä niiltä työntekijöiltä, jotka kokevat vastaavansa itse laitteidensa tietoturvasta, onko heillä riittävästi tietoa ja taitoa suojata työvälineensä tietoturvariskien varalta, ilmenee hieman epävarmuutta. Toinen vastaajista ei ole varma omasta osaamisestaan, kun taas toinen kokee, että hänen tietoturvaosaamisensa on riittävä, mutta ajattelee kuitenkin, että voisi hyötyä lisätiedosta tai lisäkoulutuksesta. Riskinä henkilöstön tietoturvaosaamisessa on se, ilman esimerkiksi ymmärrystä tietojenkalastelusta, voi vahingossa tulla paljastaneeksi luottamuksellisia tietoja ulkopuolisille. Microsoftin (2024) mukaan paras tapa suojautua tietojenkalastelulta, on oppia tunnistamaan erilaiset viestit. Lisäkoulutuksesta ja lisätiedon hankkimisesta olisi siis ehdottomasti hyötyä.

4.3 Salasanat ja tunnukset

Kysyttäessä salasanojen käytöstä ja niiden hallinnasta sekä luomismenetelmistä, kaikki työntekijät kertoivat käyttävänsä salasanaa kirjautumismenetelmänä laitteisiin, jotka sisältävät tai joilla on pääsy Yritys X:n tietoihin. Yksi työntekijä kertoo hyödyntävänsä salasananhallintaohjelmaa luodakseen vahvoja salasanoja, kun taas kaksi muuta kertovat muodostavansa itse vahvoja salasanoja. Kun kysyttiin salasanojen uudelleenkäytöstä, huomattiin siinä eroja; kaksi työntekijää ilmoittaa käyttävänsä samoja salasanoja eri palveluissa hyvin harvoin, kun taas yksi ei käytä koskaan samaa salasanaa useammassa palvelussa. Samojen salasanojen käyttö eri palveluissa on huono asia, sillä se lisää riskiä, jos jokin tili joutuu tietomurron kohteeksi (Kaila & Nyman 2018, 36). Kun kysyttiin salasanojen vaihtotiheydestä, selvisi, että se on verrattain matala; kaksi työntekijää vaihtaa salasanojaan satunnaisesti, esimerkiksi kerran vuodessa, ja yksi vaihtaa salasanoja vielä harvemmin, vain alle kerran vuodessa.

Kun selvitettiin, missä salasanoja säilytetään, havaittiin erilaisia käytäntöjä; kaikki työntekijät tallentavat salasanojaan selaimeen, ja yksi vastaajista kertoo käyttävänsä lisäksi salasananhallintaohjelmaa. Kun kysyttiin kriittisten järjestelmien, kuten CRM- ja laskutusjärjestelmien tunnuksista, selvisi, että työntekijät käyttävät niissä pääosin omia henkilökohtaisia tunnuksiaan. Yksi vastaaja mainitsee kuitenkin käyttävänsä sekä omia että yhteiskäyttötunnuksia. Yhteyskäyttötunnusten käyttäminen voi olla huono asia, sillä silloin tietojen eheys voi kärsiä, kun ei tiedetä, kuka on mahdollisesti tehnyt muutoksia tietoihin. Tietojen eheys on tarkoitus turvata edellyttämällä, ettei luvattomia muutoksia pystytä tekemään ja ne estetään (Andress 2014, 6).

4.4 Tärkeiden tietojen säilyttäminen ja varmuuskopiointi

Asiakasrekisterin ja tilaustietojen säilyttämisestä kysyttäessä, selvisi, että niitä säilytetään pääasiassa pilvipalveluissa, kuten CRM-järjestelmässä ja Fivaldi-laskutusjärjestelmässä. Yksi vastaaja kertoo kuitenkin olevansa hieman epävarma siitä, missä kaikkialla näitä tietoja säilytetään, mutta totesi kuitenkin, että ne sijaitsevat palveluntarjoajien hallinnassa. Yksi vastaajista mainitsi kuitenkin, että

tietoja säilytetään myös Dropbox-pilvipalvelussa. Kun ei olla varmoja, missä kaikkialla tietoja säilytetään, voi se heikentää tietojen eheyttä, mikäli niitä ei synkronoida tietyin aikavälein. Tietojen eheys voi myös kärsiä, mikäli tietoja säilytetään esim. Dropboxissa, eikä pääsyä sinne ole rajattu vain oikeutetuille henkilöille. Tietoihin käsiksi pääsevien henkilöiden tunnistamista ja todentamisesta pitäisi edellyttää (Järvinen 2022, 13–14), ja sen voisi ratkaista esim. monivaiheisella tunnistautumisella.

Kun selvitettiin, kuka vastaa tärkeiden tietojen varmuuskopioinnista selvisi, että niiden varmuuskopiointi on palveluntarjoajien vastuulla. Yritys X luottaa kyselyn mukaan palveluntarjoajien tietojen saatavuus- ja palautusominaisuuksiin, jos tapahtuisi tietoturvaloukkaus tai muu häiriö. On hyvä, että varmuuskopioita otetaan, eikä niiden tärkeyttä voi liioitella (Kaila & Nyman 2018, 38), mutta omaa varmuuskopiointistrategiaa olisi hyvä miettiä, jotta ei oltaisi riippuvaisia pelkästään palveluntarjoajista, mikäli asiat menevät pieleen.

4.5 Suhtautuminen tietoturvaan

Kun kysyttiin, kuinka tärkeänä henkilöstö kokee tietoturvan osana liiketoimintaa, saatiin selkeä vastaus, että koko henkilöstön mielestä se on erittäin tärkeä osa sitä. Vastauksista ilmeni, että tietoturvasta on keskusteltu jonkin verran; on käyty läpi mitkä tiedot ovat salaista tietoa ja ilmeisesti palveluntarjoaja on kertonut, miten verkkosivuston tietoturvaa ylläpidetään. Yksi henkilö kertoo lisäksi, että laitteissa on Avast-tietoturvaohjelma ja se on toistaiseksi riittänyt.

Suurin osa henkilöstöstä kokee vastauksien perusteella, että tietoturvan parantaminen voisi vaatia enemmän aikaa, resursseja, eikä lisäkoulutus ole pahitteeksi. Tietoturvaan suhtaudutaan kyselyn mukaan positiivisesti, kun kaksi kolmesta kokee sen tarpeellisena osana työtä. Yksi vastaajista ei varsinaisesti vastannut kysymykseen, vaan toteaa Avast-tietoturvaohjelmiston olleen riittävä ja ainoastaan yhden kerran on ollut jotain ongelmaa tietoturvan kanssa.

