Etätyön tietoturvasuositukset

TkK-tutkielma
Turun yliopisto
Tietotekniikan laitos
Tietotekniikka
2024
Niklas Mettälä

TURUN YLIOPISTO
Tietotekniikan laitos

Niklas Mettälä: Etätyön tietoturvasuositukset

TkK-tutkielma, 21 s.
Tietotekniikka
Huhtikuu 2024

Etätyöskentelyn määrä on jatkuvassa kasvussa. Varsinkin koronaviruspandemian jälkeen yritykset ovat alkaneet hyödyntää enemmän etätyöskentelyä toiminnassaan. Etätyöskentelyn lisääntyminen tuo mukanaan omanlaisiaan tietoturvauhkia yrityksille ja yksityishenkilöille. Tutkielmassa käsitellään kirjallisuuden perusteella etätyön aiheuttamia tietoturvauhkia, sekä erilaisia keinoja ja suosituksia niihin varautumiseen. Etätyössä työskentely-ympäristö ei ole valvottu yrityksen toimesta, joten päätelaitteisiin ja tietoverkkoihin kohdistuvat uhat korostuvat. Yleisimpiin uhkiin kuuluvat erilaiset tiedonkalasteluhyökkäykset ja haittaohjelmat. Etätyössä tietoturvan hallinta jää yksittäisen etätyötä tekevän työntekijän vastuulle, joten yksilöllä on tärkeä rooli tietoturvan toteutumisessa. Etätyön tuomien uhkien minimoimiseksi on yrityksiä ajatellen luotu useita erilaisia suosituksia. Suosituksia on luotu yleisellä tasolla muun muassa teknisen toteutuksen ohjeistamiseen, toiminnallisen ympäristön määrittelyyn ja myös yksityiskohtaisempien aiheiden, kuten turvallisten työvälineiden valintaan. Suurimpia toistuvia teemoja suositusten välillä ovat yksittäisen työntekijän vastuu ja koulutus tietoturvataitojen osalta, tietoverkkoratkaisujen turvaaminen teknisin ratkaisuin, sekä etätyöhön käytettävien päätelaitteiden ja ohjelmistojen huolellinen valinta ja niiden elinkaaren hallinta.

Asiasanat: Tietoturva, Etätyö, Tietoturvakäytänteet

Sisällys

1 Johdanto

Etätyöskentelyn lisääntyessä on tärkeää kiinnittää huomiota sen vaikutuksiin tietoturvauhkiin ja niiden minimoimiseksi muodostettuihin tietoturvakäytänteisiin. Työpaikalla tehdyt työpaikkaan liittyvät tietoturvakäytänteet eivät välttämättä toimi suoraan ihmisten siirtyessä työskentelemään erilaisiin ympäristöihin. Valvomattomien työympäristöjen, laitteiden ja työtapojen mukanaan tuomat uudet tietoturvariskit on huomioitava tietoturvakäytänteissä. Yritysten on myös tärkeä miettiä mitä juuri etäympäristössä tarvitsee tehdä tietoturvallisuuden maksimointia ajatellen [1].

Etätyön lisääntyessä, sen turvalliseen toteuttamiseen on hyvä käyttää aikaa ja resursseja, sillä etätyössä on mahdollisuus kohdata tietoturvauhkia, joita ei välttämättä toimistotyössä kohtaisi tai jotka toimistotyössä olisi helpompi minimoida. Tutkielman tarkoituksena on selvittää lisääntyvän etätyöskentelyyn erityisesti liittyviä tietoturvakysymyksiä ja niiden pohjalta muodostettuja käytänteitä yrityksissä. Sen lisäksi tarkoituksena on tarkastella materiaalia, jota on luotu yritysten avuksi tietoturvan tason nostamiseksi.

Tutkielmaa aloittaessa koronapandemia oli mahdollistanut etätyöskentelyn suuren kasvun ja kasvun uskotaan jatkuvan myös jatkossa [2]. Etätyön kasvua nopeuttavat pandemian lisäksi myös työntekijöiden muut tarpeet ja toiveet. Etätyöllä koetaan olevan positiivisia vaikutuksia ajankäytön suunnitteluun, sekä työn ja vapaa-ajan yhteen sovittamisen. [3] Tämän vuoksi myös etätyön tietoturvaa on tärkeä tarkastella, jotta yritysten toiminta ja niiden käsittelemä data voidaan turvata.

Tämä tutkielma on toteutettu kirjallisuuskatsauksena, jossa käydään läpi aiheeseen liittyvää kirjallisuutta. Kirjallisuus koostuu tieteellisistä julkaisuista, tutkimuksista, artikkeleista ja kirjoista. Tutkielma käsittelee etätyön tietoturvaa ja sen tavoitteena on vastata seuraaviin tutkimuskysymyksiin:

TK1 Mitkä ovat tyypillisimmät etätyöskentelyn tietoturvaongelmat?

TK2 Mitä suosituksia yrityksille on annettu etätyöskentelyn tietoturvakäytäntöjen parantamiseksi?

TK3 Millaisia keinoja yrityksillä on etätyöskentelyn tuomiin tietoturvauhkiin varautumiseen ja niihin vastaamisen?

