Ella Jussila

Tietosuoja ja tietoturva etätyön aikakaudella

Laskentatoimen ja rahoituksen
akateeminen yksikkö
Talousoikeuden kandidaatin tutkielma
Kauppatieteiden kandidaatti

Vaasa 2025

VAASAN YLIOPISTO
Laskentatoimen ja rahoituksen akateeminen yksikkö
Tekijä: Ella Jussila
Tutkielman nimi: Tietosuoja ja tietoturva etätyön aikakaudella
Tutkinto: Kauppatieteiden kandidaattitutkinto
Oppiaine: Talousoikeus
Työn ohjaaja: Pekka Vainio
Valmistumisvuosi: 2025 **Sivumäärä:** 43

TIIVISTELMÄ:

Etätyön lisääntyminen koronapandemian myötä on tuonut mukanaan merkittäviä haasteita tietosuojan ja tietoturvan osa-alueilla. Tämä tutkielma tarkastelee etätyön vaikutuksia organisaatioiden tietosuojaan ja tietoturvaan, erityisesti koronapandemian jälkeisessä työelämässä, missä etätyö on vakiintunut pysyväksi osaksi monien työntekijöiden arkea. Etätyön yleistyminen on luonut uusia haasteita tietoturvakäytäntöihin ja -strategioihin, kun työ on siirtynyt organisaation hallituista ympäristöistä yksityisiin tiloihin kuten koteihin. Organisaatioiden on keskeistä varmistaa, että henkilötietojen käsittely ja yrityksen tietoverkkojen suojaus säilyvät riittävällä tasolla, kun työntekijät työskentelevät eri etätyöpisteistä.

Teknologian kehitys ja globalisaatio ovat samalla muuttaneet henkilötietojen käsittelyä, lisäten tietojen määrää ja saatavuutta maailmanlaajuisesti. Tämä kehitys on haastanut perinteiset tietosuojakäytännöt ja luonut tarpeen yhtenäiselle tietosuojakehykselle. Etätyö, joka tapahtuu työnantajan tilojen ulkopuolella hyödyntää tietotekniikkaa ja tietoliikenneyhteyksiä yhteydenpidossa. Tässä uudessa tilanteessa sääntelyn kuten EU:n tietosuoja-asetuksen ja kansallisten lakien merkitys korostuu työntekijöiden ja organisaatioiden velvollisuuksien näkökulmasta.

Tutkielmassa tarkastellaan, miten etätyö on muuttanut tietoturvakäytäntöjä ja miten organisaatiot ovat sopeuttaneet toimintaansa vastatakseen riskeihin, mitä hajautetut työympäristöt luovat. Kiinnitetään huomiota siihen, millä tavoin työnantajat voivat tukea tietoturvaa ilman suoraa mahdollisuutta valvoa fyysistä työympäristöä. Keskeiseksi nousevat myös työntekijöiden rooli ja vastuu tietoturvan ylläpitämisessä sekä käytännön keinot riskien hallintaan kuten teknologiset ratkaisut, ohjeistukset ja koulutus.

Tutkielma rajautuu nimenomaan etätyöhön liittyviin tietoturvahaasteisiin jättäen muut tietoturvakysymykset kuten ulkoisten sidosryhmien tietojenkäsittelyn käsittelemättä. Tarkoituksena on muodostaa kokonaiskuva siitä, miten organisaatiot voivat turvata tietosuojaa ja tietoturvaa hajautetussa työympäristössä ja miten lainsäädäntö tukee tätä tavoitetta.

AVAINSANAT: Tietosuoja, Tietoturva, Etätyö, Tietoturvariskit

Sisällys

Kuvat

Lyhenteet

TyöturvL	Työturvallisuuslaki
ILO	Kansainvälisen työjärjestön yleissopimus
GDPR	General Data Protection Regulation
YksTL	Työelämän tietosuojalaki
ENISA	European Network and Information Security Agency
ISO	Kansainvälinen standardisoimisjärjestö
BYOD	Bring your own device
APT	Advanced Persistent Threats
KHO	Korkein hallinto-oikeus
SaaS	Software as a service
MDM	Mobile Device Management

Oikeustapausluettelo:

Korkein hallinto-oikeus

KHO 2022:131

1 Johdanto

Työelämä on muuttunut merkittävästi koronapandemian seurauksena, ja etätyön yleistyminen on yksi keskeisimmistä muutoksista. Vuoden 2020 aikana säännöllisesti kotona työskentelevien osuus kaksinkertaistui: tammikuussa 15 prosenttia kaikista työllisistä ilmoitti työskentelevänsä säännöllisesti kotona, kun taas marraskuussa osuus oli jo 31 prosenttia. Tämä muutos kuvastaa laajemmin työnteon paikkasidonnaisuuden murrosta, jossa työ siirtyy organisaation valvotusta ympäristöstä yksityisiin tiloihin, kuten koteihin.[1]

Etätyön yleistyminen on tuonut mukanaan tietosuojan ja tietoturvan varmistamiseen uudenlaisia haasteita sekä muuttanut merkittävästi organisaatioiden tietoturvatarpeita ja -strategioita. Hajautetut työympäristöt ovat tehneet sääntelyn roolista aiempaa tärkeämmän. [2] Vaikka etätyöskentely ei muuta työnantajan velvollisuuksia työsopimuslain [3] tai työaikalain [4] soveltamisen suhteen, se luo uusia vaatimuksia työntekijöiden turvallisuuden ja tietosuojan varmistamiseksi. Työnantajien vastuulla on tietosuojan takaaminen sekä työntekijän turvallisuuden varmistaminen, mutta kodin tai muun etätyöpaikan fyysinen valvonta on lainsäädännön rajoissa rajallista. Tämä rajoittaa työnantajien mahdollisuuksia valvoa esimerkiksi työvälineiden ja tietoverkkojen turvallisuutta. Digitaalisten työympäristöjen yleistyminen on lisännyt riippuvuutta tietojärjestelmistä, ja on nostanut esiin työntekijöiden laitteiden ja kotiverkkojen puutteellisen suojauksen aiheuttamat riskit. Monet organisaatiot ovat joutuneet nopeasti päivittämään tietoturvakäytäntöjään ja koulutusohjelmiaan vastatakseen näihin uusiin haasteisiin. Etätyön luoma hajautettu työympäristö korostaa tarvetta yhtenäisille tietoturvakäytännöille, jotka tukevat sekä organisaation että työntekijöiden turvallisuutta.[5]

---

[1] Leskinen 2020
[2] Andersson 2024: 1.
[3] Työsopimuslaki 55/2001
[4] Työaikalaki 872/2019
[5] Hietala & muut 2024: s.189–191

Koronarajoitusten poistumisesta huolimatta etätyön suosio on säilynyt korkeana, mikä osoittaa sen vakiintuneen osaksi nykyaikaista työelämää. Vuonna 2022 työllisistä 11 prosenttia teki koko työaikansa etänä, ja vähintään puolet työajastaan kotona työskentelevien osuus nousi 13 prosenttiin. Etätyön pysyvä luonne on nostanut esiin tarpeen tarkemmalle seurantatiedolle kotona työskentelystä. EU-asetuksen mukaan kotona työskentelyä seurataan nykyään entistä tarkemmin, mikä helpottaa vertailua muihin maihin sekä auttaa ymmärtämään etätyön laajuutta.[6]

1.1 Tutkimuskysymys ja -ongelma

Tutkimuksen tarkoituksena on selvittää, miten etätyö vaikuttaa tietosuojan ja tietoturvan hallintaan organisaatioissa. Analysoidaan sääntelyn ja organisaation käytäntöjen näkökulmasta etätyön vaikutuksia tietosuojaan ja tietoturvaan. Tarkoituksena on myös analysoida millaisia riskejä etätyö tuo tietosuojalle ja tietoturvalle, ja miten näitä riskejä hallitaan. Tutkielmassa pyritään vastaamaan seuraaviin keskeisiin tutkimuskysymyksiin:

1. Miten tietoturvakäytännöt ovat muuttuneet etätyön myötä ja millä tavoin organisaatiot valvovat näitä käytäntöjä?
2. Millaisia haasteita ja riskejä etätyö on tuonut organisaatioiden tietoturvaan ja kuinka niitä hallitaan?

1.2 Tutkielman rajaukset ja rakenne

Tämä tutkielma tarkastelee etätyön tietoturvaa ja sen luomia tietosuojahaasteita nykyaikaisessa työympäristössä, jossa teknologian kehitys ja etätyön lisääntyminen on muuttanut toimintatapoja. Tutkimus keskittyy siihen, miten tietosuoja-asetukset sekä kansalliset tietosuojalait vaikuttavat organisaatioiden ja yksilöiden tietoturvakäytäntöihin. Tutkielma jättää käsittelemättä tietoturvakysymyksiä, jotka eivät ole suorassa yhteydessä etätyöhön. Tutkimus keskittyy siihen, miten organisaatiot

[6] Leskinen 2023

soveltavat tietosuojan periaatteita etätyössä sekä siihen, miten työntekijät voivat säilyttää korkean tietoturvatason työskennellessään etänä. Tutkielmassa ei käsitellä kaikkia tietoturvariskejä, jotka liittyvät muiden sidosryhmien tietojen käsittelyyn organisaation ulkopuolella. Painotus on siinä, miten tietoturva- ja tietosuojalainsäädäntö ohjaavat etätyötä ja sen tietoturvallisuutta organisaatioiden sisäisissä prosesseissa.

Tämä tutkielma on jaettu viiteen päälukuun. Ensimmäinen pääluku on johdanto, joka esittelee tutkielman aiheen. Johdannossa käsitellään tutkielman tutkimuskysymys ja -ongelma sekä rakenne ja sisältö. Tämän luvun tavoitteena on antaa selkeä kokonaiskuva tutkielman aiheesta ja tutkimuskysymyksistä. Toisessa pääluvussa käsitellään tietoturvan ja tietosuojan sääntelyä sekä tietosuojan erityisvaatimuksia. Kolmannessa pääluvussa keskitytään etätyön tietoturvahaasteisiin ja riskeihin. Luvussa tarkastellaan, miten etätyön yleistyminen on muuttanut tietoturvan ja tietosuojan tarpeita, sekä millaisia riskejä etätyöhön liittyy. Neljäs pääluku käsittelee hyviä käytäntöjä sekä teknologisia ratkaisuja, joita voidaan hyödyntää tietoturvan ja tietosuojan parantamiseksi etätyössä. Luvussa analysoidaan, miten organisaatiot voivat tukea työntekijöitään selkeillä ohjeilla, koulutuksilla ja teknologisilla ratkaisuilla. Tutkielman viidennessä ja viimeisessä pääluvussa esitetään tutkimuksen keskeiset havainnot sekä pyritään vastaamaan tutkimuskysymyksiin.