5 JOHTOPÄÄTÖKSET

5.1 Tietoturvakäytännöt

Tutkimuksessa selvisi, että Yritys X:ssä ei ole laadittu tietoturvaan liittyen käytäntöjä tai ohjetta, joita tulisi noudattaa. Tällainen epäselvyys voi johtaa siihen, etteivät työntekijät tiedä, miten heidän pitäisi toimia esimerkiksi turvatakseen järjestelmiä tai tietoliikennettä. Tämä taas voi johtaa siihen, että tietoturvakäytännöt jäävät toteuttamatta. Epäselvyydet näissä käytännöissä voivat vaarantaa yrityksen tietojen luottamuksellisuuden, jos työntekijät eivät tiedä, miten suojata järjestelmiä tai tietoliikennettä.

Saatujen tulosten mukaan henkilöstö kuitenkin ymmärtää tietoturvan olevan tärkeä osa liiketoimintaa ja omalla toiminnallaan he ovat osanneet ottaa huomioon mm. virustentorjuntaohjelmiston ja palomuurin käytön, vaikkei niistä ole sen tarkemmin kommunikoitu. Kyselyn tulosten mukaan kahden henkilön laitteissa on käytössä palomuuri, käyttöjärjestelmän sekä ohjelmistojen päivitykset on asetettu automaattisiksi, sekä he käyttävät virustentorjuntaohjelmaa. Yksi vastaaja oli kuitenkin epävarma, kenellä on vastuu työnteossa käytettävän laitteen tietoturvasta, joten hänen laitteensa teknisestä suojauksesta ei voida olla varmoja. Tämä asia jäi tutkimuksessa selvittämättä tarkemmin. Ymmärrys tietoturvan tärkeydestä ja esim. palomuurin sekä virustentorjuntaohjelmien käyttö osoittaa kuitenkin, että henkilöstöllä on perusvalmiudet suojata järjestelmien luottamuksellisuutta.

Tulokset osoittavat, että työntekijät käyttävät laitteille kirjautumiseen salasanoja, joten yhdellekään laitteelle ei ole pääsyä ilman kirjautumista. Vahvoja salasanoja käytetään yleisesti eri järjestelmiin, mutta niiden luontimenetelmissä on eroavaisuuksia. Kaksi kolmesta kertoo muodostavansa vahvan salasanan itse, kun kolmas kertoo käyttävänsä salasananhallintaohjelmaa. CIA-mallin näkökulmasta salasanojen käytöllä suojataan tietojen luottamuksellisuutta estämällä luvaton pääsy (Andress 2014, 6). Vahvojen salasanojen käyttö parantaa tietoturvaa, mutta erot salasanojen luontimenetelmissä voivat vaikuttaa luottamuksellisuuteen. Salasanojen laatuun kannattaa kuitenkin kiinnittää huomiota ja mikäli haluaa luoda salasanan itse, on hyvä tehdä siitä mahdollisimman monimutkainen, mieluiten Kailan ja Nymanin (2018, 36) mukaan salalause kuin salasana.

5.2 Keskeisimmät riskit

Tutkimus toi esiin muutamia keskeisiä tietoturvariskejä ja kehityskohteita, jotka on tärkeää huomioida Yritys X:n toiminnan turvallisuuden ja jatkuvuuden kannalta. Näistä merkittävin havainto oli tietoturvakäytäntöjen ja vastuiden epäselvyys. Esimerkiksi työntekijöiden epäselvä ymmärrys siitä, kuka vastaa laitteiden ja järjestelmien tietoturvasta, voi johtaa siihen, että tärkeitä päivityksiä ei toteuteta johdonmukaisesti. Tämä voi lisätä riskiä tietoturvaloukkauksille, kuten haittaohjelmien leviämiselle tai tiedon menetykselle.

Toinen keskeinen riski liittyy salasanojen hallintaan. Vaikka peruskäytännöt ovat tutkimuksen mukaan kohtuullisella tasolla, ovat käytännöt hajanaisia. Tietojen luottamuksellisuus voi vaarantua, mikäli ei käytetä riittävän vahvoja salasanoja tai niitä tallennetaan turvattomiin paikkoihin, kuten selaimeen. Tietojen saatavuus voi kärsiä, mikäli työntekijä unohtaa itse luomansa monimutkaisen salasanan tai niiden tallennus on epäjärjestelmällistä.

Pilvipalvelujen käyttö ja palveluntarjoajien varmuuskopio ja palautuskäytäntöihin luottaminen ovat myös riskejä, jotka vaativat huomiota. Tutkimuksen mukaan kriittisiä tietoja säilytetään useissa eri paikoissa, kuten CRM- ja laskutusjärjestelmissä. Lisäksi yksi henkilö mainitsi tietoja säilytettävän Dropboxissa. Jos työntekijöillä ei ole selkeää kuvaa siitä, missä tietoja säilytetään, voi olla vaikeaa varmistaa, että tiedot on riittävästi suojattu. Esimerkiksi Dropboxin tai muiden pilvipalveluiden käyttö ilman monivaiheista tunnistautumista voi altistaa tiedot luvattomalle pääsylle ja siten vaarantaa tietojen luottamuksellisuuden. Pilvipalveluihin luottaminen voi myös vaarantaa tietojen saatavuuden häiriötilanteissa. Mikäli tietoja katoaa tai niihin ei ole hetkellisesti pääsyä häiriötilanteessa, ja palautusprosessi on hidas, tai tiedot eivät jostain syystä ole lainkaan palautettavissa, se voi lamauttaa yrityksen toiminnan.

Henkilöstön tietoturvaosaaminen voi myös altistaa riskeille. Vaikka työntekijät tunnistavat tutkimuksen mukaan tietoturvan tärkeyden ja ymmärtävät perusuhkia, osa kokee osaamisensa puutteelliseksi ja hyötyisi lisäkoulutuksesta tai lisätiedosta. Riskinä henkilöstön tietoturvaosaamisessa on se, ilman esimerkiksi ym-

märrystä tietojenkalastelusta, voi vahingossa tulla paljastaneeksi luottamuksellisia tietoja ulkopuolisille. Henkilöstön riittämätön osaaminen voi myös heikentää heidän kykyään reagoida tietoturvauhkien aiheuttamiin häiriötilanteisiin.

5.3 Suhtautuminen tietoturvaan

Tutkimuksen mukaan Yritys X:ssä suhtaudutaan tietoturvaan positiivisesti ja henkilöstö pitää sitä tärkeänä osana yrityksen toimintaa. Tämä on hyvä lähtökohta tietoturvan kehittämiselle, sillä asenne ja ymmärrys luovat hyvän pohjan uusien käytäntöjen ja toimintatapojen onnistuneelle käyttöönotolle.