Tutkielmassa käytetty aineisto on haettu pääosin IEEE Xpolre ja ACM Digital Library tietokantoja hyödyntäen. Hakusanoina käytettiin "remote work", "telework", "telecommuting"ja "cybersecurity". Hakutuloksia löytyi kohtuullisesti, joten aineistoa rajattiin vain vähän. Rajaus keskitettiin julkaisuajankohtaan ja tulokset rajattiin vuoden 2010 jälkeen julkaistuihin tuloksiin. Aineiston valinnassa keskityttiin pääosin tietoteknistä alaa koskeviin hakutuloksiin. Varsinkin koronapandemian vaikutuksia käsiteltäessä oli tärkeä rajata hakutuloksia julkaisuajankohdan mukaan ajankohtaisen tiedon varmistamiseksi. Tieteellistä aineistoa täydentämään on haettu suosituksia ja ohjeita valtion laitosten kuten Huoltovarmuuskeskuksen ja Kyberturvallisuuskeskuksen aineistosta.

Tutkielman toisessa luvussa käsitellään etätyöskentelyä ja esitellään sen mahdollistavia tekniikoita. Kolmannessa luvussa keskitytään tietoturvaan, yleisimpiin tietoturvauhkiin yrityksissä sekä tapoihin näiden uhkien minimoinniksi. Neljännessä luvussa käsitellään etätyön tuomiin tietoturvauhkiin, tieturvakäytänteisiin sekä suosituksiin uhkien minimoimiseksi. Lopuksi käydään läpi tutkielman yhteenveto, jossa käydään läpi käsiteltyjä asioita kokonaisuutena.

2 Etätyöskentely

Etätyöskentelyllä tarkoitetaan työskentelyä jossain muussa paikassa kuin työnantajan tiloissa. Paikka voi olla työntekijän koti tai julkinen tila. Etätyöhön liittyy myös vaihteleva työnteon ajankohta, joka on perinteisesti työnantajan määrittelemä silloin kun työskennellään työnantajan tarjoamassa tilassa. Etätyön muoto voi vaihdella joustavasta etätyöstä täyteen etätyöhön. Joustavassa etätyössä osan työstä voi suorittaa etänä työntekijän henkilökohtaisten menojen niin vaatiessa tai sovituissa jaksoissa etätyön ja työpaikalla tapahtuvan työn välillä. Täydessä etätyössä työpaikalla ei tarvitse käydä fyysisesti paikalla juuri ollenkaan ja työntekijä voi suorittaa työtehtävänsä haluamassaan paikassa. [3]

Etätyöskentelyn lisääntyminen

Etätyöskentely on lisääntymässä useasta eri syystä. Teknologian ja viestintätapojen kehittyminen, sekä teknisten laitteiden hinnan lasku on mahdollistanut etätyöskentelyn yhä useammalle työntekijälle. Etätyö mahdollistaa yrityksille myös kustannuksien madaltamisen, sillä jokaiselle työntekijälle ei enää aina tarvitse varata omaa työskentelytilaa toimistolta. Työmatkoihin käytettyä aikaa pyritään hillitsemään etätyön avulla ja siten parantamaan tuottavuutta. Etätyöstä voi olla hyötyä myös työntekijän näkökulmasta. Korostunut perheen ja vapaa-ajan merkitys yhteiskunnassa edesauttaa lisäämään etätyötä entisestään, koska se mahdollistaa työntekijälle ajankäytön paremman suunnittelun. [3]

Myös koronaviruspandemia on kasvattanut etätyöskentelyn määrää huomattavasti. Pandemian myötä etätyöskentely on korvannut monia ennen vain työnantajan tiloissa mahdollistettuja työtehtäviä. [2] Etenkin moni tietotekniikan alan yritys suositteli työntekijöilleen etätyötä pandemian aikana laajasti ja pitkäaikaisesti. [4]

Pandemian jälkeen etätyö on jäämässä pysyvästi etenkin tietotyön työntekijöiden käyttöön. Osa etätyöhön siirtyneistä on jopa uhannut lopettaa työssään, jos heidät ohjattaisiin täysin takaisin työnantajan tiloissa suoritettavaan työhön. Tulevaisuudessa tietotyössä tullaan hyödyntämään vahvasti hybridityöskentelyä, eli etätyöskentelyn ja määrätyllä työpaikalla työskentelyn sekoitusta. [5]

Etätyöskentelyn vaikutus työntekoon

Yhdysvalloissa etätyön lisääntyminen on lisännyt työntekijöiden työhönsä käyttämää aikaa. Yli kolmasosa käyttää säästyneen työmatka-ajan työnsä tekemiseen. Näiden työntekijöiden keskimääräisesti työskentelemät viikkotunnit lisääntyivät yli neljällä tunnilla etätöihin siirtymisen jälkeen. [6] Työmatkaan käytetyn ajan säästö oli yksi tärkeimmistä etätyön hyödyistä Microsoftin etätyöhön siirtyneiden kehittäjien mukaan. Heistä suurin osa koki tuottavuutensa pysyneen samana tai jopa parantuneen etätyöhön siirtyessä. Etätyön mahdollistamat joustavat työajat, vähentyneet häiriötekijät ja parantunut työn ja vapaa-ajan tasapaino koettiin tärkeiksi. Toisaalta moni etätyöhön siirtynyt koki tilanteen haasteelliseksi motivoitumisen vaikeuden tai lisääntyneiden häiriötekijöiden vuoksi. [4]