1.3 Tutkielman keskeiset käsitteet

Etätyöllä tarkoitetaan työskentelymuotoa, jossa työ tehdään muualla kuin työnantajan tiloissa, esimerkiksi kotona, liikkuvassa työssä tai erityisesti siihen suunnitelluissa etätoimistoissa. Etätyö hyödyntää yleensä tietotekniikkaa, ja työnantajan ja työntekijän välinen yhteydenpito hoidetaan tietoliikenneyhteyksien avulla. Etätyölle on ominaista, että työ voidaan suorittaa joustavasti ajasta ja paikasta riippumatta, mikä tekee siitä myös modernin työelämän keskeisen osan. Se ei ole erillinen työsuhdemuoto, vaan

tapa organisoida työtä uudella tavalla, huomioiden sekä työntekijän tarpeet, että työnantajan velvollisuudet.[7]

Vaikka etätyötä sovelletaan samoilla työlainsäädännön säännöksillä kuin työpaikalla tehtävää työtä, sillä ei ole tarkkaa määritelmää Suomen työlainsäädännössä. Etätyö on käytännössä jatkumoa kotityöskentelylle, jota on aiemmin säännelty Kansainvälisen työjärjestön (ILO) yleissopimuksissa nro 177 ja 189. Näiden sopimusten mukaan kotona tehtävä työ kuuluu työsuhteen piiriin ja työntekijän oikeudet kuten työturvallisuus ja sosiaaliturva on turvattava samalla tavalla kuin työnantajan tiloissa tehtävässä työssä.[8]

Etätyön ehdot perustuvat myös Euroopan tasolla solmittuun puitesopimukseen, joka ohjaa etätyötä koskevien sopimusten tekemistä niin julkisella kuin yksityisellä sektorilla. Asiantuntijat korostavat, että etätyöstä tulisi aina sopia kirjallisesti, riippumatta siitä onko se jatkuvaa, säännöllistä tai satunnaista. Puitesopimus toimii myös perustana työ- ja virkaehtosopimuksissa ja sen rinnalla voidaan hyödyntää keskusjärjestöjen laatimia ohjeita, jotka sisältävät tärkeimmät huomioitavat seikat etätyöjärjestelyistä sovittaessa. Etätyön juridinen asema vaatii myös tarkkaa sopimista työnantajan ja työntekijän välillä, jotta työn tekemiseen liittyvät vastuut ja oikeudet ovat molemmin puolin selkeitä.[9]

Tietoturva liittyy tietohallintoon.[10] Sillä viitataan toimintatapoihin ja käytäntöihin, joilla suojataan tietoja luvattomalta pääsyltä, muutoksilta, paljastumiselta ja tuhoutumiselta. Yrityksissä tietoturvaan panostetaan erityisesti digitalisoitumisen myötä ja se kattaa sekä tekniset ratkaisut että organisatoriset käytännöt. Teknisistä keinoista yleisimpiä ovat ajantasaiset ohjelmistot, vahvat salasanat, varmuuskopiointi sekä salaustekniikat ja VPN-yhteydet. Myös henkilöstön koulutuksella on merkittävä rooli, sillä 66 % yrityksistä tarjoaa joko vapaaehtoista tai pakollista ohjeistusta tietoturvan velvollisuuksista. Tietoturvaan liittyy myös selkeiden prosessien sekä dokumentaation

[7] Nieminen 2024: s.49
[8] Hietala & muut 2024: s.187
[9] Vilkman 2016: s.200
[10] Niemi 2018: s.415

merkitys. Dokumentit sisältävät usein datan käsittelyn, käyttöoikeudet ja toimintatavat. Tietoturva on kokonaisvaltainen prosessi, jossa yhdistyvät teknologiset, hallinnolliset sekä inhimilliset tekijät tietojen suojaamiseksi.[11]

Tietosuoja on perusoikeus, joka turvaa yksilön oikeudet ja vapaudet henkilötietojen käsittelyssä. Sen tavoitteena on varmistaa, että henkilötietoja käsitellään lainmukaisesti, läpinäkyvästi ja rekisteröidyn oikeuksia kunnioittaen. Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön, ja niiden käsittely edellyttää aina laillista perustetta, kuten suostumusta, sopimuksen täytäntöönpanoa tai lakisääteistä velvoitetta. Rekisterinpitäjä määrittää tietojen käsittelyn tarkoitukset ja keinot, kun taas henkilötietojen käsittelijä toimii rekisterinpitäjän lukuun. Tietosuojan toteutumista valvoo riippumaton viranomainen, joka huolehtii siitä, että henkilötietojen käsittelyssä noudatetaan säädettyjä periaatteita.[12] Tietosuoja keskittyy siis henkilötietojen suojaamiseen – ei suojata pelkästään tietoa, vaan yksilöitä tietojen takana.[13]

[11] Tilastokeskus 2019: 7.
[12] Tietosuojavaltuutetun toimisto: Tietosuoja
[13] Edilex. Karvinen 2021: webinaari

2 Tietosuojan ja tietoturvan sääntely

Tietosuojan ja tietoturvan sääntely muodostaa perustan sille, miten organisaatiot voivat varmistaa etätyöympäristössä tietojen turvallisuuden ja yksityisyyden. Jenna Anderssonin väitöskirja ”Organisaation hyvä tietoturvan sääntelyjärjestelmä” tarkastelee nykyistä tietoturvasääntelyn tilaa Suomessa ja tuo esiin merkittävimpiä puutteita. Hänen tutkimuksensa mukaan sääntely on tällä hetkellä hajanaista, mikä vaikeuttaa organisaatioiden mahdollisuuksia noudattaa sääntöjä yhdenmukaisesti ja tehokkaasti. Etätyössä tämä haaste korostuu, jossa työntekijät työskentelevät ympäristöissä, jotka ovat hajautettuja ja käsittelevät arkaluonteisia tietoja usein epäyhtenäisten teknologisten ratkaisujen kautta. [14] Tietosuojalainsäädännön perinteinen tapa luokitella henkilötiedot arkaluonteisiin ja ei-arkaluonteisiin on saanut kritiikkiä nykyaikaisten tietojenkäsittelymenetelmien valossa. Arkaluonteisten tietojen määrittely on usein mielivaltaista, sillä monia henkilötietoja voidaan yhdistää ja analysoida niin, että niistä paljastuu arkaluonteisia tietoja. Tämä korostuu etätyössä, jossa kerätyt tiedot kuten sijainti- ja käyttödata, voivat johtaa päätelmiin työntekijän yksityiselämästä tai henkilökohtaisista ominaisuuksista. Sääntelyn tulisi painottua tietojen ominaisuuksien sijaan henkilötietojen käytön riskien ja seurausten arviointiin.[15]

Andersson nostaa esille tarpeen kansalliselle tietoturvalaille, joka mahdollisesti yhtenäistäisi sääntelyjärjestelmän ja tarjoaisi selkeät ohjeet organisaatioille. Se vahvistaisi organisaatioiden luottamuksellisten tietojen ja yksilöiden oikeuksien suojaa sekä mahdollistaisi proaktiivisemman toiminnan nopeasti muuttuvassa yhteiskunnassa. Etätyöympäristöön liittyy monia uusia riskitekijöitä, kuten suojaamattomat verkot sekä lisääntynyt riippuvuus pilvipohjaisista palveluista. Ilman yhtenäistä sääntelyjärjestelmää organisaatioiden on luotettava omiin tulkintoihinsa monimutkaisista ja keskenään ristiriitaisista säädöksistä.[16]

---

[14] Andersson 2024: 128–129
[15] Solove 2024: 2 A, 3.
[16] Andersson 2024: s.128–136

Selkeä ja yhtenäinen sääntelyjärjestelmä ei kuitenkaan yksinään paranna organisaatioiden kykyä noudattaa tietoturvavaatimuksia, vaan myös lisää työntekijöiden luottamusta tietojensa käsittelyn turvallisuuteen. Tämän merkitys korostuu etätyöympäristössä, jossa yksityiselämän ja työelämän rajat hämärtyvät ja työntekijät joutuvat usein tekemään itsenäisiä päätöksiä tietoturvan ylläpitämiseksi. Yhtenäinen sääntely voisi parantaa tietoturvaohjeiden soveltamista ja tarjota organisaatioille selkeämmän viitekehyksen työntekijöidensä kouluttamiseen tietoturva-asioissa.

2.1 EU:n tietosuoja-asetus ja sen merkitys etätyöympäristössä

Euroopan unionin yleinen tietosuoja-asetus GDPR (General Data Protection Regulation) otettiin käyttöön 27. huhtikuuta 2016 ja se kumosi Euroopan parlamentin ja neuvoston direktiivin 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja tietojen vapaasta liikkuvuudesta.[17] Asetus sisältää yhteensä 99 artiklaa, jotka jaetaan 11 lukuun, jossa käsitellään muun muassa tietosuojaperiaatteita, henkilötietojen käsittelyn oikeusperusteita sekä yksilöiden oikeuksia. Tietosuoja-asetus pyrkii edistämään vapautta, turvallisuutta ja oikeudenmukaisuutta Euroopan unionissa sekä tukemaan taloudellista ja sosiaalista kehitystä sisämarkkinoilla. Asetuksen tavoitteena ei ole rajoittaa henkilötietojen käsittelyä liiketoiminnassa, vaan tarjota säännöt, jotka määrittelevät miten henkilötietoja voidaan laillisesti hyödyntää.[18] Asetus asettaa laajat puitteet henkilötietojen käsittelylle, ja se on sovellettavissa aina, kun henkilötietoja hallinnoidaan esimerkiksi yrityksien tietojärjestelmissä.[19]

GDPR on keskeinen säädös, joka asettaa velvoitteita organisaatioille henkilötietojen käsittelyyn liittyen Euroopan unionissa. Sen keskeinen tavoite on varmistaa, että henkilötietoja käsitellään selkeästi määritellyissä ja lainmukaisissa tarkoituksissa, ja että

[17] Finlex, HE 2/2020
[18] Korpisaari, Pitkänen, Warma-Lehtinen 2018: 1.
[19] Hanninen ja muut 2017: 2.

käsittelyn turvallisuudesta pidetään huoli teknisin ja organisatorisin toimin. GDPR luo yhtenäisen sääntelykehyksen koko Euroopan unionin alueelle, mikä helpottaa tietosuojakäytäntöjen yhdenmukaistamista organisaatioissa. Tämä on erityisen tärkeää, kun työntekijät voivat tehdä etätyötä useista eri maista käsin.[20]

Asetus ei pelkästään vahvista sääntöjä henkilötietojen suojeluun ja vapaaseen liikkuvuuteen, vaan se turvaa myös luonnollisten henkilöiden perusoikeudet. Asetuksen perusedellytyksenä on, että henkilötietojen käsittely on läpinäkyvää ja se perustuu rekisteröidyn antamaan selkeään suostumukseen. GDPR korostaa tietojen minimointia, tietoturvan tärkeyttä ja antaa yksilöille oikeuden saada tietoonsa, miten heidän tietojaan käytetään. [21]

2.2 Kansallisen tietosuojalain rooli henkilötietojen käsittelyssä

Tietosuojalaki [22] (1050/2018) täsmentää sekä täydentää henkilötietojen käsittelyn säännöksiä kansallisella tasolla Euroopan unionin yleisen tietosuoja-asetuksen (GDPR) rinnalla. Laki kattaa tietosuoja-asetuksen soveltamisalan mukaiset toiminnat ja sen lisäksi tiettyjä poikkeuksia, kuten kansallisen turvallisuuden ja rikosasioissa tapahtuvan henkilötietojen käsittelyn. Tietosuojalaki on keskeinen osa lainsäädäntöä ja sitä sovelletaan Suomessa sijaitsevien rekisterinpitäjien toimintaan. Se myös määrittää, että Suomen lakia noudatetaan, jos rekisterinpitäjän toimipaikka sijaitsee Suomessa.[23] Rekisterinpitäjä voi olla henkilö, yritys, viranomainen tai muu vastaava taho, joka määrittelee henkilötietojen käsittelyn keinot. [24] Tietosuojalaki vaikuttaa laajasti julkishallinnon, yritysten ja yksittäisten kansalaistenkin toimintaan, varmistaen yksityisyyden suojan ja henkilötietojen turvallisen käsittelyn digitaalisessa ympäristössä.[25]

---

[20] Hoofnagle & muut 2019: s.72–73
[21] Suomen laki hakupalvelu 2016: I luku 1 artikla
[22] Tietosuojalaki 1050/2018
[23] Suomen laki hakupalvelu 2018: 1 luku 3 §
[24] Hanninen ja muut 2017: 3.1
[25] Finlex 2018: 2 luku 4 §