Tutkimusvastauksessa mainittu Avast-tietoturvaohjelmisto on koettu yhden henkilöstön jäsenen toimista riittäväksi, mutta Yritys X:n kannattaa harkita tietoturvastrategian monipuolistamista. Avast-ohjelmisto voi tarjota perussuojan esim. viruksia vastaan, mutta lisäksi on hyvä miettiä varmuuskopiointia, salasanakäytäntöjä, missä salasanoja ja yrityksen tärkeitä tietoja säilytetään, sekä säilytyspaikkojen turvallisuutta. Unohtamatta kuitenkaan omia toimintatapoja, koska ihminen on tietoturvassa usein heikoin lenkki (Caldwell 2016, 8).

6 KEHITYSSUUNNITELMA

6.1 Tietoturvakäytäntöjen ja vastuiden selkiyttäminen

Kehityssuunnitelmaan (liite 2) on kerätty toimenpide-ehdotuksia sekä suosituksia, jotka ovat pitkälti nopeasti toteutettavia, eivätkä vaadi paljoa resursseja. Tärkeimpänä kehotuskohteena näen tietoturvakäytäntöjen ja vastuiden selkiyttämisen, koska tämä on perusta yrityksen tietoturvan tehokkaalle toteuttamiselle.

Tutkimuksessa selvisi, ettei Yritys X:llä ole käytössä selkeää kirjallista ohjetta, tai tietoturva-asioista ei ole keskusteltu kovinkaan syvällisesti. Riskinä on, jos tällaista ohjetta ei ole laadittu, että työntekijät eivät tiedä, mitä käytäntöjä noudattaa, ja se voi johtaa tietoturvatoimien laiminlyöntiin ja sitä kautta nostaa riskiä inhimillisiin virheisiin sekä altistaa mm. tietovuodoille.

Suosituksena on laatia yksinkertainen tietoturvapolitiikka ja dokumentoida se. Dokumentin olisi hyvä sisältää perusohjeet ja vastuut tietoturvaan liittyen. Se voisi sisältää myös esim. myös ohjeet salasanojen hallinnasta, haittaohjelmilta suojautumisesta sekä etätyön tietoturvakäytännöistä. Tällainen dokumentti olisi hyvä antaa myös uudelle työntekijälle, jotta hän tietää heti työsuhteensa alusta lähtien mitä käytäntöjä noudattaa. Selkeät käytännöt ja vastuunjaot auttavat varmistamaan, että kaikki työntekijät ymmärtävät roolinsa tietoturvan ylläpitämisessä.

Kehityssuunnitelman toteuttamisen kannalta kannattaa pohtia olisiko yrityksessä henkilö, kenellä olisi riittävää osaamista tai mielenkiintoa hoitamaan tietoturvan kehittämistoimia, jotka on suunnitelmassa kuvattu, vai onko prosessiin mahdollista ottaa ulkopuolinen asiantuntija. Jos vastuuta ei määritetä selkeästi, on vaarana, ettei mitään tapahdu ja tietoturva-asiat jäävät hoitamatta, tai niiden kehittäminen jää puolitiehen. Mikäli Yritys X:n sisältä vastuutetaan henkilö hoitamaan tehtävää, on tärkeää varmistaa, että henkilö saa riittävän tuen tehtävän hoitamiseen.

6.2 Salasanojen hallinnan ja käytön parantaminen

Tulosten mukaan salasanakäytännöt vaihtelevat; vahvoja salasanoja käytetään, mutta niitä säilytetään mm. selaimessa ja vaihdetaan harvakseltaan. Vahvoja salasanoja kannattaa ehdottomasti käyttää, mutta niiden säilyttämistä selaimessa kannattaa harkita, sillä se altistaa tietovuodoille, mikäli ulkopuolinen pääsee käsiksi selaimen tietoihin. Lisäksi on hyvä huolehtia, ettei samoja salasanoja uudelleen käytettäisi sen helppouden vuoksi, sillä salasanan vuotaminen ulkopuoliselle voi altistaa useamman palvelun tietomurrolle (Kaila & Nyman 2018, 36).

Salasananhallintaohjelmaa suositellaan käytettäväksi sekä salasanojen vaihtotiheyttä on hyvä pohtia, vähintään kriittisten järjestelmien osalta. Monivaiheista tunnistautumista suositellaan otettavaksi käyttöön vähintään kriittisissä sovelluksissa, mikäli se on mahdollista, sillä se suojaa järjestelmää estämällä luvattoman pääsyn, vaikka salasana joutuisi vääriin käsiin (Kaila & Nyman 2018, 36–37).

6.3 Pilvipalveluiden hallinta ja varmuuskopiointi

Tutkimuksessa tuli ilmi, että palveluntarjoajien varmuuskopiointi- ja palautuskäytäntöihin luotetaan asiakasrekisterin ja tilaustietojen turvaamiseksi. Lisäksi henkilöstön keskuudessa oli hieman epäselvää kriittisten tietojen säilytyspaikoissa. Tässä on riskinä se, että jos CRM-järjestelmään on pääsy estetty, ei tietoja pystytä käyttämään ja hyödyntämään ja se voi aiheuttaa toimintakatkoksen.

Suosituksena on, että vaikka palveluntarjoajat huolehtivat tietojen varmuuskopioinnista, voisi olla hyödyllistä harkita omaa varmuuskopiointistrategiaa tärkeimmille tiedoille. Tämä voi parantaa tietojen saatavuutta häiriötilanteissa ja vähentää riippuvuutta ulkoisista toimijoista. Palveluntarjoajilta on hyvä varmistaa heidän varmuuskopiointikäytäntönsä, eli esim. kuinka kauan tietoja säilytetään, ja miten nopeasti tiedot voidaan palauttaa häiriön sattuessa. Kriittisten tietojen sijainnit on tärkeää dokumentoida ja kommunikoida selkeästi henkilöstön kesken, jotta voidaan varmistaa, että ne on riittävällä tavalla suojattu ja pääsy niihin on vain oikeutetuilla henkilöillä.

6.4 Etätyö

Vaikka henkilöstön julkisen Wi-Fi-verkon käyttö on tutkimuksen mukaan vähäistä, lisää sen käyttö ilman VPN-yhteyttä tietovuodon riskiä, koska julkiset verkot ovat vähemmän suojattuja ja siten alttiimpia hyökkäyksille (F-Secure 2024c). Henkilöstöä tulisi ohjeistaa käyttämään VPN-yhteyttä aina, kun yhdistetään julkiseen Wi-Fi-verkkoon, mutta tämä kannattaa ottaa huomioon myös etätyöskentelyssä.

Etätyöskentelyssä myös hyvä tarkistaa kotiverkon asetukset Traficomin (2024a) suosituksen mukaisesti: tarkista verkkokaapelin kytkentä, vaihda reitittimen oletussalasana, poista etähallinnan mahdollisuus ja tarkista laitteen päivitykset. Näillä toimilla voidaan pienentää riskiä, että ulkopuolinen pääsisi käsiksi kotiverkkoon ja siten tärkeisiin tietoihin (Viestintävirasto 2014).