Suurimpia tietotyöntekijöiden kokemia haasteita etätyöskentelyssä ovat tietototeknisten yhteyksien toimivuus, läsnä olevat perheenjäsenet kommunikaatio ja työn ja vapaa-ajan rajan hämärtyminen. [4] Etääntyminen muista ihmisistä on koettu haasteeksi etätyöskentelyssä, jolloin työntekijän sosiaalisuus on jäänyt tekniikan varaan. Työntekijöille jaettava tieto voi saavuttaa heidät heikommin etätyövälineiden kautta ja tärkeät uudet käytännöt tai ohjeistukset voivat jäädä toteuttamatta. [7]

Etätyöskentelyn mahdollistava teknologia

Etätyöskentely ja siinä käytettävät etäkokoukset, sähköpostit ja muu elektroninen viestintä on mahdollista tietotekniikan avulla. [8] Työntekoon käytettyjä latteita ovat kannettavat tietokoneet, tabletit ja älypuhelimet, jotka mahdollistavat työssä käytettävien ohjelmistojen käytön. [7] Kannettavien tietokoneiden ja tablettien tehokkuus on kehittynyt kiinteiden työasemien tasolle, joka mahdollistaa niiden tehokkaan hyödyntämisen etätyöskentelyssä. [9]

Tietoliikenneyhteydet työnantajaan ovat myös tärkeä tekninen etätyön mahdollistaja. Niitä käytetään työskentelyyn tarvittavien materiaalien ja datan saatavuuteen ja työn tulosten siirtämiseen työnantajan tietojärjestelmiin. Etätyöskentelyyn voidaan käyttää julkisia ja yksityisiä tietoverkkoja, jotka voivat olla langattomia tai langallisia. Tietoverkkojen avulla päästään myös työskentelemään pilvipalveluja, eli verkossa sijaitsevia tietoteknisiä palveluja, hyödyntämällä. [8] Tietoverkkoympäristössä käytössä ovat erilaiset verkkoratkaisut. Työtä voidaan suorittaa julkisen internetin yli tai hyödyntää VPN (Virtual Private Network) yhteyttä työnantajan verkkoon. Näiden ratkaisujen lisäksi voidaan käyttää virtuaalisia työasemia, joita hallitaan verkkoyhteyden välityksellä. Verkkoyhteys mahdollistaa myös viestintä- ja kokoussovellusten käytön työasemalta. [4]

Etätyön mahdollistamiseksi käytetään siis teknologiaa laajasti päätelaitteiden, sovellusten ja verkkoratkaisujen muodossa. Hyvät tietoliikenneyhteydet ovat tehokkaan etätyön tärkein mahdollistaja, sillä niiden avulla toteutetaan työntekijöiden välinen viestintä ja yrityksen datan liikuttaminen yrityksen tietovarastoista työntekijän käyttöön. Etätyön määrä on kasvussa ja tulevaisuudessa merkittävä työn suorittamisen muoto. Teknologian tehokkaalla hyödyntämisellä etätyöskentelystä pyritään tekemään sujuvaa ja turvallista.

3 Tietoturva

Tietoturva on tietoteknisten laitteiden, tietoverkkojen ja ohjelmistojen suojaamista hyökkäyksiltä, vahingolta sekä luvattomalta käytöltä. Tällaiset tietoturvaan kohdistuvat uhat voivat aiheuttaa vakavia taloudellisia menetyksiä ja ne vaikuttavat ihmisten turvallisuuteen henkilötietojen tai muun arkaluonteisen tiedon vahingoittamisella. [10] Kaikkien tietoteknisten laitteiden käyttäjien ja palveluntarjoajien on tärkeä huolehtia tietoturvasta. Usean tahon samanaikaiset tietoturvatoimet toimivat tehokkaasti uhkien minimoinnissa. Ne mahdollistavat tehokkaan hyökkäysten havaitsemisen ja niihin reagoinnin. [11]

3.1 Yleisimpiä tietoturvauhkia

Tietotekniikan käyttäjiä ja heikkoa tietoturvaosaamista pidetään suurimpana uhkana tietoturvallisuudelle. Jatkuvasti kehittyvä teknologia ja sen myötä uudet uhat tietoturvallisuudelle vaikeuttavat käyttäjien tietoturvaosaamisen kasvattamista ja ajan tasalla pitämistä. [12] Käyttäjiin kohdistuvia tietoturvauhkia ovat esimerkiksi roska- ja huijaussähköpostit sekä tietojenkalasteluhyökkäykset.

Roskasähköpostit ovat käyttäjälle saapuvia ei toivottuja sähköposteja. Roskapostin sisältönä voi olla markkinointia, valheellista tietoa tai haitallisia linkkejä haittaohjelmistojen lataamiseen tai muun hyökkäyksen mahdollistamiseen. Roskapostin lähettäminen on helppoa ja lähettäjälle edullista, joten niitä lähetetään suuria määriä kerralla. Ne vaikuttavat tiedon saatavuuteen, eheyteen ja luottamuksellisuuteen.