2.3 Työntekijöiden yksityisyydensuoja ja tarpeellisuusvaatimus työelämässä

Suomessa työelämän tietosuojakysymyksiä säätelee erityisesti laki yksityisyyden suojasta työelämässä eli Työelämän tietosuojalaki (YksTL 759/2004), joka myös täydentää EU:n yleisen tietosuoja-asetuksen vaatimuksia. Lain tarkoituksena on turvata työntekijöiden yksityisyydensuoja työsuhteen aikana ja määrittää, millä edellytyksillä työnantaja voi käsitellä työntekijöiden henkilötietoja. Työelämän tietosuojalaki asettaa erityisen tiukan tarpeellisuusvaatimuksen, jonka mukaan työnantaja saa käsitellä vain sellaisia henkilötietoja, jotka ovat välttämättömiä työsuhteen kannalta.[26]

2.4 Tietoturvan valvonta

Tietoturvallisuus on ollut osa yhteiskuntaa jo pitkään, mutta sen laajempi merkitys on noussut esiin vasta viime vuosikymmeninä. Suomessa nykyaikainen tietoturvallisuuden sääntely käynnistyi vuonna 1987 säädetyllä henkilörekisterilailla, joka toi esiin uuden oikeudellisen käsitteen, eli tietosuojan. Tietosuoja edellyttää toimiakseen vahvaa tietoturvaa, mutta pitkään tietoturva jäi sääntelyssä taka-alalle. Lainsäädäntö oli yleisluonteista ja käytännön toteutuksen kannalta riittämätöntä.[27]

Suomessa ei ole erillistä lakia, joka kattavasti määrittelisi käyttäjien tietoturvan velvoitteita ja oikeuksia. Lainsäätäjät ja organisaatiot eivät ole pitäneet erityistä tietoturvalakia välttämättömänä. Tämän sijaan tietoturvavelvoitteet on liitetty osaksi muita lainsäädännön osia. Vaikka tämä ratkaisu on katsottu perustelluksi, tekee se tietoturvan käytännön toteutuksesta monimutkaisempaa, sillä tietoturvanormit on hajautettu useisiin eri lakeihin.[28] Tietoturvasääntely on siis edennyt hitaasti ja usein vasta ongelmien paljastuttua. Käännekohtia ovat kuitenkin olleet keskeiset säädökset,

[26] Työ- ja elinkeinoministeriö 2019: 1–3
[27] Saarenpää ja Riekkinen 2023: 3.3.4.5
[28] Kinnunen 2015: s.84–85

kuten vuonna 1999 voimaan tullut henkilötietolaki, joka perustui EU:n henkilötietodirektiiviin, vuonna 2018 sovellettavaksi tullut EU:n yleinen tietosuoja-asetus (GDPR) sekä vuonna 2019 kehitetty tiedonhallintalaki, joka asetti vaatimuksia tietojärjestelmien suunnittelulle ja tietoaineistojen suojaukselle.[29]

Suomessa tietoturvan ohjaaminen ja valvonta on hajautettu useille viranomaisille ja toimielimille, jotka yhdessä muodostavat kattavan tietoturvaohjeistusten verkoston. Esimerkiksi Liikenne- ja viestintäministeriö, Valtiovarainministeriö sekä sisäasiainministeriö ovat keskeisiä toimijoita tietoturvan kehittämisessä. Tämän lisäksi Euroopan verkko- ja tietoturvavirasto (ENISA) sekä kansainvälinen standardisoimisjärjestö ISO tuovat omat standardinsa ja ohjeistuksensa, jotka vaikuttavat merkittävästi kansallisten säädösten sisältöön ja soveltamiseen.[30]

Euroopan unionin verkko- ja tietoturvavirasto (ENISA, European Network and Information Security Agency) perustettiin vuonna 2004 ja sen toiminta käynnistyi vuonna 2005. ENISA:n päätehtävänä on edistää korkeatasoista verkko- ja tietoturvaa Euroopan unionissa. Se pyrkii lisäämään tietoisuutta tietoturvaan liittyvistä ongelmista ja luomaan tietoturvakulttuurin, joka hyödyttää kansalaisia, kuluttajia, yrityksiä sekä julkisen sektorin organisaatioita. ENISA tukee Euroopan unionin politiikan ja lainsäädännön kehittämistä tarjoamalla neuvoja verkko- ja tietoturva-asioissa, kehittämällä valmiuksia jäsenvaltioissa sekä tukemalla yhteistyötä eri toimijoiden välillä. Virasto pyrkii luomaan yhteistyöetuja EU:n toimielinten välille erityisesti tietoverkkorikollisuuden ja yksityisyydensuojan alueilla.[31]

2.5 Tietosuojan erityisvaatimukset etätyössä

Työn tekeminen kodin kaltaisissa ympäristöissä lisää henkilötietojen käsittelyyn liittyviä riskejä, jonka takia etätyö asettaa erityisvaatimuksia tietosuojalle. GDPR:n periaatteet

[29] Saarenpää ja Riekkinen 2023: 3.3.4.5
[30] Kinnunen 2015: s.84
[31] EUR-Lex 2014: ENISA

kuten tietojen minimointi ja käsittelyn lainmukaisuus ovat erityisen tärkeitä etätyössä, jossa henkilötietojen käsittely voi ulottua yrityksen hallitsemien järjestelmien ulkopuolelle. Tietojen minimoinnin periaatteen mukaisesti työntekijöiden tulisi käsitellä vain välttämättömiä tietoja työtehtäviensä suorittamiseksi. Esimerkiksi henkilötietoihin pääsy rajoitetaan tiukasti ja vain niihin, jotka ovat olennaisia kyseisen työn suorittamisessa. GDPR:n mukainen vaatimus henkilötietojen asianmukaisesta suojauksesta korostuu etätyöympäristöissä, joissa tietojen suojaaminen on usein riippuvainen kotiverkkojen ja työntekijöiden omien laitteiden turvallisuudesta. Tähän liittyvät tekniset ja organisatoriset vaatimukset, kuten tiedon salaus ja pääsynhallinta ovat ratkaisevassa roolissa etätyön tietosuojan toteutumisessa.[32]

Henkilötietojen suojaaminen edellyttää etätyössä erityistä huomiota teknologian käyttöön ja tietojen käsittelyn tarkoituksenmukaisuuteen. Tietosuojaa koskevat vaatimukset tulisi rakentaa sen mukaan, millaisia riskejä ja haittoja tietojen käsittely aiheuttaa yksilöille. Etätyössä tämä tarkoittaisi esimerkiksi sitä, että työntekijöiden sijaintitietojen, viestinnän ja muiden työhön liittyvien tietojen tarpeellisuutta arvioitaisiin tarkasti. Riskiperusteinen lähestymistapa mahdollistaisi tietojen käsittelyn asianmukaisessa laajuudessa ja keskittyisi estämään tietojen tarpeettoman keräämisen ja väärinkäytön.[33]

[32] Hoofnagle & muut 2019: s.85–88
[33] Solove 2024: 4 A

3 Tietoturvahaasteet ja riskit

Tietoturvan päämääränä on suojata tiedon luottamuksellisuutta, eheyttä sekä saatavuutta. Tietoturvariskeillä viitataan niihin tilanteisiin, joissa nämä tekijät ovat vaarassa. Riskit voivat syntyä tahallisista teoista tai tahattomista vahingoista ja ne voivat johtaa taloudellisiin tappioihin kuten omaisuuden vahingoittumiseen, liiketoiminnan keskeytymiseen tai mainehaittoihin. Lainsäädännössä, kuten EU:n yleisessä tietosuoja-asetuksessa riski määritellään potentiaalisena haitallisena tapahtumana, joka uhkaa tietojärjestelmien turvallisuutta.[34]

Etätyön yleistyminen on tuonut mukanaan merkittäviä muutoksia tietoturvaan, kun perinteiset fyysiset turvatoimet kuten lukitut ovet ja vartiointi ovat väistyneet digitaalisten suojakeinojen tieltä. Nykyään palomuurit, tietoturvaprotokollat ja dataa seuraavat järjestelmät ovat muodostuneet keskeisiksi elementeiksi yritysten tietoturvan ylläpitämisessä. Digitaalinen viestintä ja videokokoukset mahdollistavat globaalin yhteydenpidon, mutta luovat myös uusia haavoittuvuuksia. Ne vaativat jatkuvaa huomiota ja päivitystä turvastrategioissa, jotta voidaan reagoida nopeasti muuttuviin ja kasvaviin uhkiin.[35] Etätyöskentely edellyttää, että työntekijät pääsevät käsiksi järjestelmiin kotoa käsin. Nämä järjestelmät käyttävät internet-yhteyksiä, jotka mahdollistavat pääsyn organisaatioiden palvelimille. Pienikin turvallisuusvirhe organisaation turvajärjestelmässä tai työntekijän toimesta voi katkaista nämä yhteydet ja vuotaa arkaluonteista tietoa vääriin käsiin.[36]

Organisaatioiden tietoturvahaasteet ovat kasvaneet kyberhyökkäysten myötä, minkä seurauksena erilaiset tietovuodot voivat johtaa merkittäviin taloudellisiin tappioihin sekä yritysten mainehaittoihin. Tiedon suojaaminen on monimutkaistunut sen myötä, kun työntekijät käyttävät työssään omia älylaitteitaan kuten matkapuhelimia ja tabletteja, jotka eivät ole organisaatioiden omistuksessa. Näiden laitteiden tietoturva

[34] Andersson 2018: 2–3.
[35] Wainwright ja muut 2024: s.251
[36] Vivekananth 2022: 2.

vaatii käyttäjien aktiivisia toimenpiteitä, sillä automaatio ei itsessään riitä takaamaan riittävää suojaa. Älylaitteet ovat myös alttiita viruksille ja muille haittaohjelmille, kun niihin ladataan kolmannen osapuolen sovelluksia. Lisäksi älylaitteiden pieni koko lisää katoamisen tai varastamisen riskiä. Näin ollen tietoturvauhkia voi syntyä huonosti suojattujen IT-järjestelmien, laitteiden ja ohjelmistojen lisäksi myös työntekijöiden tahallisten tai huolimattomien toimien seurauksena.[37]

3.1 Tyypilliset tietoturvariskit ja haasteet

3.1.1 Työntekijöiden omien laitteiden käyttö

Etätyön tekeminen kotona, työmatkat tai henkilökohtaisten laitteiden käyttö työssä eli BYOD (bring your own device) mahdollistavat työntekijöiden toiminnan seurannan perinteisen työpaikan ulkopuolella. Tämä ei kuitenkaan rajoitu pelkästään työtehtäviin, vaan voi ulottua myös henkilökohtaiseen elämään.[38] Työntekijöiden omien laitteiden käytön yleistyessä yrityksissä on tullut entistä tärkeämmäksi tunnistaa ja hallita siihen liittyviä tietoturvahaasteita. BYOD-käytäntö aiheuttaa huomattavan kasvun työntekijöiden lukumäärässä, jotka käyttävät omia mobiililaitteitaan työssään. BYOD-käytännön avulla organisaatiot antavat työntekijöiden yhdistää henkilökohtaiset laitteensa organisaation IT-järjestelmiin. Tämä käytäntö tarjoaa monia etuja kuten joustavuutta, mutta se aiheuttaa myös mahdollisia turvallisuusriskejä. Erityisesti laitteiden katoaminen tai varastaminen on merkittävä huolenaihe, sillä laitteet saattavat sisältää arkaluonteista tietoa. Kadonneet tai varastetut laitteet voivat joutua väärän henkilön haltuun ja tämä voi käyttää tallennettua tietoa väärin.[39]

3.1.2 Kotiverkkojen suojaus ja heikot salasanat

Kotiverkkojen turvallisuus on tärkeä tietoturvan osa-alue, sillä jokainen ICT-laitteiden käyttäjä voi olla potentiaalinen tietoverkkorikoksen uhri. Erityisesti kodin nettiyhteys on

[37] Niemi 2018: s.416
[38] Korpisaari, Pitkänen, Warma-Lehtinen 2022: s.709
[39] Drew 2012: s.44–46

suojelun kannalta keskeisin. Väärinkäytön kohteeksi joutunut kotiverkon reititin voi mahdollistaa laajan tietoliikenteen seurannan ja tulla käytetyksi palvelunestohyökkäyksissä laitteen hallinnan kaappauksen yhteydessä.[40]

Työntekijät, jotka työskentelevät kotona tarvitsevat internet-yhteyden yhdistääkseen laitteensa organisaation palvelimiin. Työntekijät käyttävät usein kotiverkkoja sekä julkisia suojaamattomia yhteyksiä, jotka altistavat heidät haavoittuvaisiksi erilaisille verkkouhille ja pahimmassa tapauksessa vuotaa henkilökohtaisia sekä luottamuksellisia tietoja. Suojaamaton tieto voidaan helposti kaapata ja se voi päätyä rikollisten käsiin. Kotona olevat Wi-Fi-verkot ovat helpompi kohde hakkerointiin kuin tyypilliset organisaatioverkot. Ne käyttävät harvemmin palomuureja ja luottavat todennäköisemmin edullisiin kuluttajatason internet-reitittimiin, jotka saattavat olla heikommin suojattuja.