6.5 Tietoturvaosaaminen

Tietoturvauhkista henkilöstöllä on kyselyn mukaan jonkin asteinen perusymmärrys, ja he kokevat sen tärkeänä osana liiketoimintaa, mutta ymmärtääkseen tietoturvauhkia paremmin, lisätiedon hankkiminen aiheesta olisi suositeltavaa. Näin vahvistettaisiin henkilöstön kykyä suojautua mm. tietojenkalastelulta ja haittaohjelmilta.

Netistä löytyy paljon ilmaista materiaalia, jota on mahdollista hyödyntää. Nopealla hakukonehaulla löytyi ilmaisia luentoja ja oppaita, mistä on varmasti apua, mikäli ulkopuolista asiantuntija-apua ei haluta käyttää. Lisäksi toivon, että jokainen henkilöstön jäsen lukee tämän opinnäytetyön, koska se tarjoaa arvokasta tietoa tietoturvasta.

6.6 Jatkuvuussuunnitelma

Viimeisenä suosituksena on laatia jatkuvuus-/palautumissuunnitelma. Vaikka riskien vähentämiseksi olisi tehty paljon erilaisia toimenpiteitä, on kuitenkin tärkeää varautua etukäteen häiriötilanteisiin laatimalla palautumissuunnitelma, jos jokin asia menee pieleen kaikista varotoimista huolimatta. Suunnitelman tarkoitus on turvata liiketoiminnan jatkuvuus häiriöiden sattuessa. (Kaila & Nyman 2018, 38–39.)

Palautumissuunnitelma voi esim. kuvata, miten edetään, jos tietoja menetetään tai kriittinen palvelu on pois käytöstä. Suunnitelma voi olla yleisluontoinen ja sen olisi hyvä sisältää tarkat palvelut ja vastuuhenkilöiden nimet. Jos jokin kriittinen toiminta esimerkiksi häiriintyy, käytössä olisi varasuunnitelma tämän toiminnon takaamiseksi. Palautussuunnitelma voi kuvata esimerkiksi, miten toimitaan, jos dataa katoaa tai kriittinen palvelu on pois käytöstä. (Kaila & Nyman 2018, 38–39.)

7 POHDINTA

7.1 Tulokset

Opinnäytetyössä tarkasteltiin tietoturvaa sekä yleisellä tasolla että Yritys X:n näkökulmasta, keskittyen siihen, mitä kyseisen yrityksen tulisi muuttaa tai parantaa tietoturvan osalta. Tavoitteena oli sähköisen kyselyn perusteella selvittää, minkälaisia tietoturvakäytäntöjä Yritys X:llä on käytössä tällä hetkellä, mitkä ovat keskeisimmät tietoturvariskit Yritys X:ssä ja millaisilla toimenpiteillä ja käytännöillä Yritys X:n tietoturvaa saataisiin parannettua.

Tutkimuksen perusteella saatiin luotettavaa tietoa Yritys X:n tietoturvan nykytilasta, sillä koko henkilöstö vastasi kyselyyn. Tulokset osoittivat, että joitakin käytäntöjä oli jo olemassa, vaikka niistä ei ole keskusteltu sen kummemmin. Tällaisia käytäntöjä ovat muun muassa palomuurin, virustentorjuntaohjelmiston käyttö ja ohjelmistojen sekä käyttöjärjestelmän päivitysten automaattinen asentaminen. Vahvoja salasanoja on käytössä, mutta niiden muodostamiseen käytetään erilaisia menetelmiä.

Tutkimuksen perusteella saatiin selville muutamia keskeisiä riskejä, joista ensimmäisenä esiin nousi epäselvyys laitteiden tietoturvan vastuusta, eli kuka huolehtii niiden tietoturvasta. Lisäksi huomattiin hajanaiset käytännöt salasanojen muodostamisessa ja hallinnassa. Salasanoja muun muassa luodaan itse, jolloin riski, että samaa salasanaa käytetään uudelleen jossain toisessa paikassa kasvaa. Salasanoja myös tallennetaan selaimeen, mikä voi olla riski, mikäli ulkopuolinen pääsee käsiksi selaimen tietoihin. Varmuuskopiointia ei Yritys X:ssä suoriteta tutkimuksen mukaan ollenkaan itse, vaan luotetaan palveluntarjoajien varmuuskopiointi- ja palautuskäytäntöihin. Henkilöstön tietoturvaosaaminen tunnistettiin myös riskinä, sillä vaikka he tutkimuksen mukaan ymmärtävät perusuhkia, osa kokee osaamisensa puutteelliseksi.

Kyselyn vastausten ja riskien tunnistamisen perusteella voitiin lähteä kehittämään tietoturvaa konkreettisilla toimenpiteillä ja suosituksilla. Tuotoksena syntyi kehityssuunnitelma (liite 2), jossa suositellaan laatimaan tietoturvaohje tai -politiikka ja dokumentoimaan se. Tällainen ohje luo perustan tietoturvalliselle toimin-

nalle ja sen avulla työntekijät tietävät millaisia käytäntöjä noudattaa. Salasananhallintaohjelmaa suositellaan otettavaksi käyttöön, sillä se helpottaa vahvojen salasanojen luomista sekä niiden hallintaa. Pilvipalveluiden osalta varmuuskopiointistrategiaa on hyvä pohtia, sillä nyt luotetaan ainoastaan palveluntarjoajien varmuuskopiointikäytäntöihin. Häiriötilanteissa omista varmuuskopioista voisi olla merkittävä apu. Koska henkilöstö työskentelee etänä, on oman kotiverkon turvallisuudesta huolehdittava, jottei ulkopuoliset pääse käsiksi yrityksen tietoihin, ja siksi kehityssuunnitelmassa on kehotus tarkistaa oman Wi-Fi-verkon asetukset. Henkilöstön tietoturvaosaamisesta löytyi parannettavaa, sillä vaikka heillä on tutkimuksen mukaan perusymmärrys tietoturvauhkista ja ymmärtävät sen tärkeänä osana liiketoimintaa, olisi lisätiedon hankkimisesta hyötyä. Lisätiedon avulla henkilöstö osaisi tunnistaa paremmin erilaisia uhkia ja toimia epäilyttävissä tilanteissa oikein. Lisätiedon hankkimiseen suositellaan netissä olevien ilmaisten materiaalien hyödyntämistä, mikäli ei haluta käyttää ulkopuolista apua. Viimeisenä kohtana kehityssuunnitelmassa on laatia jatkuvuussuunnitelma, jonka avulla häiriötilanteissa osataan toimia oikein, jos jokin asia menee pieleen.

7.2 Jatkokehittämisaiheet

Aikataulullisista syistä päädyttiin sähköiseen kyselyyn ja sillä saavutettiin kohtalaisia tuloksia, mutta menetelmä rajasi hieman tutkimuksen laajuutta. Haastattelut olisivat mahdollistaneet tarkempien ja yksityiskohtaisempien tietojen keräämisen.