Roskapostit ovat olleet myös osa palvelunestohyökkäyksiä, sillä ne hidastavat tuottavuutta ja kuluttavat tietoliikenneresursseja.

Tietojenkalasteluhyökkäyksissä käyttäjä huijataan antamaan salaista tai arkaluonteista tietoa. Tällaista tietoa ovat etenkin eri palveluiden salasanat ja käyttäjän henkilötiedot. Tietojenkalasteluhyökkäyksissä voidaan hyödyntää verkkosivustoja, jotka on suunniteltu näyttämään täysin samalta kuin jonkun palveluntarjoajan, esimerkiksi verkkopankin, verkkosivu. Tällaiselle verkkosivulle käyttäjä voidaan huijata syöttämään arkaluonteista tietoa pyytämällä päivittämään tietojaan tai salasanaansa. Tietojenkalasteluhyökkäyksellä voidaan tavoitella yksittäisten henkilöjen tai suurempien organisaatioiden tietoja niiden hyödyntämistarkoituksessa. [13]

Muita vakavia tietoturvauhkia ovat haavoittuvat verkkosivustot, päivittämättömät tietokoneet ja ohjelmistot, suojaamattomat tietokoneet ja heikot salasanat. [14] Näistä kaikki ovat myös käyttäjien aiheuttamia uhkia, jotka johtuvat siitä, että käyttäjät hoitavat omat tietoturvaratkaisunsa itsenäisesti. [11] On olemassa myös käyttäjästä riippumattomia, ulkoisen hyökkääjän aiheuttamia, tietoturvauhkia. Tällaisiä hyökkäyksiä ovat erilaiset haittaohjelmat, kuten virukset ja troijalaiset, sekä vakoiluohjelmat ja kiristysohjelmistot. Hyökkääjät voivat myös päästä luvattomasti kirjautumaan järjestelmiin arvaamalla tai varastamalla salasanoja. [15]

Haittaohjelmistot ovat ohjelmistoja, jotka on suunniteltu leviämään tietokoneesta toiseen ja aiheuttamaan jotain hyökkääjän haluamia vaikutuksia. Virukset leviävät muiden ohjelmistojen mukana ja kopioivat itseään, kun tällainen ohjelma suoritetaan. Virukset leviävät, kun saastuneita ohjelmia jaetaan laitteesta toiseen. Troijalaiset ovat hyödyllisiksi ohjelmistoiksi naamioituja ohjelmistoja, jotka sisältävät piilotettua koodia, joka suoritetaan ohjelma käynnistettäessä.

Kiristysohjelmistot lukitsevat käyttäjältä pääsyn järjestelmään tai johonkin sen osa-alueeseen ja vaativat maksua pääsyn palauttamiseksi. Esimerkki laajalle levinneestä kiristysohjelmasta on WannaCry-haittaohjelma, joka vaikutti yli 200 000

käyttäjään yli 150 maassa. Vakoiluohjelmistot seuraavat tietokoneella tai verkossa tapahtuvaa toimintaa ja keräävät informaatiota hyökkääjälle. Ne voivat kerätä saastuttamaltaan laitteelta arkaluontoista tietoa kuten käyttäjien sähköpostiosoitteita tai salasanoja. [15]

3.2 Tietoturvauhkien minimointi

Tietotekniikan käyttäjien on tärkeää kouluttautua tietoturvauhkia vastaan, sillä teknisten laitteiden määrä kasvaa nopeasti. Varsinkin verkkoon kiinnitetyt laitteet muodostavat tietoturvauhkia, joten laitteiden verkkoyhteyden katkaiseminen tarvittaessa on hyvä tapa suojautua tietoverkkojen tietoturvauhilta. Lisäksi laitteisiin saatavilla olevat virustentorjuntaohjelmat ovat työkalu uhkien minimoinnissa. [11]

Roskapostien huomaaminen voi olla käyttäjälle vaikeaa sillä niiden lähettäjät usein esittävät tietoa jonkun luotettavan tahon nimissä. Roskapostin torjuntaan on kehitetty suodattimia, jotka etsivät sähköposteista haitallista sisältöä. Tietojenkalasteluhyökkäysten osalta uhkien minimoinnissa tärkeintä on käyttäjän tietoturvakoulutus, jotta käyttäjä osaa tunnistaa mahdollisen tietojenkalastelun tunnusmerkit. Tämä on haastavaa, sillä hyökkäykset on valmisteltu uskottavan näköisiksi. [13]

Laitteiden päivitysten asentaminen ja ohjelmistojen pitäminen ajan tasalla on tärkeä osa tietoturvauhkien ehkäisyssä. Päivitykset korjaavat löydettyjä aukkoja laitteen tai ohjelmiston tietoturvassa. Monet tiedossa olevat haavoittuvuudet ovat hyökkääjälle helppoja toteuttaa, kun hyökkäys kohdistetaan päivittämättömään laitteeseen. Osa tietoturvatoteutuksesta on mahdollista ulkoistaa Internet-palveluntarjoajalle. Palveluntarjoajan tietoturvaratkaisut, kuten haittaohjelmien havainnointi ja käyttäjän tarkan verkko-osoitteen salaaminen, auttavat minimoimaan käyttäjään kohdistuvia tietoturvauhkia. [11]