Työntekijöiden työskentely kotona tekee salasanoista vieläkin haavoittuvampia. Noin 75 % kotona työskentelevistä henkilöistä käyttää samoja salasanoja useimmissa verkkopalveluissa. Tämä voi aiheuttaa haitallisia seurauksia organisaatioille. Help Net Securityn tekemän tutkimuksen mukaan noin 42 % työntekijöistä pitää edelleen salasanojaan kirjoitettuna paperille, 34 % tallentaa ne älypuhelimiinsa, kun taas noin 27 % työntekijöistä tallentaa salasanansa tietokoneisiin.[41]

3.1.3 Tiedonkalastelu

Phishing eli tiedonkalastelu on kyberrikollisuuden muoto, jossa huijarit pyrkivät tarkkailemaan käyttäjien salasanoja ja käyttäjätunnuksia väärennetyillä verkkosivuilla. Kohteina ovat usein suosittujen verkkopalveluiden, kuten eBayn, Amazonin, Twitterin ja Gmailin käyttäjätiedot. Vaikka tämä saattaa vaikuttaa harmittomalta niin seuraukset voivat olla sitäkin vakavampia. Rikolliset voivat esimerkiksi tilata tuotteita henkilön nimissä tai käyttää kaapattua sähköpostitiliä huijausviestien lähettämiseen.

[40] Järvinen ja Rousku 2017: 2.
[41] Vivekananth 2022: 2.

Tiedonkalasteluyritykset alkavat yleensä sähköpostiviestillä, joka näyttäisi tulevan luotettavalta taholta, kuten pankilta tai tunnetulta yritykseltä. Viesti saattaa kehottaa kirjautumaan palveluun jonkin tekosyyn vuoksi ja sisältää linkin, joka ohjaa käyttäjän väärennetylle sivustolle. Tämä sivusto on usein tarkka kopio aidosta palvelusta, mutta se on perustettu rikollisten hallinnoimalle palvelimelle. Kun käyttäjä syöttää tunnuksensa sivustolle, ne päätyvät suoraan rikollisten haltuun.[42]

3.1.4 Haittaohjelmat, Yksityisyysriskit ja teknologian haavoittuvuus

Haittaohjelmat ovat ohjelmistoja, jotka ovat suunniteltu vahingoittamaan tietokonetta pyytämättä käyttäjän lupaa. Ne voivat päästä järjestelmään monin tavoin, esimerkiksi sähköpostin liitetiedostojen tai haavoittuvuuksia sisältävien verkkosivujen kautta. Kun haittaohjelma on päässyt laitteeseen, se voi aiheuttaa monenlaisia ongelmia. Erityisen haastavia ovat tilanteet, joissa haittaohjelma leviää koko verkkoon, mikä voi johtaa laajamittaisiin tietoturvaloukkauksiin. Tällaiset voivat johtaa arkaluonteisen tiedon vuotamiseen, identiteettivarkauksiin ja taloudellisiin menetyksiin. Jos työtietokoneeseen asennetaan ylimääräisiä sovelluksia, apuohjelmia tai selainlaajennuksia, lisää se merkittävästi haittaohjelmien tartuntapintaa. Mitä enemmän ohjelmia koneella on, sitä suurempi riski on siihen, että haittaohjelmat löytävät ja hyödyntävät niiden heikkouksia. Microsoft Officen toimistosovellusten työtiedostot ovat yksi suosituimmista haittaohjelmien levityskanavista, sillä tiedostot ovat yleisesti käytössä kaikenlaisissa organisaatioissa ja vastaavat sovellukset löytyvät melkein jokaisen työntekijän tietokoneilta.

Kohdistetut hyökkäykset, eli APT (Advanced Persistent Threats) ovat erittäin määrätietoisia ja strategisesti toteutettuja tietoturvaloukkauksia. Nämä hyökkäykset suunnitellaan erityisesti tiettyä organisaatiota vastaan hyödyntämällä useita tiedonlähteitä kuten julkisia tietoja, sosiaalista mediaa ja organisaation sisäisiä

[42] Järvinen ja Rousku 2017: 3.

tietoturvaohjeita. Hyökkääjät perehtyvät organisaation rakenteeseen, sen keskeisiin henkilöihin sekä käytössä oleviin turvajärjestelmiin kuten virustorjuntaohjelmistoihin. Hyökkääjät muokkaavat tai kehittävät haittaohjelmia, jotka on suunniteltu välttämään havaitsemista ja lähettävät niitä kohdehenkilöille sähköpostien kautta niin, että viestit näyttävät tulevan luotettavilta lähettäjiltä. Haittaohjelmat saattavat olla peitettyinä työhön liittyviksi dokumenteiksi tai verkkosivuston linkiksi. Kun kyseinen tiedosto tai linkki avataan, haittaohjelma aktivoituu. Se alkaa seuraamaan verkon liikennettä ja etsimään hyödynnettäviä tietoja. Haittaohjelmalla voi olla myös etäkäyttöominaisuuksia, jotka mahdollistavat hyökkääjille suoran pääsyn organisaation verkkoon. APT-hyökkäykset kohdistetaan usein suuriin yrityksiin ja hallinnollisiin organisaatioihin.[43]

Henkilötietojen tietoturvaloukkauksella viitataan tilanteisiin, joissa henkilötietoja on siirretty, tallennettu tai muuten käsitelty, jonka seurauksena tiedot ovat vahingossa tai laittomasti tuhoutuneet, kadonneet, muuttuneet, niitä on jaettu luvattomasti tai niiden suoja on muutoin murtunut.[44]

Laajat käyttöoikeudet ja puutteellinen suojaus kehittyneitä verkkohyökkäyksiä vastaan pahentavat merkittäviä tietoturvaongelmia, joita etätyössä yleisesti käytettävät VPN-teknologiat aiheuttavat. Perinteiset VPN-ratkaisut antavat käyttäjille usein laajan pääsyn verkkoon tunnistautumisen jälkeen, mikä saattaa altistaa tärkeät liiketoimintatiedot ja järjestelmät merkittäville tietoturvauhkille. Lisäksi VPN-yhteydet voivat aiheuttaa huomattavia viiveitä sekä suorituskykyongelmia, mikä saattaa heikentää liiketoiminnan tehokkuutta ja hidastaa tärkeiden toimintojen sujuvuutta.[45]

Langattomat näppäimistöt ovat mukavia käyttää ja ne tekevät työtilasta siistejä, mutta ne sisältävät myös merkittäviä tietoturvariskejä. Näppäimistöt, jotka lähettävät tietoa infrapunan tai radiotaajuuksien avulla ovat alttiita tietoturvariskeille, sillä ne saattavat

[43] Järvinen ja Rousku 2017: 3.
[44] Hanninen ja muut 2017: 2.14
[45] Zohaib & muut 2024: 1.

lähettää näppäinpainalluksia ilman salausta. Tämä tekee niistä helpon kohteen, jolloin on mahdollista saada jopa sadan metrin päästä näppäimistön syötteet. Bluetooth-näppäimistöt tarjoavat parempaa turvallisuutta salauksen ansiosta, mutta niihinkin liittyy riskejä. Ne voidaan yhdistää huomaamatta toiseen laitteeseen, mikä voi johtaa tietojen vuotamiseen. Myös tietokoneiden kameroita käytetään laajalti videopuheluihin, mutta ne voivat olla alttiita vakoilulle. Erilaiset haittaohjelmat voivat ottaa kameran haltuunsa ja mahdollistaa käyttäjän salakatselun. Tämä voi paljastaa henkilökohtaisia tietoja kuten salasanoja.[46]

3.2 Tietosuojan ja tietoturvan toteutuminen käytännön tilanteissa

3.2.1 Sijaintitietotoiminnon käyttö työntekijöiden kannettavissa tietokoneissa

Etätyössä, jossa työntekijät käyttävät työvälineitä organisaation ulkopuolella korostaa tarvetta huolehtia paitsi tietoturvan teknisestä toteutuksesta myös työntekijöiden yksityisyyden suojasta. Windows 10 -käyttöjärjestelmän sijaintitietotoiminnon käyttö Pohjois-Savon sairaanhoitopiirin työntekijöiden kannettavissa tietokoneissa tarjoaa konkreettisen esimerkin tietosuojan ja tietoturvan sääntelyn toteutumisesta etätyössä. Tapauksessa korostuvat erityisesti tietosuojalainsäädännön vaatimukset kuten henkilötietojen minimointi ja oletusarvoinen tietosuoja, sekä työnantajan vastuu työntekijöiden yksityisyyden suojasta teknisiä ratkaisuja valittaessa.

Tapauksessa todettiin, että työntekijöiden tietokoneissa oli oletusasetuksena päällä sijaintitietotoiminto, jota työntekijät eivät voineet itse poistaa käytöstä. Vaikka organisaatio ei ollut käyttänyt sijaintitietoa mihinkään, sijaintitietojen kerääminen ilman lainmukaista perustetta rikkoi sekä EU:n yleisen tietosuoja-asetuksen (GDPR) tietojen minimoinnin ja oletusarvoisen tietosuojan periaatteita, että Suomen kansallisen työelämän tietosuojalain tarpeellisuusvaatimusta. Sijaintitietojen kerääminen ei ollut välttämätöntä työntekijöiden työtehtävien hoitamiseksi, eikä tietojen käsittelylle ollut olemassa lainmukaista perustetta. Tämä rikkoi työnantajan

[46] Järvinen ja Rousku 2017: 4.

velvollisuutta varmistaa, että henkilötietojen käsittely tapahtuu lain vaatimusten mukaisesti.

Tapaus havainnollistaa, miten teknisten järjestelmien oletusasetukset voivat aiheuttaa tietosuojaongelmia erityisesti etätyössä. Etätyöympäristössä yksityisyys saattaa vaarantua erityisesti silloin, kun sijaintitietoja yhdistetään kolmansien osapuolten järjestelmiin kuten tässä tapauksessa sijaintitietoja lähetettiin sijaintipalveluntarjoajalle Microsoftille. Vaikka tietojen käsittelyssä pyrittiin anonymisointiin, niiden yhdistely muihin tietoihin voi mahdollistaa työntekijöiden epäsuoran tunnistamisen.