Työssä olisi voitu hyödyntää riskianalyysiä, mutta aikataulullisista syistä se jäi toteuttamatta. Tutkimuksessa jäi selvittämättä myös sähköpostin sekä yrityksen kotisivujen tietoturva, joita voisi tutkia tarkemmin. Molemmat ovat erittäin tärkeitä työvälineitä yritykselle ja niiden tietoturvaan kannattaisi kiinnittää huomiota enemmän. Sähköpostin osalta voisi selvittää roskapostin ja tietojenkalastelun suodattimia, salausta sekä kaksivaiheisen tunnistautumisen hyödyntämistä. Yrityksen kotisivujen osalta olisi hyödyllistä selvittää, kuinka hyvin niiden alusta ja palvelin on suojattu ja millainen varmuuskopiointikäytäntö niillä on.

Koska tutkimuksen mukaan yrityksessä käytetään myös omia laitteita, lähinnä tietokoneiden osalta, voitaisiin niille kehittää BYOD-politiikka (Bring Your Own

Device), eli määriteltäisiin, miten työntekijöiden omia laitteita voidaan käyttää yrityksen töissä turvallisesti. Lisäksi tutkimuksessa ei selvitetty mitä tapahtuu yrityksestä lähteneen henkilön tunnuksille ja pääsyoikeuksille erilaisiin järjestelmiin.

7.3 Oman oppimisen pohdinta

Onneksi valitsin aiheen, joka oikeasti kiinnosti minua ja, joka tarjosi mahdollisuuden syventää osaamistani. Tämä teki kirjoittamisesta sekä koko prosessista mielekkään ja motivoivan. Suurimpana haasteena koin aiheen rajaamisen ja aikataulun. Tietoturva on laaja aihealue, ja saatavilla on paljon tietoa. Oli haastavaa valita juuri olennaisimmat ja työhön parhaiten sopivat teoriat raporttiin. Aikataulu oli melko tiukka ja olisin kaivannut enemmän aikaa työn huolelliseen suunnitteluun ja toteuttamiseen. Työn edetessä huomasin, kuinka tärkeää huolellinen suunnittelu on, ja siitä syystä muutamia asioita jäi tutkimuksessa selvittämättä.

Koen kuitenkin, että onnistuin tavoitteissani kohtalaisesti. Opin muokkaamaan teoreettista tietoa käytännönläheiseksi ratkaisuiksi, jotka ovat helposti toteutettavissa case-yrityksessä ja opin huomioimaan yrityksen resurssit ja tarpeet, kun suunnittelin tietoturvan kehittämistoimia. Tämä koko prosessi lisäsi varmuutta tietoturvaan liittyvässä osaamisessani ja kyvyssä soveltaa sitä käytännön tilanteissa. Opin miten pienetkin parannukset tietoturvakäytännöissä voivat merkittävästi vähentää riskejä.

Opinnäytetyö ei pelkästään hyödyttänyt minua oppimisprosessina, vaan se toi myös lisäarvoa ammatilliseen osaamiseeni. Voin soveltaa opittuja tietoja nykyisessä työssäni IT-alalla sekä kehittää taitojani uran edetessä.

LÄHTEET

Ammattikorkeakoulujen rehtorineuvosto Arene ry 2020. Ammattikorkeakoulujen opinnäytetöiden eettiset suositukset. Viitattu 28.11.2024 https://www.arene.fi/wp-content/uploads/Raportit/2020/AMMATTIKORKEAKOULUJEN%20OPINN%C3%84YTET%C3%96IDEN%20EETTISET%20SUOSITUKSET%202020.pdf?_t=1578480382

Andress, J. 2014. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. 2nd edition. Oxford, England: Syngress.

Bautomo 2024. Tietoturva (Tietoturvallisuus, Kyberturvallisuus, Tietojen suojelu). Viitattu 5.10.2024 https://bautomo.com/sanastoa/tietoturva/.

Caldwell, T. 2016. Making security awareness training work. Computer fraud & security, 2016(6), 8–14. Viitattu 6.10.2024 https://doi.org/10.1016/S1361-3723(15)30046-4.

Cloudflare 2024. What is a denial-of-service (DoS) attack? Viitattu 20.10.2024 https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/.

dela Luna, C. 2024. How does a VPN Work? A Comprehensive Beginner's Overview. eSecurity Planet 27.8.2024. Viitattu 10.11.2024 https://www.esecurityplanet.com/networks/how-does-a-vpn-work/.

Forculus 2024. Luottamuksellisuus, eheys ja saatavuus tietoturvan johtamisen ja yrityksen liiketoiminnan tukipilareina. Viitattu 26.10.2024 https://forculus.fi/blogi/tietoturva-osana-yrityksen-johtamista/.

F-Secure 2024a. Mikä on antivirus eli virustorjunta? Viitattu 4.11.2024 https://www.f-secure.com/fi/articles/antivirus.

F-Secure 2024b. Mikä on palvelunestohyökkäys (DDoS)? Viitattu 26.10.2024 https://www.f-secure.com/fi/articles/what-is-ddos.

F-Secure 2024c. Onko julkinen Wi-Fi turvallinen? Viitattu 10.11.2024 https://www.f-secure.com/fi/articles/is-public-wi-fi-safe.

Gupta, C. P. & Goyal, K. K. 2020. Cybersecurity: A self-teaching introduction. Dulles, Virginia: Mercury Learning and Information.

Hakala, J. T. 2024. Laadullisen tutkimuksen ABC. Menetelmäopas opinnäytteen tekijälle. Helsinki: Gaudeamus.

Heikkilä, M. 2024. Nordean häiriö ohi – verkkopankissa oli Pohjoismaiden laajuinen palvelunestohyökkäys. YLE 25.10.2024. Viitattu 26.10.2024 https://yle.fi/a/74-20120325.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2007. Tutki ja kirjoita. 13.–14., osin uudistettu painos. Helsinki: Tammi.

IBM 2024. What is malware? Viitattu 2.11.2024 https://www.ibm.com/topics/malware.

Integral 2024. Tietoturvan jatkuva kehittäminen on kriittisen tärkeää yrityksille. 19.8.2024. Viitattu 2.11.2024 https://integral.fi/blogi/tietoturvan-jatkuva-kehittaminen-on-kriittisen-tarkeaa-yrityksille/.

Jurvanen, L. 2023a. Mitä tarkoittaa hallinnollinen tietoturva? Save LAN Oy 11.10.2023. Viitattu 10.11.2024 https://www.savelan.fi/mita-tarkoittaa-hallinnollinen-tietoturva/.