Teknisiä ratkaisuja tietoturvauhkien minimointiin ovat palomuurit, virustentorjuntaohjelmistot ja tunkeutumisenestojärjestelmät. Dataa voidaan myös suojata sa-

lausalgoritmien avulla ja se voidaan sulkea salasanasuojauksen taakse. [15]

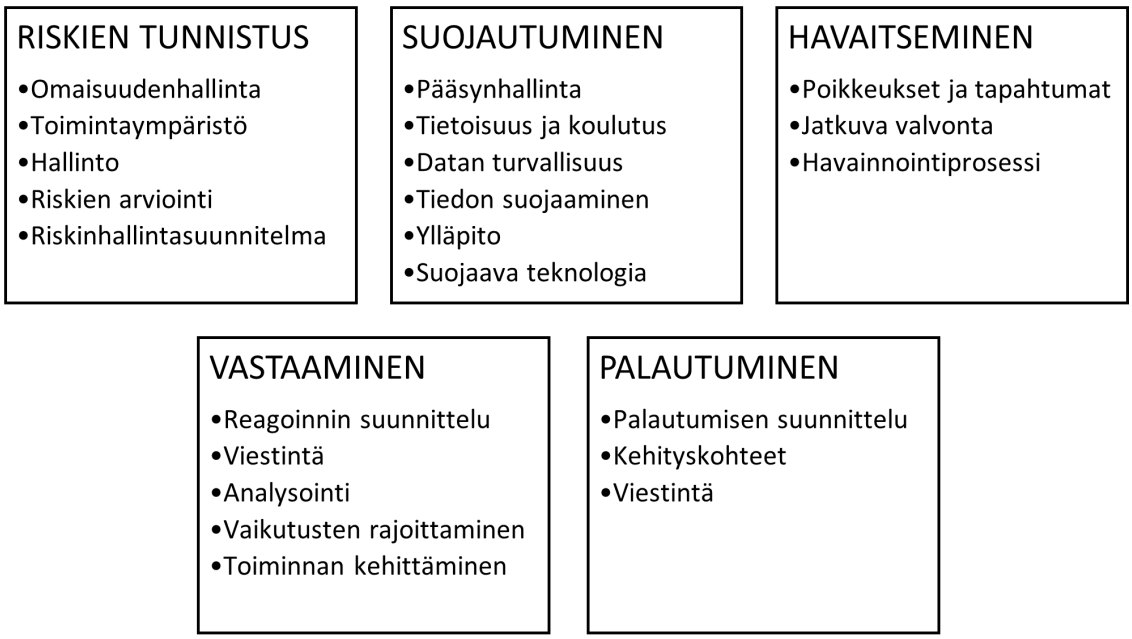
Palomuurit ovat tietoverkkolaitteita, jotka suodattavat niiden läpi kulkevaa verkkoliikennettä. Parhaan tietoturvan saavuttamiseksi kaiken verkkoliikenteen lähiverkon ja internetin välillä tulee kulkea palomuurin läpi ja vain tietyn tyyppinen luotettu verkkoliikenne saa päästä siitä ohi. Virustentorjuntaohjelmisto käy läpi laitteella olevia tiedostoja ja etsii niistä haittaohjelmia. Ohjelmiston käyttämiä tekniikoita ovat ohjelmien koon vertailu muistissa olevan eheän ohjelman koon kanssa ja ohjelman toiminnan seuraaminen ja suorituksen aikaisten poikkeavuuksien tarkkailu.

Tietoturvauhkien minimoimiseksi kaikki tallennettu data tulee suojata salaamalla se salausalgoritmien avulla. Salausalgoritmeja on kehitetty useita erilaisia, jotka voidaan toimintaperiaatteen mukaan symmetrisiin ja epäsymmetrisiin salausalgoritmeihin. Symmetrisissä algoritmeissa data salataan ja salaus puretaan samalla salausavaimella. Epäsymmetrisissä, eli julkisen avaimen algoritmeissa salaukseen ja salauksen purkamiseen käytetään eri avaimia. [15]

3.3 Tietoturva yritysten toiminnassa

Yritysten tietokoneet ovat yleisesti paremmin suojattuja kuin kotikäyttäjien tietokoneet. Yrityksillä on usein käytössään tietoturvakäytänteitä, joita työntekijöiden tulee seurata. [11] Kyberhyökkäyksien ja kyberuhkien lisääntyessä myös organisaatioiden tietoturvaan liittyvät kustannukset on kasvaneet. Vaikka osa yrityksistä on vähentänyt tietoturvainvestointejaan koska hyökkäyksiä on vaikea havainnoida. [16]

Yritysten tietoturvatoimintaan on kehitetty useita erilaisia viitekehyksiä ja standardeja, jotka auttavat tietoturvaloukkausten hallinnassa. Yksi esimerkki tällaisesta standardista on Yhdysvaltain standardointi- ja teknologiainstituutin (NIST) kehittämä tietoturva viitekehys, joka toimii yritysten apuna tietoturvariskien minimoinnissa ja on kehitetty olemassa olevien hyvien käytänteiden, ohjeiden ja standardien avulla. [15]



Kuva 3.1: NIST tietoturvan viitekehyksen funktiot [17]

Tämän viitekehys jakautuu viiteen ydin funktioon, jotka ovat riskien tunnistus, suojautuminen, havaitseminen, vastaaminen ja palautuminen. Nämä ydinfunktiot on vielä jaettu eri kategorioihin ja alikategorioihin, joista jokainen sisältää niihin liittyviä tietoturvatavoitteita ja ratkaisuja.