Työnantajan tulisi kiinnittää erityistä huomiota laitteiden teknisiin oletusasetuksiin jo ennen niiden käyttöönottoa. Tämä edellyttää teknisten toimintojen yksityiskohtaista arviointia sekä tiivistä yhteistyötä järjestelmätoimittajien ja muiden palveluntarjoajien kanssa, jotta henkilötietojen tarpeeton kerääminen voitaisiin estää. Lisäksi henkilöstön kouluttaminen tietosuoja- ja tietoturvakäytännöistä on tärkeää, jotta työntekijät ymmärtävät tietosuojaan liittyvät riskit ja voivat tarvittaessa hallita laitteidensa yksityisyysasetuksia.[47]

3.2.2 Tietoturvaloukkaus ja rekisteröidyn oikeuksien suojaaminen

KHO: 2022:131 tapaus antaa näkökulmaa siihen, miten tietoturvaloukkaukset vaikuttavat rekisteröityjen henkilöiden oikeuksiin ja vapauksiin etätyöympäristössä, jossa tietoturvahaasteet ovat entistä merkittävämpiä. Asianajotoimiston palveluksessa olevan henkilön sähköpostitunnukset joutuivat kalastelusähköpostin kautta ulkopuolisen tahon haltuun. Kyseinen taho oli päässyt käsiksi sähköpostitunnuksiin noin kahdeksi vuorokaudeksi. Tietoturvaloukkauksen seurauksena arviolta noin 100–200 henkilötunnusta, 250–500 osoitetta sekä 2000–2500 muita henkilötietoja päätyi ulkopuolisen käsiin.

[47] Finlex 2022, Tietosuojavaltuutetun ratkaisu EU:n yleisen tietosuoja-asetuksen, rikosasioiden tietosuojalain ja henkilötietolain tulkinnasta

Korkein hallinto-oikeus (KHO) totesi, että vaikka ei ollut varmuutta siitä, kuinka laajasti tietoja oli hyödynnetty, oli kuitenkin selvää, että ulkopuolisella taholla oli ollut pääsy suureen määrään henkilötietoja, jotka mahdollistivat identiteettivarkauden. Tämä nosti esiin henkilötietojen käsittelyn korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille tietosuoja-asetuksen 34 artiklan 1 kohdassa tarkoitetulla tavalla. Tapaus korostaa, että tietoturvaloukkauksesta ilmoittaminen rekisteröidylle on tärkeä toimenpide, joka vaaditaan EU:n yleisen tietosuoja-asetuksen (GDPR) mukaan, kun loukkauksen seurauksena on todennäköisesti korkea riski rekisteröidyn oikeuksille. Tietosuojavaltuutettu määräsi asianajotoimiston ilmoittamaan tietoturvaloukkauksesta rekisteröidyille, joilla oli korkea riski joutua identiteettivarkauden kohteeksi tai joiden luottamuksellisia tietoja oli paljastunut ulkopuolisille.

Tapaus osoittaa, että organisaation tulee arvioida huolellisesti käyttämiensä järjestelmien tietoturvariskit ja varmistaa, että kaikki tietosuojalainsäädännön vaatimukset täyttyvät etenkin etätyöympäristössä. Tietoturvaloukkauksista tiedottaminen on oleellinen osa riskien hallintaa ja se auttaa suojaamaan rekisteröityjen henkilöiden oikeuksia etätyössä, jossa tietoturvauhat voivat olla monimutkaisempia ja vaikeammin hallittavia.[48]

[48] Edilex, KHO:2022:131

4 Etätyön tietoturvakäytännöt ja teknologiset ratkaisut

4.1 Hyvät käytännöt tietoturvan varmistamiseksi

Tietoturvallisuus on olennainen osa organisaation toimintaa. Sen vaatimukset muodostuvat monista tekijöistä kuten lainsäädännöstä, toimialan vaatimuksista, asiakassopimuksista ja tietoturvariskeistä. Työnantajan vastuulla on arvioida ja hallita riskit sekä tarjota työntekijöille selkeät ohjeet laitteiden ja palveluiden turvalliseen käyttöön. Tietoturvan laiminlyönti voi heikentää organisaation mainetta ja taloudellista tilannetta, jos tiedon saatavuus tai luottamus organisaatioon kärsii. Tietoturvan tulisi tukea liiketoimintaa, ei hankaloittaa sitä. Jos tietoturvatoimet koetaan haittaavan työtä, niitä kannattaisi tarkastella sekä mahdollisesti uudistaa käytössä olevia turvamekanismeja.[49]

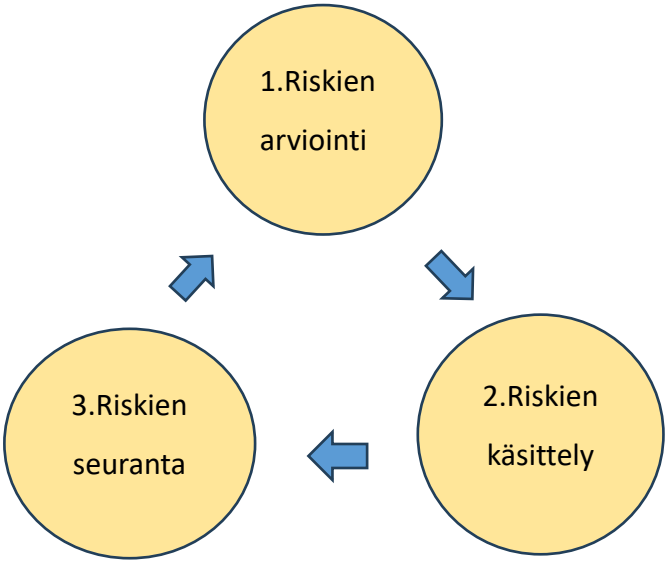
Hyvä riskienhallinta on olennainen osa tietoturvallisuuden ylläpitoa ja kehitystä organisaatiossa. Laaja-alainen tietoturva edellyttää, että organisaatio noudattaa selkeitä prosesseja ja viitekehyksiä, jotka tukevat riskienhallintaa ja varmistavat säädösten ja toimialavaatimusten noudattamisen. Riskien hallintaan voidaan hyödyntää esimerkiksi Katakri 2015 -viitekehystä, joka tarjoaa valmiita malleja riskien arviointiin, hallintaan ja dokumentointiin. Säännöllinen riskienarviointi auttaa pitämään turvatoimet ajan tasalla.

Riskienhallinta ei ole vain reaktiivista, vaan sen tulisi olla ennakoivaa ja joustavaa, sopeutuen jatkuvasti muuttuviin olosuhteisiin ja teknologisiin innovaatioihin. Tämä tarkoittaa käytännössä sitä, että turvatoimet kuten salasanasuojaukset, tietoliikenteen salaaminen ja pääsynvalvonta tulisi suunnitella sekä toteuttaa niin, etteivät ne haittaa työntekoa tai liiketoiminnan sujuvuutta. Viitekehysten avulla organisaatiot voivat myös varmistaa, että riskienhallintatoimet ovat linjassa kansainvälisten standardien ja

[49] Järvinen ja Rousku 2017: 1.

käytäntöjen kanssa, mikä edistää luottamusta ja turvallisuutta. Näin turvatoimet eivät hankaloita työskentelyä vaan tukevat sitä.[50]

Valtiovarainministeriön julkaisemat riskienhallinnan ja sähköisen asioinnin tietoturvallisuusohjeet tukevat julkishallinnon tietoturvaprosesseja ja edistävät sähköisten palveluiden turvallista kehittämistä. Ohjeistus kannustaa organisaatioita hyödyntämään ISO 31000 -standardia riskienhallinnan perustana, mikä auttaa ylläpitämään tietoturvan luotettavuutta. Se tarjoaa myös käytännön työkaluja, kuten Excel-pohjan riskien arviointiin. Ohjeiden avulla tietoturva voidaan huomioida jo suunnitteluvaiheessa, mikä parantaa organisaation kykyä vastata muuttuviin tietoturvahaasteisiin ja -uhkiin tehokkaasti.[51] Kun yritykset tunnistavat tietoturvaan kohdistuvat uhat, ne voivat tehokkaasti parantaa tietoturvansa tasoa.[52]



Kuva 1. Riskienhallinnan vaiheet (Andersson 2024: 4.2.2)

Riskien arviointi on prosessi, jossa organisaatio tunnistaa potentiaaliset haavoittuvuudet ja uhkat, jotka voivat vaikuttaa sen toimintaan. Arviointi alkaa toimintaympäristön määrittelystä: laaditaan riskienhallintapolitiikka, tunnistetaan

[50] Andersson 2018: 2.
[51] Valtiovarainministeriö 2017
[52] Ratsula 2021: 3.

keskeiset muuttujat ja määritellään riskien arviointikriteerit. Tämän jälkeen arviointi jaetaan kolmeen päävaiheeseen. Ensimmäisenä ovat riskien tunnistaminen, missä selvitetään, mitkä tekijät voivat potentiaalisesti aiheuttaa haittaa organisaatiolle. Toisena on riskianalyysi, jossa arvioidaan tunnistettujen riskien todennäköisyyttä ja niiden mahdollisia vaikutuksia, jolloin voidaan arvioida riskien suuruutta. Kolmantena riskien merkityksen arviointi, missä puolestaan määritellään kuinka kriittisiä tunnistetut riskit ovat organisaation toiminnalle ja mitä hallintakeinoja voidaan käyttää niiden hallitsemiseksi. Koska toimintaympäristö ja ulkoiset tekijät muuttuvat jatkuvasti, on tärkeää, että riskien arviointi on jatkuva prosessi.[53]

Riskien käsittely seuraa arviointia. Sen tarkoituksena on toteuttaa toimenpiteitä, joilla hallitaan, pienennetään tai rajoitetaan tunnistettuja riskejä. Näitä hallintakeinoja ovat mitigointi: riskin merkityksen tai suuruuden pienentäminen tai poistaminen: vaikka riskin kokonaisvaltainen poistaminen ei usein ole mahdollista, voidaan sen mahdollisia seurauksia ennakoida ja lieventää. Välttäminen: riskialttiista toiminnasta luopuminen ja siirtäminen: riskin jakaminen toisen osapuolen tai osapuolten kanssa, sekä hyväksyminen: riskin hyväksyminen, jos se on hallittavissa tai siihen liittyvät hyödyt katsotaan merkittävämmiksi kuin haitat. On kuitenkin tärkeää ymmärtää, että jokainen hallintakeino voi luoda uusia riskejä.

Riskien seuranta varmistaa, että toteutetut toimenpiteet ovat tehokkaita ja pysyvät ajan tasalla. Seurantaprosessi alkaa käsittelyn jälkeen ja sisältää seuraavat osa-alueet:

1. Toimintaympäristön ja riskikriteerien tarkastelu: Arvioidaan, miten ulkoiset ja sisäiset tekijät vaikuttavat tunnistettuihin riskeihin.
2. Dokumentointi: Kaikki riskienhallintaprosessin vaiheet, kuten tunnistetut riskit ja toteutetut toimenpiteet tulee dokumentoida huolellisesti. Dokumentointi ei ainoastaan todista organisaation noudattavan lainsäädännöllisiä vaatimuksia,

[53] Andersson, J. 2024: 4.2.2

vaan myös mahdollistaa kustannusten seurannan ja oppimisen aiemmista toimenpiteistä.