Jurvanen, L. 2023b. Mitä tarkoittaa tekninen tietoturva? Save LAN Oy 29.12.2023. Viitattu 10.11.2024 https://www.savelan.fi/mita-tarkoittaa-tekninen-tietoturva.

Juuti, P. & Puusa, A. 2020. Laadullisen tutkimuksen näkökulmat ja menetelmät. Helsinki: Gaudeamus.

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

Jäärni, C. 2024. Nordea toivoo, että asiakkaiden luottamus säilyy ongelmista huolimatta, mutta Minnamari Dahlberg menetti sen jo. YLE 10.10.2024. Viitattu 26.10.2024 https://yle.fi/a/74-20114346.

Kaila, U. & Nyman, L. 2018. Information Security Best Practices: First Steps for StartUps and SMEs. Technology Innovation Management Review, 8(11) 32–42. Viitattu 20.10.2024 https://doi.org/10.22215/timreview/1198.

Konttoripiste 2024. Mitä tietoturva tarkoittaa ja miksi se on tärkeää? Viitattu 6.10.2024 https://kskp.fi/2024/mita-tietoturva-tarkoittaa-ja-miksi-se-on-tarkeaa/.

Kosinski, M. 2024. What is ransomware? IBM 4.6.2024. Viitattu 2.11.2024 https://www.ibm.com/topics/ransomware.

Microsoft 2024. Tietojen kalastelulta suojautuminen. Viitattu 2.11.2024 https://support.microsoft.com/fi-fi/windows/tietojen-kalastelulta-suojautuminen-0c7ea947-ba98-3bd9-7184-430e1f860a44.

NordVPN 2024a. Mikä on palomuuri? Viitattu 4.11.2024 https://nordvpn.com/fi/blog/palomuuri/.

NordVPN 2024b. Mitä on haittaohjelma, eli malware? Viitattu 2.11.2024 https://nordvpn.com/fi/cybersecurity/what-is-malware/.

Palvelunestohyökkäysten ehkäisy ja torjunta 2016. Viestintäviraston ohje 3/2016. Viitattu 2.11.2024 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Ohje_3_2016_Palvelunestohyokkaysten_ehkaisy_ja_torjunta_0.pdf.

Rouse, M. 2024. Tietoturva. Techopedia 24.6.2024. Viitattu 19.10.2024. https://www.techopedia.com/fi/sanasto/tietoturva.

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. Kvantifiointi. KvaliMOTV – Menetelmäopetuksen tietovaranto. Yhteiskuntatieteellinen tietoarkisto. Viitattu 26.10.2024 https://www.fsd.tuni.fi/menetelmaopetus/kvali/L7_3_3.html.

Sanastokeskus ry 2024. Tietoturva. TEPA-termipankki. Viitattu 6.10.2024 https://termipankki.fi/tepa/fi/haku/tietoturva.

Selviytymisopas kiristyshaittaohjelmia vastaan 2016. Kokemuksia kiristyshaittaohjelmista Suomessa ja neuvoja niistä selviytymiseen. Viestintäviraston julkaisu 005/2016. Viitattu 2.11.2024 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kiristyshaittaohjelmat__teemakooste_07_2016.pdf.

Sussman, B. 2022. The 3 Pillars of Cybersecurity: People, Process, and Technology. BlackBerry 26.6.2024. Viitattu 9.11.2024 https://blogs.blackberry.com/en/2022/10/the-3-pillars-of-cybersecurity-people-process-and-technology.

Traficom 2020. Pienyrityksen kyberturvallisuusopas. Liikenne- ja viestintävirasto. Kyberturvallisuuskeskus. Viitattu 6.10.2024 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf.

Traficom 2022. Toimintaohje – Palvelunestohyökkäys. Liikenne- ja viestintävirasto. Kyberturvallisuuskeskus. Viitattu 20.10.2024 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Palvelunestohy%C3%B6kk%C3%A4ysToimintaohje.pdf.

Traficom 2024a. Kotiverkon ja reitittimen tietoturva. Liikenne- ja viestintävirasto. Kyberturvallisuuskeskus. Viitattu 10.111.2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/kotiverkon-ja-reitittimen-tietoturva.

Traficom 2024b. Kyberturvallisuuskeskuksen viikkokatsaus – 37/2024. Liikenne- ja viestintävirasto. Kyberturvallisuuskeskus. Viitattu 26.10.2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-372024#74606-0.

Valimail 2024. Complete Guide to Phishing: Techniques & Mitigations. Viitattu 3.11.2024 https://www.valimail.com/resources/guides/guide-to-phishing/.

Valli, R. 2018. Aineistonkeruu kyselylomakkeella. Teoksessa R. Valli (toim.) Ikkunoita tutkimusmetodeihin 1. Metodin valinta ja aineistonkeruu: virikkeitä aloittelevalle tutkijalle. 5., uudistettu painos. Jyväskylä: PS-kustannus, 92–116.

Valli, R. & Perkkilä P. 2018. Sähköinen kyselylomake ja sosiaalinen media aineistonkeruussa. Teoksessa R. Valli (toim.) Ikkunoita tutkimusmetodeihin 1. Metodin valinta ja aineistonkeruu: virikkeitä aloittelevalle tutkijalle. 5., uudistettu painos. Jyväskylä: PS-kustannus, 117–128.

Vehkalahti, K. 2014. Kyselytutkimuksen mittarit ja menetelmät. Helsinki: Finn Lectura.

Viestintävirasto 2014. Kyberturvallisuuskeskus. Langattomasti, mutta turvallisesti. Langattomien lähiverkkojen tietoturvallisuudesta. Viitattu 5.11.2024 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Langattomasti_mutta_turvallisesti._Langattomien_lahiverkkojen_tietoturvallisuudesta.pdf.

XeneX 2023. People Process Technology. Viitattu 9.11.2024 https://www.xenexsoc.com/blog/51bpom4k8jm7jdaxc3u5zr75ung4kj.