Riskien tunnistus pitää sisällään tietoturvariskien ymmärtämiseen ja hallintaan liittyviä ohjeita. Sen avulla yritys voi tunnistaa dataan, henkilöstöön, laitteisiin ja järjestelmiin liittyviä tietoturvariskejä. Suojautuminen pitää sisällään riskeiltä suojautumiseen tarvittavien turvajärjestelmien kehittämisen ja toimeenpanon välineitä. Suojautumisen funktio liittyy etenkin yrityksen kriittisen infrastruktuurin suojaukseen. Havaitsemisfunktio sisältää käytänteitä tietoturvaloukkauksen tai tietoturvatapahtuman havainnointiin. Havainnoinnin lisäksi funktio keskittyy tapahtuman mahdollisten vaikutusten ymmärtämiseen. Vastaamisen funktio auttaa havaitun tietoturvatapahtuman oikeanlaisessa käsittelyssä. Vastaaminen sisältää hyviä toimintatapoja käsittelyn koordinointiin ja vaikutusten minimointiin. Palautumisen funktio

käsittelee tietoturvatapahtuman jälkeisiä toimintoja ja niiden järjestelmien ja toimintojen palauttamista joihin tapahtuma vaikutti. [17]

Niissä yrityksissä, joissa noudatetaan hyvin määriteltyjä tietoturvakäytänteitä työntekijät pitävät tietoturvaa ja tietoturvaloukkausten ehkäisemistä huomattavasti tärkeämpänä kuin niissä, joissa ei ole tietoturvakäytänteitä käytössä. Tietoturvakäytänteitä noudattavien yritysten työntekijät pitävät paremmin huolta myös henkilökohtaisesta tietoturvastaan ja osaavat suojautua tietoturvauhkia vastaan. [18]

Tietoturvallisuuteen kohdistuvista uhista suurin osa voidaan linkittää käyttäjiin tai käyttäjien toimiin. Käyttäjiin kohdistuvien uhkien ohella myös käytössä oleviin järjestelmiin voi kohdistua uhkia, jotka ovat käyttäjistä riippumattomia, joko heikon päivitystahdin tai konfiguraation kautta. Yrityksiin ja yksilöihin kohdistuvat tietoturvauhat ovat luonteeltaan erilaisia, mutta yritysympäristössä työntekijöihin kohdistuu myös yksilötason uhkia. Uhkiin on mahdollista varautua useilla eri tavoilla, niin teknisesti kuin koulutuksenkin kautta. Tapojen samanaikainen hyödyntäminen ja usean kerroksen puolustuksen rakentaminen on tehokkain tapa varautua niin yritystä, kuin yksilöäkin kohtaan kohdistuviin tietoturvauhkiin.

Aineiston pohjalta voidaan todeta, että tietoturvauhkiin varautumiseen ja vastaamiseen on käytössä useita teknisiä ja hallinnollisia keinoja. Tietoturvakäytänteiden luominen ja seuraaminen sekä useiden eri varautumis- tai vastaamiskeinojen yhtäaikainen käyttö on tehokkainta tietoturvan kannalta. Tietoturva on käsitteenä laaja, joten uhkia ja haasteita on myös tunnistettu paljon ja monimuotoisesti. Uhat pystytään karkeasti jaottelemaan joko laitteisiin ja järjestelmiin tai käyttäjiin kohdistuviin uhkiin.

4 Etätyön tietoturva

Etätyöhön kohdistuu samoja tietoturvaongelmia, kuin työnantajan tiloissa tehtävään työhön. Niiden lisäksi työskentelypaikan ollessa joku muu kuin työnantajan tila tietoturvallisuuteen kohdistuu myös muita etätyölle ominaisia tietoturvauhkia. Siksi yritysten tulee muokata olemassa olevia tietoturvakäytänteitään etätyöhön sopivaksi tai kehittää täysin uudet tietoturvakäytänteet etätyöskentelyä varten. [1]

4.1 Etätyöskentelyn tietoturvariskit

Etätyöhön kohdistuu samoja tietoturvariskejä kuin työnantajan tiloissa työskentelyyn. Erityisesti etätyöhön liittyviä riskejä ovat työntekijän kotona yhteiskäytössä olevat tietokoneet, epäluotettavien tietoverkkojen käyttö tai etätyöskentelyn aikana työntekijän olan yli tapahtuva tietojen katselu. [1] Yhteiskäytössä olevat tietokoneet voivat mahdollistaa ulkopuolisten henkilöiden pääsyn arkaluontoiseen dataan, tietoihin tai ohjelmistoihin, joihin heillä ei ole käyttöoikeutta. Perhe voi jakaa yhteisen tietokoneen, jota yksi perheenjäsen käyttää myös etätyöskentelyyn. Tällaista konetta voidaan jopa käyttää saman käyttäjän ja salasanan kanssa.