3. Jatkuvuus ja ajantasaisuus: On tärkeää, että riskienhallinta on jatkuvaa, ja että hallintatoimenpiteet päivitetään säännöllisesti. Tämä takaa, että toimenpiteet ovat riittäviä suhteessa tunnistettuihin riskeihin. Nopeasti muuttuvilla aloilla, kuten kyberturvallisuudessa tämä on erityisen tärkeää.[54]

Työntekijöille myönnettävät perusoikeudet ovat keskeinen turvakeino tietoturvan hallinnassa, sillä sen avulla minimoidaan vahinkojen riski. Yleensä työntekijöille annetaan vain rajoitetut käyttöoikeudet, mikä estää heitä tekemästä vahingossa muutoksia järjestelmän asetuksiin. Etätyöntekijöille suositellaan myös erillisen ylläpitäjätunnuksen luomista, jotta päivittäinen käyttö rajoittuu perusoikeuksiin, mikä suojaa koneita haittaohjelmilta. Perusoikeuksien avulla käyttäjät voivat suorittaa perustoimintoja kuten käyttöjärjestelmän päivityksiä ja tulostimen asennuksia, mutta eivät voi muokata verkkoasetuksia tai hallita muita käyttäjätilejä, mikä vähentää haitallisten ohjelmien aiheuttamia riskejä.[55]

4.1.1 Organisaation ja työntekijöiden roolit ja vastuut

Työympäristöt ovat usein hajautettuja ja monimuotoisia, mikä tarkoittaa myös sitä, että etätyön erityispiirteet asettavat työntekijöille korostuneen vastuun tietoturvan ylläpitämisestä. Työntekijöiden henkilökohtaiset asenteet, sosiaalinen paine ja koettu hallinnan tunne vaikuttavat merkittävästi heidän halukkuuteensa noudattaa organisaatioiden tietoturvaohjeita. Tämä korostaa sitä, että organisaatioiden tulisi tarjota selkeitä ja helposti omaksuttavia tietoturvaohjeita, mutta luoda samalla työympäristö, jossa työntekijät tuntevat olevansa motivoituneita ja päteviä suojaamaan organisaation tietoja. Näiden tekijöiden huomioiminen voi auttaa minimoimaan

[54] Andersson, J. 2024: 4.2.2
[55] Järvinen ja Rousku 2017: 4.

tietoturvariskejä etätyössä ja vahvistaa työntekijöiden roolia osana organisaation tietoturvastrategiaa.[56]

Hietala & muut (2024) korostavat, että työnantajan vastuu ulottuu myös etätyöntekijöiden työturvallisuuden ja tietoturvan varmistamiseen. Työturvallisuuslain 5 § mukaan työnantajan tulee huolehtia siitä, että työolosuhteet ovat turvalliset, vaikka työntekijä työskentelisi kotona tai muussa valitsemassaan paikassa. Tämä tarkoittaisi sitä, että työnantajan tulisi vastata etätyössä käytettävien työvälineiden toimivuudesta ja tietoturvasta, mutta kotona tehtävän työn fyysinen valvonta on kuitenkin rajallista.[57]

Etätyössä työntekijän oma vastuu korostuu erityisesti tietoturvakäytäntöjen noudattamiseen. Työntekijän odotetaan käyttävän työvälineitä ja tietojärjestelmiä ohjeiden mukaisesti sekä varmistavan, että esimerkiksi kotiverkko on riittävästi suojattu. Näin työnantajan ja työntekijän roolit täydentävät toisiaan, mikä on keskeistä sekä fyysisen turvallisuuden että tietoturvan ylläpitämiseksi hajautetuissa työympäristöissä.[58]

4.1.2 Turvallisuusohjeet ja työntekijöiden koulutus

On olennaisen tärkeää ohjeistaa henkilöstöä tietoturva-asioissa. Ohjeistuksen tulisi aina olla kirjallisessa muodossa, jotta siihen on mahdollista tarpeen vaatiessa palata. Ohjeistuksessa voidaan muun muassa määritellä selkeästi, mitkä laitteet, verkot sekä ohjelmat ovat työntekoon hyväksyttyjä sekä minkälaisissa tiloissa kyseisiä laitteita on luvallista käyttää.[59]

Työntekijöiden ohjeistuksen lisäksi keskeisessä roolissa ovat myös erilaiset tietoturvaohjeistukset ja -standardit, jotka tukevat organisaation turvallisuusjohtamisen käytäntöjä. Esimerkiksi ISO/IEC 27002 -standardi tarjoaa yleisiä

[56] Godlove 2012: 5.2: s.227
[57] Työturvallisuuslaki 738/2002
[58] Hietala & muut 2024: s.187–191
[59] Edilex, Karvinen 2021: webinaari

suuntaviivoja tietoturvan hallinnalle auttaen organisaatioita kehittämään tehokkaita toimintatapoja ja lisäämään luottamusta organisaatioiden välillä. Nämä standardit varmistavat, että tietoturvatoimenpiteet ovat yhdenmukaisia ja tarpeeksi kattavia, minkä tärkeys korostuu etätyöympäristössä.[60]

Työssä oppiminen on jatkuva prosessi, joka vaatii merkittävästi motivaatiota erityisesti, kun kyseessä on tietoturvallisuuden noudattaminen etätyöympäristössä. Motivaation ylläpitäminen on oleellista, sillä se tukee työssä oppimista ja on olennainen osa työelämässä toimimista ja toiminnan ohjaamista. Yritysten tietoturvaohjeiden jatkuva päivittäminen ja noudattaminen on välttämätöntä, joten työntekijöiltä vaaditaan jatkuvaa motivaatiota pysyä ajan tasalla tietoturvakäytäntöjen suhteen. Tässä yhteydessä yksilön tarpeiden, kuten turvallisuuden ja fyysisten tarpeiden tyydyttäminen on tarpeellista, jotta oppimista voi tapahtua ja työntekijä voi keskittyä työhönsä. Työntekijöiden koulutuksessa tulisi näin ollen keskittyä tietoturvaosaamisen kehittämisen lisäksi myös motivaation ylläpitämiseen ja vahvistamiseen, mikä edistää tietoturvaohjeistusten tehokasta noudattamista.[61]

Työntekijöiden tietoturvatietoisuus sekä osaaminen ovat suuressa roolissa nykypäivänä, eikä pelkkä teknologinen suojaus kuten palomuurit ja salaukset riitä. CAT-kehys (Cybersecurity Awareness and Training Framework) tarjoaa käytännönläheisen mallin organisaatioille työntekijöiden tietoturvatietoisuuden vahvistamiseksi. Tämän kehyksen merkitys on korostaa ennaltaehkäisevän koulutuksen merkitystä, jotta työntekijöillä on paremmat lähtökohdat tunnistaa sekä välttää tietoturvariskejä. Kehyksen mukaan tarvitaan säännöllisiä harjoituksia, joiden avulla työntekijät voivat kokeilla ja kehittää kyvykkyyksiään tosielämän kaltaisissa tilanteissa turvallisuusohjeiden lisäksi.

CAT-kehyksen mukaan turvallisuusohjeiden tulisi olla selkeitä, helposti ymmärrettäviä ja käytännönläheisiä, jotta ne tukevat työntekijöitä arjen tilanteissa. Näitä ohjeita

[60] Kinnunen, N. 2015: s.87–88
[61] Kinnunen, N. 2015: s.25–28

täydentävät jatkuva viestintä ja tuki, jotka pitävät tietoturvan esillä organisaation arjessa. CAT-kehyksen ideana on, että tietoturva ei ole vain teknologian tai IT-osaston vastuulla, vaan jokainen työntekijä on tärkeä osa organisaation tietoturvan suojelua. Sen tavoitteena ei ole vain riskien tunnistaminen, vaan myös työntekijöiden rohkaiseminen toimimaan aktiivisesti tietoturvan hyväksi. Tämä tarkoittaa sitä, että organisaatiot eivät ainoastaan ennaltaehkäise tietoturvaloukkauksia, vaan myös varmistavat, että työntekijät voivat toimia itsenäisesti tietoturvatilanteissa.[62]

4.2 Teknologiset ratkaisut

Nykyään etätyöskentelyä tukevat teknologiat ovat monipuolisia ja helposti saavutettavia. Työskentelyyn voidaan hyödyntää lukuisia työkaluja, kuten pikaviestivälineiden ja videokokouspalveluiden kaltaisia viestintävälineitä, pilvipalveluita, kalenterisovelluksia, sähköposteja ja ohjelmistoja palveluna eli SaaS (software as a service). Näiden välineiden laaja tarjonta ei kuitenkaan aina helpota valintaprosessia, vaan asettaa organisaatiot tilanteeseen, jossa täytyy tarkasti arvioida mitkä teknologiat ja järjestelmät vastaavat parhaiten työn tarpeita.

Teknologisten ratkaisujen käyttöönotossa tietoturva on keskeisessä roolissa. Tietoturvaohjeistuksilla ja työntekijöiden opastuksella voidaan ehkäistä tietoturvaloukkauksia. Esimerkiksi laitteiden ja ohjelmistojen säännöllinen päivittäminen vähentää tietoturvaloukkauksien riskiä. Lisäksi työnantajien tulisi ohjeistaa työntekijöitä välttämään suojaamattomien tai jaettujen verkkojen käyttöä ja suosimaan esimerkiksi oman puhelimen verkkoyhteyksiä liikkuvassa työssä. Työntekijöiden on tärkeää käyttää vain työnantajan hyväksymiä työvälineitä ja välttää omien laitteiden käyttöä, ellei sitä ole erikseen sallittu ja ohjeistettu. Näillä toimenpiteillä voidaan minimoida tietoturvariskejä ja suojautua mahdollisilta tietomurroilta.[63]

---

[62] Hijji ja Alam 2022: s.1–2, s.7–9 ja s.10–12
[63] Vilkman, U. 2016: s.185–187

Etätyössä käytettävät teknologiset ratkaisut voivat lisätä tietosuojan ja tietoturvan riskejä, jos tietojen käyttöä ei suunnitella huolellisesti. Etätyöympäristössä henkilötiedot voivat paljastua huomaamatta. Tämän vuoksi organisaatioiden tulisi käyttää anonymisointia, pseudonymisointia ja muita teknologisia keinoja minimoidakseen riskit.[64] Pseudonymisoinnissa henkilötiedot korvataan tunnisteilla kuten koodeilla, mutta henkilö on edelleen tunnistettavissa lisätietojen avulla. Pseudonymisoidut tiedot ovat yhä henkilötietoja, ja niitä koskee tietosuojalainsäädäntö, kun taas anonymisoinnissa henkilötiedot muokataan niin ettei henkilöä voi enää tunnistaa, eikä tunnistaminen ole palautettavissa. Anonymisoituja tietoja ei pidetä henkilötietoina, eikä niihin sovelleta tietosuojasäädäntöä.[65]

Tietojen suojaamista tukee säännöllinen riskien arviointi, jonka avulla voidaan tunnistaa tietoturvan ja tietosuojan mahdolliset haavoittuvuudet etätyössä. Organisaation tulisi huolehtia siitä, että organisaatioilla on käytössä tehokkaat pääsynhallintajärjestelmät, jotka takaavat, että työntekijät pääsevät käsiksi vain työtehtäviensä kannalta olennaisiin tietoihin. Tietojen salaaminen ja muiden teknisten suojakeinojen, kuten monivaiheisen tunnistautumisen käyttöönotto tukevat tietosuojan ylläpitämistä etäyhteyksillä.[66]

Käyttäjätunnukset ja salasanat ovat olennaisia tietoturvaan liittyviä elementtejä, jotka varmistavat pääsyn tietoihin vain niihin oikeutetuille käyttäjille. Tietoturvan parantamiseksi kaksivaiheinen tunnistautuminen on yleistynyt, jossa käyttäjän on syötettävä salasanan lisäksi erillinen vahvistuskoodi, jonka voi saada esimerkiksi tekstiviestillä tai sähköpostitse. Lisäksi on olemassa tunnistautumissovelluksia, jotka tarjoavat samankaltaisia koodeja. Organisaatiot voivat tarjota salasanojen hallintaohjelmia, kuten F-Securen tai KeePass:in tuotteita ja käyttää kertakirjautumisjärjestelmiä, jotka vähentävät tarvetta salasanakyselyille. Myös vieraissa tiloissa työskennellessä on tärkeää suojata salasanat valvontalaitteiden

[64] Solove 2024: 2 A
[65] Tietosuojavaltuutetun toimisto: Pseudonymisoidut ja anonymisoidut tiedot
[66] Hoofnagle & muut 2019: s.85–88

lähettyvillä ja varoa keskustelemasta arkaluonteisista asioista, koska on mahdollista, että ympäristössä on nauhoittavia laitteita.[67]

Työntekijöiden henkilökohtaisten laitteiden käyttö tuo omat riskinsä. Yritykset voivat vähentää riskejä vaatimalla lukituskoodien käyttöä. Sillä varmistetaan, että vain valtuutetut käyttäjät pääsevät käsiksi laitteisiin. Lisäksi laitteilla työdatan salaus suojaa arkaluontoista tietoa, mikäli laite joutuisi vääriin käsiin. Etäpyyhkäisyn mahdollisuus antaa yrityksille valtuudet poistaa kaikki tiedot kadonneesta laitteesta, mikä minimoi tietovuodon riskiä.