LIITTEET

Liite 1 1(4). Kyselylomakkeen kysymykset

1. **Käytätkö omia vai yrityksen laitteita työssäsi? Voit valita useamman vaihtoehdon.**
    a. käytän omaa tietokonettani
    b. käytän yrityksen tietokonetta
    c. käytän omaa puhelinta
    d. käytän yrityksen puhelinta

2. **Missä työskentelet? Voit valita useamman vaihtoehdon.**
    a. toimistolla
    b. etänä

3. **Vastasit, että työskentelet etänä. Kerro tarkemmin työskenteletkö esim. kotona tai jossain julkisessa tilassa (esim. kahvila).** ***(näytetään jos vastasi kysymykseen 2: etänä)***

4. **Käytätkö työskennellessäsi julkista WiFi-verkkoa?**
    a. kyllä, säännöllisesti
    b. kyllä, satunnaisesti
    c. hyvin harvoin
    d. en koskaan
    e. en osaa sanoa

5. **Käytätkö VPN-yhteyttä julkisessa WiFi-verkossa** ***(näytetään jos vastasi kysymykseen 4: a, b tai c)***
    a. kyllä
    b. en

6. **Onko yrityksessä olemassa selkeät tietoturvakäytännöt- tai ohjeet?**
    a. kyllä
    b. ei
    c. en osaa sanoa

7. **Kuinka hyvin tunnet yleisimmät tietoturvauhkat (esim. phising, haittaohjelmat)?**
    a. erittäin hyvin – tiedän, miten tunnistaa ja välttää ne
    b. melko hyvin – olen tietoinen, mutta saatan tarvita lisää tietoa
    c. jonkin verran – tunnen käsitteet, mutta en tiedä tarkasti, miten toimia
    d. vähän – olen kuullut niistä, mutta en ymmärrä niiden toimintaa
    e. en lainkaan – en tunne näitä uhkia

8. **Kenen vastuulla on huolehtia työssä käytettävän laitteen (puhelin/tietokone) tietoturvasta? Tähän kuuluu mm. palomuuri, virustentorjunta sekä ohjelmistojen ja järjestelmien päivitykset.**
    a. itseni vastuulla
    b. yrityksen vastuulla
    c. en osaa sanoa

Liite 1 2(4). Kyselylomakkeen kysymykset

9. **Miten huolehdit tietokoneesi ja sen ohjelmistojen päivityksistä? Onko päivitykset asetettu automaattisiksi vai päivitätkö ne manuaalisesti?** ***(näytetään jos vastasi kysymykseen 8: itseni vastuulla)***
    a. päivitykset tehdään automaattisesti
    b. päivitän manuaalisesti
    c. en osaa sanoa

10. **Käytätkö tietokoneessasi virustentorjuntaohjelmaa?** ***(näytetään jos vastasi kysymykseen 8: itseni vastuulla)***
    a. käytän virustentorjuntaohjelmaa
    b. en käytä: kerro miksi
    c. en osaa sanoa

11. **Onko tietokoneessasi palomuuri päällä?** ***(näytetään jos vastasi kysymykseen 8: itseni vastuulla)***
    a. kyllä
    b. ei
    c. en osaa sanoa

12. **Koetko, että sinulla on tarpeeksi tietoa ja taitoa suojata oma työvälineesi tietoturvariskien varalta?** ***(näytetään jos vastasi kysymykseen 8: itseni vastuulla)***
    a. kyllä, olen varma taidoistani
    b. kyllä, mutta voisin hyötyä lisätiedosta tai -koulutuksesta
    c. en ole varma
    d. ei, minulla ei ole riittävästi tietoa tai taitoa

13. **Käytätkö salasanaa tai muuta tunnistautumismenetelmää laitteissasi, jotka sisältävät yrityksen tietoja, tai niillä on pääsy yrityksen tietoihin? Voit valita useamman vaihtoehdon.**
    a. kyllä, käytän salasanaa
    b. kyllä, käytän muuta tunnistautumismenetelmää (sormenjälkitunnistus, kasvojentunnistus)
    c. en, laitteeni aukeaa ilman tunnistautumista

14. **Miten muodostat salasanat eri sovelluksiin ja järjestelmiin? Voit valita useamman vaihtoehdon.**
    a. käytän salasananhallintaohjelmaa, joka luo vahvan salasanan
    b. käytän salasanageneraattoria luomaan vahvoja salasanoja
    c. muodostan salasanat itse ja käytän vahvoja salasanoja
    d. käytän helposti muistettavia sanoja tai lauseita, jotka eivät sisällä erikoismerkkejä
    e. käytän mahdollisimman yksinkertaisia salasanoja, jotka on helppo muistaa
    f. käytän jotain muuta tapaa. Kerro mitä

Liite 1 3(4). Kyselylomakkeen kysymykset

15. **Käytätkö samoja salasanoja useissa eri palveluissa tai järjestelmissä?**
    a. usein
    b. joskus
    c. hyvin harvoin
    d. en koskaan
    e. en osaa sanoa
16. **Kuinka usein vaihdat salasanoja eri paikkoihin, mikäli sovellus tai järjestelmä ei itse muistuta/pakota salasanan vaihtamista?**
    a. säännöllisesti (esim. kerran kuussa tai useammin)
    b. melko usein (esim. muutaman kuukauden välein)
    c. satunnaisesti (esim. kerran vuodessa)
    d. hyvin harvoin (harvemmin kuin kerran vuodessa)
    e. en koskaan vaihda salasanoja

17. **Miten säilytät salasanoja? Voit valita useamman vaihtoehdon.**
    a. käytän salasananhallintaohjelmaa
    b. tallennan salasanoja selaimeen
    c. säilytän salasanoja paperilla
    d. säilytän salasanoja erillisessä tiedostossa (esim. word, excel tms.) Kerro missä säilytät tiedostoa?
    e. säilytän salasanoja jossain muualla. Missä?

18. **Käytätkö kriittisiin järjestelmiin tai sovelluksiin yhteisiä tunnuksia, vai onko jokaisella omat henkilökohtaiset tunnukset? Kriittisillä järjestelmillä tai sovelluksilla tarkoitetaan tässä tapauksessa esim. CRM-järjestelmää, laskutusjärjestelmää tai muuta, joka sisältää asiakas- ja tilaustietoja.**
    a. käytän omia henkilökohtaisia tunnuksia
    b. käytän yhteisiä tunnuksia
    c. käytän sekä omia että yhteisiä tunnuksia

19. **Missä yrityksen tärkeät tiedot, kuten asiakasrekisteri tai tilaustiedot säilytetään? Onko käytössä pilvipalveluja, paikallisia tallennusratkaisuja tai molempia? Kerro mahdollisimman tarkasti.**

20. **Varmuuskopioidaanko yrityksen tärkeät tiedot (asiakasrekisteri, tilaustiedot) ja kuka niistä vastaa?**

21. **Miten varmistatte, että kriittiset tiedot ovat aina käytettävissä, vaikka tapahtuisi tietoturvaloukkaus tai muu häiriö?**
    a. käytämme säännöllisiä varmuuskopioita, jotka voidaan palauttaa tarvittaessa
    b. luotamme palveluntarjoajan tietojen saatavuus- ja palautusominaisuuksiin
    c. luotamme siihen, että tietoturvaongelmia ei ilmene tai ne ratkeavat nopeasti
    d. emme ole varautuneet tietoturvaloukkauksiin tai häiriöihin
    e. muu, kerro lisää

Liite 1 4(4). Kyselylomakkeen kysymykset

22. Miten tärkeänä pidät tietoturvaa yrityksen toiminnan kannalta?

a. erittäin tärkeänä
b. melko tärkeänä
c. jonkin verran tärkeänä
d. ei kovin tärkeänä
e. ei lainkaan tärkeänä

23. Miten tietoturva-asioihin suhtaudutaan yrityksessä? Onko tietoturvasta keskusteltu avoimesti?

24. Koetko, että tietoturvan parantaminen vaatisi enemmän aikaa, resursseja tai koulutusta? Voit kirjoittaa omia ajatuksiasi aiheesta.