Julkisten tietoverkkojen käyttöön liittyy useita tietoturvauhkia. Suojaamattomat yleiset tietoverkot ovat yksityisiä verkkoja huomattavasti alttiimpia tietoturvahyökkäyksille. Verkon yli kulkeva tieto on salaamatonta, joten hyökkääjän on helppo kaapata tällaisen verkon yli kulkevaa liikennettä ja päästä käsiksi verkossa liikkuvaan tietoon. Suojaamattoman verkon yli tiedon saa haltuunsa usein salaamattomana,

jolloin hyökkääjä pääsee vaivattomasti katselemaan kaapattua tietoa. [19]

Fyysistä tietojenkalastelua voi tapahtua, kun julkisella paikalla etätyötä tehdessä ulkopuolinen henkilö pääsee käsiksi tietoon tai järjestelmään, johon hänellä ei ole oikeutta. Julkisilla paikoilla, kuten junassa tai kahvilassa, liikkuu paljon ihmisiä ja voi olla vaikea havaita arkaluontoista tietoa havittelevia hyökkääjiä. Jopa puolelle etätyöskentelevistä ei ole määritelty vaatimuksia työympäristölle tai työvälineistön säilytykseen. [20]

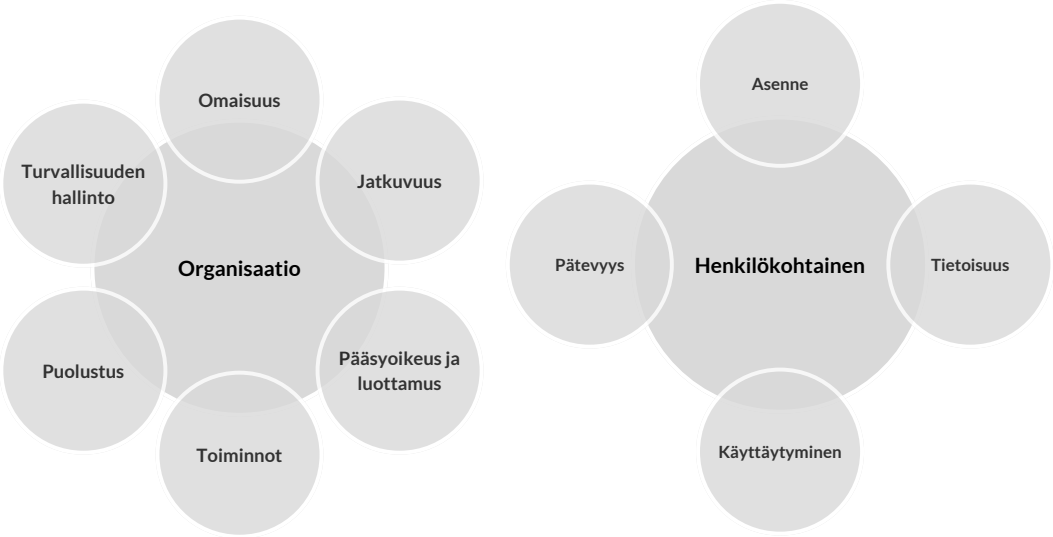
Etätyöskentelyssä käytettyihin päätelaitteisiin liittyy myös teknisiä uhkia. Uhkia kohdistuu niin yksityiseen kuin yhteisessä käytössä oleviin laitteisiin. Yhteiskäytössä olevilla laitteissa uhat korostuvat usean eri käyttäjän vuoksi. Tällaisia uhkia ovat laitteen salauksen murtaminen ja näin kirjautuneena käyttäjänä esiintyminen, laitteella tehtyjen toimien salaaminen ja laitteelle murtautuminen verkkoyhteyden avulla. Myös fyysiset muistilaiteet, kuten USB-muistitikut ja ulkoiset kovalevyt muodostavat tietoturvauhan, sillä ne voidaan varastaa tai kadottaa. [21]

Norjassa kartoitettiin yritysten edustajien näkemyksiä yritystensä tietoturvallisuudesta. Heidän tunnistamistaan uhista suurin on osassa järjestelmissä käytössä olevat jaetut käyttäjätunnukset ja salasanat, jotka aiheuttavat tietoturvariskin. Tietoturvauhat nähtiin laajenemassa IT-järjestelmistä mahdollisesti myös tuotantolaitoksiin ja niissä käytössä olevien järjestelmiin ja laitteisiin. Tutkimuksen mukaan yritysten edustajat odottavat tietoturvaan liittyen etenkin tietoturvatilanteen valvontaa, valvottuja etätyöskentelytiloja ja yrityksessä käytössä olevien vaatimusten ja prosessien noudattamista. [22]

Pandemian aikana etätyöhön siirtyneiden joukossa eniten tietoturvaan liittyviä uhkia on havaittu tietojenkalastelun muodossa. 15,15 prosenttia siirtyneistä havaitsivat jonkinlaista tietojenkalastelua. Tämä on huomattavasti enemmän kuin muita tietoturvauhkia. Muista tietoturvauhista havaitsi haittaohjelmia, kuten viruksia tai vakoiluohjelmistoja 4.55 prosenttia ja kiristysohjelmia 3.79 prosenttia siirtyneistä.