Kotiverkkojen osalta, joissa turvallisuus voi olla heikompi kuin yrityksen tiukasti valvotuissa IT-ympäristöissä, on tärkeää soveltaa turvatoimenpiteitä johdonmukaisesti. Kotona työskentelevien työntekijöiden tulisi varmistaa, että heidän henkilökohtaiset verkkonsa ovat suojattuja vahvoilla salasanoilla, ja että he käyttävät VPN-yhteyksiä aina kun mahdollista. Tämä lisää turvallisuutta, suojellen sekä yrityksen että henkilön henkilökohtaisia tietoja.[68]

4.2.1 Tietoturvan hallintaratkaisut

Älylaitteita voidaan hallinnoida erilaisin keinoin ja sitä voidaan kutsua nimellä Mobile Device Management (MDM). MDM ratkaisujen avulla voidaan pakottaa salasanojen käyttö, päivittää ohjelmistot automaattisesti, seurata laitteiden käyttöä ja poistaa etänä tietoja tai sovelluksia, mikä parantaa sisäisen valvonnan kontrollia. Tämä on apukeino organisaatioille tunnistaa sekä hallinnoida arvokasta tietoa sekä reagoida nopeasti mahdollisiin tietoturvaloukkauksiin.[69]

Kauppakamarin julkaisema Tietoturvaopas yrityksille tarjoaa kuusi keskeistä käytännöntoimenpidettä, joita yritykset voivat hyödyntää vähentääkseen

[67] Järvinen ja Rousku 2017: 5.
[68] Drew 2012: s.44–46
[69] Niemi 2018: s.416–417

tietoturvariskejä. Ensimmäinen askel on varmuuskopioida yrityksen tiedot säännöllisesti ja varmistaa, että palautusprosessi on toimiva ja testattu, sisältäen varmuuskopioinnin ulkoisille palveluille ja fyysisten tallennusvälineiden suojauksen. Toisena on tärkeää päivittää kaikki tietotekniset järjestelmät ja laitteet ajan tasalle, jotta tunnetut haavoittuvuudet saataisiin korjattua ja järjestelmät pysyisivät turvallisina. Kolmanneksi yrityksen henkilöstön kouluttaminen keskeisistä tietoturvauhista ja jatkuvan koulutuksen tarjoaminen auttavat vahvistamaan tietoturvatietoisuutta. Neljäs toimenpide on tietoympäristön valvonta, mukaan lukien tekniset ratkaisut kuten tunkeutumisenestojärjestelmät ja tietojen jatkuva analysointi, mikä varmistaisi, että mahdolliset tietoturvaloukkaukset havaittaisiin ajoissa. Viidenneksi monikerroksinen suojaus on välttämätön verkon ja laitteiden suojaamiseksi ulkoisilta uhkilta, yhdistämällä erilaisia turvatoimia riskien minimoimiseksi. Kuudentena organisaatioiden tulisi varautua tietoturvaloukkauksiin suunnittelemalla ja testaamalla vastatoimia, jotta ne pystyisivät reagoimaan nopeasti ja tehokkaasti mahdollisiin tietoturvatapauksiin minimoimalla niiden vaikutukset liiketoimintaan. Tietoturvariskien hallinta on loputon prosessi ja yritysten tulee kehittää tietoturvallisuutta jatkuvasti.[70] Riskejä arvioitaessa on myös tärkeää ottaa huomioon niiden ihmisten näkökulma, joiden henkilötietoja käsitellään ja tietoturvariskien vakavuuden arvioinnissa on keskeistä miettiä, millaista vahinkoa ihmisille voi aiheutua.[71]

[70] Keskuskauppakamari 2016: s.12–15
[71] Korpisaari, Pitkänen & Warma-Lehtinen 2022: 33.

5 Johtopäätökset

Koronapandemia pakotti organisaatiot nopeaan siirtymiseen etätyöhön, mikä toi mukanaan merkittäviä haasteita tietoturvalle ja tietosuojalle. Etätyön myötä organisaatioiden haavoittuvuus kasvoi, sillä perinteiset tietoturvakäytännöt on ensisijaisesti suunniteltu toimimaan toimistoympäristöissä, eivätkä ne sovellu sellaisenaan hajautettuun etätyömalliin. Pandemian aiheuttama epävarmuus on luonut otollisen toimintaympäristön kyberrikollisuudelle kohdistamalla hyökkäyksiä sekä yksityishenkilöihin että organisaatioiden järjestelmiin.[72]

Nopea siirtyminen uusiin työskentelytapoihin edellytti sekä teknisten ratkaisujen että organisatoristen käytäntöjen huolellista suunnittelua ja toteutusta. Työnantajien on tarjottava työntekijöille asianmukaiset työvälineet sekä selkeät ohjeistukset tietoturvan ylläpitämiseksi. Näin voidaan turvata sekä organisaation että yksilön tiedot tehokkaasti. Työelämän jatkuva digitalisoituminen edellyttää, että tietosuoja- ja tietoturvakäytännöt kehittyvät samassa tahdissa. Vain näin voidaan vastata muuttuvan työympäristön riskeihin ja turvata luottamus digitaaliseen työskentelyyn.[73] Tietoturva on tänä päivänä paljon enemmän kuin pelkkä tekninen ratkaisu, sillä se on myös olennainen osa yhteiskunnan ja oikeusvaltion toimintaa. Suomessa olisi tarpeen säätää yleinen tietoturvalaki ja tunnustaa tietoturvan merkitys perusoikeutena perustuslaissa. Tieto ei ole vain dataa, vaan siihen liittyy olennaisesti yksityisyyden suoja, oikeudet ja luottamus. Tietoturvan asianmukainen sääntely ja toteutus ovat keskeisiä ihmisoikeuksien turvaamisessa digitaalisessa ympäristössä.[74]

Tutkielma osoittaa, että etätyön laajamittainen yleistyminen on pakottanut organisaatiot uudelleenarvioimaan ja päivittämään tietoturvakäytäntöjään. Käytäntöjen muutos on näkynyt erityisesti henkilöstön tietoturvakoulutuksen tehostamisena ja organisaatioiden valvontakeinojen monipuolistumisena.

[72] Pranggono ja Abdullahi 2021: 1.
[73] Edilex, Karvinen 2021: webinaari
[74] Saarenpää ja Riekkinen 2023: 3.3.4.5

Työntekijöiden etätyöympäristöjen turvallisuutta on pyritty parantamaan esimerkiksi säännöllisillä tarkastuksilla ja reaaliaikaisella uhkien seurannalla. Tämä osoittaa, että organisaatiot pyrkivät aktiivisesti vastaamaan etätyön tuomiin haasteisiin ja vähentämään tietoturvariskejä.

Teknologia on kehittynyt valtavasti viime vuosikymmeninä, mikä on mahdollistanut työn tekemisen ajasta ja paikasta riippumatta, mutta samalla se on tuonut mukanaan uusia uhkia. Turvattomat Wi-Fi-verkot, heikot salasanat, tietojenkalastelu ja muut kyberhyökkäykset muodostavat merkittäviä riskejä, jotka voivat johtaa tietomurtoihin. Näihin riskeihin voidaan vastata hyödyntämällä turvallisia etätyökäytäntöjä, kuten VPN-yhteyksiä, palomuureja ja monivaiheista tunnistautumista.

Tutkielman tavoitteena oli tarkastella, miten etätyö vaikuttaa organisaatioiden tietosuojaan ja tietoturvaan, sekä tunnistaa millaisia riskejä ja haasteita siihen liittyy. Pandemian seurauksena etätyö on tullut osaksi arkea, ja se on muuttanut työympäristöjä merkittävästi. Työntekijöiden siirtyminen toimistoista usein vähemmän suojattuihin tiloihin on lisännyt organisaatioiden haavoittuvuutta, mikä edellyttää strategioiden ja käytäntöjen uudelleentarkastelua. Tietoturvakäytäntöjen kehittäminen ei ole pelkästään teknologinen tai organisatorinen kysymys, vaan se vaatii myös asenteiden ja toimintatapojen muutosta. Työntekijöiden koulutus ja tietoisuuden lisääminen ovat keskeisessä roolissa, jotta käytännöt eivät jää irrallisiksi ohjeiksi, vaan niistä tulee osa jokapäiväistä toimintaa. Teknologian osalta organisaatiot ovat vastanneet etätyön haasteisiin ottamalla käyttöön uusia työkaluja kuten etäyhteydet ja pilvipohjaiset palvelut, joiden avulla työntekijät voivat jatkaa työskentelyään turvallisesti kodin ulkopuolella. Kuitenkin samalla ne tuovat mukanaan uusia haavoittuvuuksia, jos niitä ei hallita oikein.

Tutkielmassa korostettiin selkeiden ohjeistusten ja käytäntöjen tärkeyttä, jotka ohjaavat työntekijöitä etätyössä ja auttavat heitä ymmärtämään oman roolinsa organisaation tietoturvan ylläpitämisessä. Työntekijöiden tietoisuuden lisääminen, koulutus sekä

selkeät tietoturvaohjeet ovat kriittisiä tekijöitä, jotka auttavat ehkäisemään tietoturvauhkia. Organisaatioiden on tehtävä selväksi, että tietoturva kuuluu kaikille, eikä se rajoitu pelkästään IT-osastolle. Lisäksi tietoturva vaatii jatkuvaa ylläpitoa, valvontaa ja kykyä reagoida uusiin uhkiin nopeasti ja joustavasti.

Sääntelyn ja lainsäädännön merkitys tietoturvan hallinnassa on olennainen. EU:n yleinen tietosuoja-asetus (GDPR) ja kansalliset tietosuojalait määrittelevät toiminnan kehyksen, jonka mukaisesti organisaatioiden tulisi toimia. Kun työympäristöt hajautuvat ja digitaaliset järjestelmät kehittyvät yhä monimutkaisemmiksi, on melko välttämätöntä, että lainsäädäntöä on päivitettävä jatkuvasti vastaamaan uusia haasteita.

Yhteenvetona voidaan todeta, että etätyön aikakaudella tietosuoja ja tietoturva vaativat kokonaisvaltaista lähestymistapaa, jossa teknologia, käytännöt, sääntely ja työntekijöiden koulutus tukevat toisiaan. Vaikka etätyö tarjoaa monia mahdollisuuksia organisaatioille laajentaa toimintaansa entisestään ja tarjoaa työntekijöille joustavuutta, sen tuomat riskit on otettava vakavasti ja niihin on varauduttava ennakoivasti. Organisaatioiden on jatkuvasti kehitettävä tietosuoja- ja tietoturvakäytäntöjään sekä investoida resurssejaan näiden käytäntöjen tehokkaaseen toteuttamiseen. Etätyö ei ole ohimenevä ilmiö, vaan uusi normaali, joka edellyttää uusia strategioita ja käytäntöjä, jotka vastaavat nykyisiin haasteisiin ja ennakoivat myös tulevia riskejä.