25. Miten suhtaudut tietoturvaan yleisesti? Koetko, että tietoturva on helppo ja tarpeellinen osa työtäsi, vai aiheuttaako se haasteita tai rajoituksia?

Liite 2. Kehityssuunnitelma

Yritys X:n tietoturvan kehityssuunnitelma

1. Tietoturvakäytäntöjen ja vastuiden selkiyttäminen

Nykytila:	Epäselvyyksiä tietoturvakäytäntöjen ja -ohjeiden osalta. Selkeää kirjallista ohjetta ei ole annettu tai selkeästi kommunikoitu koko henkilöstölle. Lisäksi epäselvyyttä kuka huolehtii laitteiden tietoturvasta.
Riski liiketoiminnalle:	Epäselvyys voi johtaa tietoturvatoimien laiminlyöntiin, inhimillisiin virheisiin ja tietovuotoihin.
Kehitystoimenpide:	Suosituksena on laatia yksinkertainen tietoturvapolitiikka ja dokumentoida se. Dokumentin olisi hyvä kattaa perusohjeet ja vastuut liittyen tietoturvaan. Dokumenttiin on hyvä sisällyttää esimerkiksi ohjeet salasanojen hallinnasta, tietojenkalastelun tunnistamisesta, haittaohjelmilta suojautumisesta ja etätyön tietoturvakäytännöistä. Tällainen dokumentti on hyvä myös antaa uudelle työntekijälle perehdytyksen yhteydessä, jotta hän tietää heti työsuhteensa alusta lähtien mitä käytäntöjä noudattaa.

2. Salasanojen hallinnan ja käytön parantaminen

Nykytila:	Salasanakäytännöt vaihtelevat; vahvoja salasanoja käytetään, mutta salasanoja säilytetään mm. selaimessa ja vaihdetaan harvakseltaan.
Riski liiketoiminnalle:	Voi altistaa tietovuodoille, mikäli ulkopuolinen pääsee käsiksi selaimen tietoihin.
Kehitystoimenpide:	Salasanahallintaohjelman käyttöönotto ja säännöllinen salasanojen vaihtotiheys. Monivaiheisen tunnistautumisen käyttöönotto vähintään kriittisissä järjestelmissä, mikäli se on mahdollista.

Liite 2. Kehityssuunnitelma

3. Pilvipalveluiden hallinta ja varmuuskopiot

Nykytila:	Luotetaan palveluntarjoajien varmuuskopiointi- ja palautuskäytäntöihin. Kriittisten tietojen säilytyspaikoista ei ole täyttä varmuutta koko henkilöstön keskuudessa.
Riski liiketoiminnalle:	Jos pääsy esim. CRM-ohjelmaan on estetty, ei tietoja pystytä käyttämään ja se voi aiheuttaa toimintakatkoksen. Häiriötilanteessa kriittisiin tietoihin ei päästä käsiksi.
Kehitystoimenpide:	Vaikka palveluntarjoajat huolehtivat tietojen varmuuskopioinnista, voisi olla hyödyllistä harkita omaa varmuuskopiointistrategiaa tärkeimmille tiedoille. Tämä voi parantaa tietojen saatavuutta häiriötilanteessa ja vähentää riippuvuutta ulkoisista toimijoista. Palveluntarjoajilta on syytä varmistaa varmuuskopiointikäytännöt, eli esimerkiksi kuinka usein varmuuskopiointi tehdään, kuinka kauan tietoja säilytetään, ja miten nopeasti tiedot voidaan palauttaa tietoturvaloukkauksen tai muun häiriön sattuessa. Kriittisten tietojen sijainnit on tärkeää dokumentoida ja kommunikoida selkeästi henkilöstön kesken.

4. Etätyö

Nykytila:	Henkilöstö työskentelee pääosin etänä omassa kodissa. Julkista Wi-Fi-verkkoa käytetään harvoin, mutta silloin ei käytetä VPN-yhteyttä.
Riski liiketoiminnalle:	Julkisen Wi-Fi-verkon käyttö ilman VPN-yhteyttä lisää merkittävästi riskiä yrityksen tietojen joutumista ulkopuolisten haltuun ja altistaa tietovuodoille. Mikäli kotiverkko on riittämättömästi suojattu, voi altistaa vakoilulle ja tietovuodoille.
Kehitystoimenpide:	Henkilöstöä tulisi ohjeistaa käyttämään VPN-yhteyttä aina, kun yhdistetään julkiseen Wi-Fi-verkkoon. VPN:n käyttö kotona työskennellessä on myös hyvä huomioida. Kotiverkon asetusten tarkistaminen (verkkokaapelin kytkentä, etähallinnan mahdollisuuden poistaminen, oletussalasanan vaihto, laitteen päivitysten tarkistaminen ja asentaminen).

Liite 2. Kehityssuunnitelma

5. Henkilöstön tietoturvaosaamisen kehittäminen

Nykytila:	Henkilöstö tunnistaa tietoturvan tärkeyden osana liiketoimintaa, mutta osa kokee tietoturvauhkien tunnistamisen haastavaksi.
Riski liiketoiminnalle:	Puutteellinen osaaminen voi johtaa esim. tunnusten tai tietojen vuotamiseen ulkopuolisille kalasteluyritysten tai haittaohjelmien kautta, mikä vaarantaa yrityksen tiedot.
Kehitystoimenpide:	Netistä löytyy paljon ilmaista materiaalia, mikäli ulkopuolista asiantuntijaa ei haluta käyttää resurssisyistä. Ilmaisia luentoja sekä oppaita löytyy helposti, mistä on varmasti apua ja niitä suositellaan hyväksikäytettävän. Lisäksi suositellaan, että jokainen henkilöstön jäsen lukee opinnäytetyöraportin, koska se tarjoaa arvokasta tietoa tietoturvasta.

6. Jatkuvuussuunnitelma

Nykytila:	Tämän olemassaoloa ei tutkimuksella selvitetty
Riski liiketoiminnalle:	Ei tiedetä miten toimia häiriötilanteessa.
Kehitystoimenpide:	Jos jokin menee pieleen, jatkuvuus- tai palautumissuunnitelma auttaa takaamaan toiminnan jatkumisen. Suunnitelma voi sisältää esim. kaikki palvelut ja vastuuhenkilöiden nimet. Suunnitelman olisi tarkoitus kuvata miten toimitaan häiriötilanteessa esim., jos dataa katoaa tai jokin kriittinen palvelu ei ole saatavilla.