Jatkotutkimusehdotuksena olisi hyödyllistä tutkia tarkemmin, miten vastuu tietoturvan ylläpitämisestä jakautuu organisaation sisällä tilanteissa, joissa suunnitellut riskienhallintakeinot eivät toimi odotetusti. Tällainen tutkimus voisi tuoda esiin, miten organisaatiot käytännössä toteuttavat korjaavia toimenpiteitä ja miten eri rooleissa toimivat työntekijät voivat osallistua tietoturvan ylläpitoon. Tämä voisi tarjota syvällisempää ymmärrystä siitä, miten tietoturvariskien hallinta voidaan yhdistää osaksi organisaation jokapäiväistä toimintaa ja päätöksentekoa. Lisäksi se voisi tarjota uusia

keinoja kehittää tietoturvan hallintaa vastaamaan paremmin etätyön erityisvaatimuksia ja nopeasti muuttuvaa uhkaympäristöä.

Lähdeluettelo

Andersson, J. (2024). Organisaation hyvä tietoturvan sääntelyjärjestelmä. Väitöskirja. https://osuva.uwasa.fi/bitstream/handle/10024/18074/978-952-395-150-1.pdf?sequence=2&isAllowed=y

Andersson, J. (2018). Edilex. Organisaation tietoturva- ja tietosuojariskienhallinta sekä lainsäädännön vaatimukset. https://www-edilex-fi.proxy.uwasa.fi/artikkelit/18528.pdf

Drew, J. (2012). Managing Cybersecurity Risks. Journal of Accountancy. https://www.proquest.com/docview/1032813550?accountid=14797&sourcetype=Trade%20Journals#center

Edilex. (21. tammikuuta 2021). Karvinen, K. Tietoturva, tietosuoja ja muut etätyön erityiskysymykset pohdinnassa Editan webinaarissa. Noudettu 3.3.2025 osoitteesta https://www-edilex-fi.proxy.uwasa.fi/uutiset/67416?allWords=tietoturva+etätyössä&offset=1&perpage=20&sort=relevance&searchSrc=1&advancedSearchKey=1083491

Edilex. (23. marraskuuta 2022). KHO: 2022:131. Noudettu 22.3.2025 osoitteesta https://www-edilex-fi.proxy.uwasa.fi/kho/vuosikirjat/202203377h?offset=1&perpage=20&phrase=tietoturva&sort=relevance&typeIds[]=7&typeIds[]=8&typeIds[]=9&searchKey=1567697&quickSearch=true

EUR-Lex. (6. huhtikuuta 2014). ENISA – Euroopan unionin verkko- ja tietoturvavirasto. https://eur-lex.europa.eu/FI/legal-content/summary/enisa-the-european-union-agency-for-network-and-information-security.html

Finlex. (2020). Hallituksen esitys eduskunnalle laeiksi oikeusministeriön hallinnonalan eräiden henkilötietojen käsittelyä koskevien säännösten muuttamisesta. Noudettu 23.3.2025 osoitteesta: https://finlex.fi/fi/hallituksen-esitykset/2020/2#OT0

Finlex. (31. toukokuuta 2022). Sijaintitietotoiminnon käyttö työntekijöiden kannettavissa tietokoneissa. https://finlex.fi/fi/viranomaiset/tsv/2022/20221463

Finlex. (2018). Tietosuojalaki. https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

Godlove, Timothy. (2012). Examination of the Factors that Influence Teleworkers' Willingness to Comply with Information Security Guidelines, Information Security Journal. https://research.ebsco.com/c/slwlh3/search/details/cl4qk3g7ar?db=afh&isDashboardExpanded=true&limiters=None&q="remote%20work"%20AND%20%28"data%20security"%20OR%20"privacy%20impact"%29

Hanninen, M. Laine, E. Rantala, K. Rusi, M. Varhela, M. (2017). Henkilötietojen käsittely. Kauppakamari. https://kauppakamaritieto-fi.proxy.uwasa.fi/ammattikirjasto/teos/henkilotietojen_kasittely#kohta:Henkil((f6)((ad)tietojen((20)k((e4)sittely

Hietala, H. Hurmalainen, M. Kaivanto, K. (2024). Työsuojeluvastuuopas. https://verkkokirjahylly-almatalent-fi.proxy.uwasa.fi/teos/FAIBBXXTBBAEF#kohta:7((a0)((a0)((7c)((20)Ty((f6)suojelu((20)erityisryhmiss((e4)(:7.5((20)Et((e4)ty((f6)((20)ja((20)kotity((f6)/piste:t1Ah

Hijji, Mohammad ja Alam, Gulzar. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. Sensors. Noudettu 15.11.2024

osoitteesta https://research.ebsco.com/c/slwlh3/search/details/wdjlyzn2zr?db=afh&isDashboardExpanded=true&limiters=None&q=“telecommuting”%20AND%20%28“data%20protection”%20OR%20“cybersecurity”%29

Hoofnagle, C ja muut. (2019). The European Union general data protection regulation: What it is and what it means. Information & communications technology law. https://www.tandfonline.com/doi/pdf/10.1080/13600834.2019.1573501?needAccess=true

Järvinen, P. Rousku, K. (2017). Työpaikan tietoturvaopas: tunnista uhat, hallitse riskit. Alma Talent Oy. https://tritonia.finna.fi/Record/tria.378280?sid=4916170224

Kauppakamari. (2016). Tietoturvaopas yrityksille – ICC Cyber security guide for business. International Chamber of Commerce (ICC). Noudettu 27.1.2025 osoitteesta https://kauppakamari.fi/wp-content/uploads/2020/06/tietoturvaopas-yrityksille.pdf

Kinnunen, N. (2015). Tietoturvaohjeistusten noudattamisen motivaatio ja sen muuttuminen. Väitöskirja. Noudettu 23.3.2025 osoitteesta: https://tritonia.finna.fi/Record/osuva_diss.10024_7444?sid=4973173867

Korpisaari, P. Pitkänen, O. Warma-Lehtinen, E. (2022). Tietosuoja. Alma Talent Oy. https://verkkokirjahylly-almatalent-fi.proxy.uwasa.fi/teos/CAIBCXETEB#kohta:I((20)YLEISET((20)S((c4)((c4)NN((d6)KSET/piste:b1

Korpisaari, P. Pitkänen, O. Warma-Lehtinen, E. (2018). Uusi tietosuojalainsäädäntö. https://verkkokirjahylly-almatalent-

fi.proxy.uwasa.fi/teos/BAXBBXATHBBED#kohta:((20)Uusi((20)tietosuojalains((e4)((e4)d((e4)nt((f6)/piste:t4B

Leskinen, T. (14. huhtikuuta 2023). Korona hellitti, mutta etätyötä tekevien määrä ei juuri vähentynyt. Tilastokeskus. Noudettu 1.12.2024 osoitteesta https://stat.fi/tietotrendit/artikkelit/2023/korona-hellitti-mutta-etatyota-tekevien-maara-ei-juuri-vahentynyt

Leskinen, T. (22. joulukuuta 2020). Säännöllisesti kotona työskenteleminen on kaksinkertaistunut. Tilastokeskus. Noudettu 1.12.2024 osoitteesta https://stat.fi/tietotrendit/blogit/2020/saannollisesti-kotona-tyoskenteleminen-on-kaksinkertaistunut

Nieminen, K. (2024). Työpaikan lait ja työsuhdeopas 2025. Alma Talent Oy. https://verkkokirjahylly-almatalent-fi.proxy.uwasa.fi/teos/FAEBCXFTEB#kohta:7.((20)Ep((e4)tyypilliset((20)ty((f6)suhteet((20)(:7.4((20)Et((e4)ty((f6)/piste:b1511

Niemi, P. (2018). Sisäinen tarkastus käytännössä (1.painos). Alma Talent Oy. https://verkkokirjahylly-almatalent-fi.proxy.uwasa.fi/teos/BAXBBXATEBEED#kohta:Sis((e4)inen((20)tarkastus((20)k((e4)yt((e4)nn((f6)ss((e4)/piste:t1gG

Pranggono, B. ja Abdullahi, A. (2021). COVID-19 pandemic cybersecurity issues. Internet technology letters. Noudettu 23.3.2025 osoitteesta: https://tritonia.finna.fi/PrimoRecord/pci.cdi_pubmedcentral_primary_oai_pubmedcentral_nih_gov_7675576?sid=4973109133

Ratsula, N. (2021). Sisäinen valvonta: käsikirja tulokselliseen organisaation ohjaukseen. https://digikirja-edita-fi.proxy.uwasa.fi/digikirja/3780883?lid=25e1f&edilex_redir=true#Esipuhe

Saarenpää, A. ja Riekkinen, J. (2023). Oikeusinformatiikan perusteet. https://lauda.ulapland.fi/bitstream/handle/10024/65315/978-952-337-347-1.pdf?sequence=1&isAllowed=y

Solove, Daniel J. (2024). Data is what data does: regulating based on harm and risk instead of sensitive data. Northwestern University Law Review. https://www.proquest.com/abicomplete/docview/2928642068/fulltext/8F2FA26168164944PQ/11?accountid=14797&sourcetype=Scholarly%20Journals

Suomen laki hakupalvelu. (2016). Tietosuoja-asetus. Alma Talent. https://suomenlaki-almatalent-fi.proxy.uwasa.fi/#//Regulation$yes/EuRegulation/SiEU108///2025-02-12

Suomen laki hakupalvelu. (2018). Tietosuojalaki. Alma Talent. https://suomenlaki-almatalent-fi.proxy.uwasa.fi/#//Regulation$yes/Regulation/Si111///2025-02-12

Tietosuojavaltuutetun toimisto. Pseudonymisoidut ja anonymisoidut tiedot. Noudettu 13.1.2025 osoitteesta https://tietosuoja.fi/pseudonymisointi-anonymisointi

Tietosuojavaltuutetun toimisto. Tietosuoja. Noudettu 13.1.2025 osoitteesta https://tietosuoja.fi/tietosuoja

Tietotekniikan käyttö yrityksissä. (2019). Tilastokeskus. Noudettu 1.12.2024 osoitteesta https://stat.fi/til/icte/2019/icte_2019_2019-12-03_kat_007_fi.html

Työ- ja elinkeinoministeriö. (2019). Työelämän tietosuojalaki. https://tem.fi/documents/1410877/2917589/Työelämän+tietosuoja/f94a4e13-9e89-43ea-a6f0-f7c3de37ab9d/Työelämän+tietosuoja.pdf

Valtiovarainministeriö. (2017). Valtiovarainministeriö pyytää lausuntoja riskienhallinnan ja sähköisen asioinnin tietoturvallisuus -ohjeisiin. Noudettu 5.3.2025 osoitteesta https://vm.fi/-/valtiovarainministerio-pyytaa-lausuntoja-riskienhallinnan-ja-sahkoisen-asioinnin-tietoturvallisuus-ohjeisiin

Vilkman, U. (2016). Etäjohtaminen: Tulosta joustavalla työllä. Talentum Pro. s.185 https://verkkokirjahylly-almatalent-fi.proxy.uwasa.fi/teos/DAEBIXCTEB#/kohta:Et((e4)johtaminen/piste:thR

Vivekananth, P. (2022). Cybersecurity risks in remote working environment and strategies to mitigate them. International journal of engineering and management research. https://ijemr.vandanapublications.com/index.php/j/article/view/630/595

Wainwright, P. Katamba, F. Henderson, D. (2024). Cybersecurity Risks to Business and Legal Sectors. Business Law International.https://www.proquest.com/docview/3113826807/fulltext/AFF1DABD981A4A56PQ/1?accountid=14797&sourcetype=Scholarly%20Journals

Zohaib, S. Sajjad, S. Iqbal, Z. Yousaf, M. Haseeb, M. Muhammad, Z. (2024). Zero trust VPN (ZT-VPN): A systematic Literature Review and Cybersecurity Framework for hybrid and remote work. Information (Basel). https://tritonia.finna.fi/PrimoRecord/pci.cdi_doaj_primary_oai_doaj_org_article_010ac02a41724e538835a68afbdd77e9?sid=4904134971