Tietojen menetystä tai hakkerointia havaittiin aikaisempiin verrattuna vähän. On myös huomattu, että vanhemmat työntekijät havaitsivat uhkia useammin kuin nuoremmat. [23]

Tietoturvauhkiin varautumiseen ja uhkien muodostumiseen liittyy erilaisia osa-alueita yksilöjen ja yritysten näkökulmasta. Uhkien muodostumisen kannalta on luotu tietoturvakulttuurin malli, jonka osa-alueet vastaavat osin tietoturvauhkien kohteita. Yksilön näkökulmasta on tärkeää asennoitua tietoturvallisuuteen toimintaan ja pitää osaamisensa ajan tasalla. Yritysten kohdalla on mietittävä useampia eri osa-alueita, jotka liittyvät omistettuun tietoon, puolustuksen suunnitteluun sekä hallinnollisen tietoturvan toteuttamiseen. [23]



Kuva 4.1: Tietoturvakulttuurin malli [23]

Tutkimuskysymyksen yksi osalta voidaan siis todeta, että etätyöskentelyyn kohdistuu yleisesti työympäristössä huomioitavien uhkien lisäksi myös vain etätyöhön liittyviä uhkia. Näihin kuuluvat tilat, jotka eivät ole työnantajan tai yrityksen hallinnassa, julkiset työskentelyyn käytettävät tietoverkot sekä yksittäisen työntekijän

korostunut vastuu tietoturvan ylläpidosta. Etenkin työntekijän vastuu korostuu, sillä erilaiset tietojenkalasteluhyökkäykset ovat erittäin yleisiä ja kohdistuvat yksittäisiin työntekijöihin. Työskentelyyn käytettyihin päätelaitteisiin kohdistuu myös enemmän uhkia valvomattomassa ympäristössä.

4.2 Tietoturvasuositukset etätyöskentelyyn

Turvalliseen etätyöskentelyyn ja sen mahdollistamiseen on tietoturvariskien pohjalta tehty useita suosituksia. Niissä on käsitelty esimerkiksi työntekijöiden tietoturvaosaamisen kehittämistä ja työnantajan sovellusten ja järjestelmien suojaamista. Huoltovarmuuskeskuksen julkaiseman ohjeistuksen pääkohdat tietoturvalliseen etätyöskentelyyn ovat verkkoyhteyksien suojaaminen, käyttäjien tunnistaminen, sisällön suojaus ja roolien määrittäminen, ohjelmien ja laitteistojen päivitys sekä työntekijöiden kouluttaminen riskien tunnistukseen. Jokaisen osa-alueen yhtäaikainen onnistuminen takaa parhaat edellytyksen turvalliseen etätyöhön.

Erityisesti etätyössä huomioitavia asioita on myös yksilöity suosituksissa. Niihin kuuluvat tiedon suojaaminen yrityksen ulkopuolisilta, kuten työntekijän perheenjäseniltä, ja yrityksen ulkopuolisten oheislaitteiden ja latureiden käytön välttäminen. Työntekijöitä suositellaan vaihtamaan kodin IoT (Internet of Things) laitteiden oletussalasanat turvallisemmiksi. Myös ulkomaan matkoihin ja niiden aiheuttamaan riskiin kehotetaan varautumaan. [20]

Yrityksen kannalta on huomattu, että etätyöskentelyyn siirryttäessä tietoturvallisuus käytäntöjen noudattamisen valvonta ja varmistaminen on IT-osastolle haastavaa. Työntekijöiltä on turvallisten yhteyksien varmistamiseksi vaadittava vpn yhteyden käyttöä. VPN on tietoverkkoratkaisu, joka luo salatun tunnelin yrityksen verkon ja työntekijän laitteen välille. Yrityksen on hyvä myös vaatia pilvipalvelujen käyttöä työntekijältä, jotta työntekijän omalle tai muuten työnantajan hallitsemattomissa olevalle laitteistolle ei tallennettaisi suoraan arkaluontoista tietoa. Tällöin

kaikki yrityksen data pysyy yrityksen hallitsemilla laitteilla. [19]

Tietoturvalliseen päätelaitteen huomiointi on yritysten tietoturvan kannalta tärkeää. Etätyöskentelyyn käytettyjen laitteiden käyttöjärjestelmät, asetukset tai sovellukset eivät usein ole yrityksen IT-osaston hallittavissa. Varsinkaan jos kyse on työntekijän omasta laitteesta. Tällaisten laitteiden tietoturvallisen käytön varmistaminen on yritykselle vaikeaa ilman hallintaoikeuksia. Yrityksen tuleekin vaatia, että etätyöskentelyyn käytetään vain yrityksen tarjoamia tai hyväksymiä laitteita. Jos laite ei ole yrityksen tarjoama on myös mahdollista käyttää erillistä ohjelmistoa tai usb-laitetta työntekijän oman laitteen yhteydessä, joka mahdollistaa yritykselle hallinnan heille tärkeisiin turvaominaisuuksiin. Näitä turvaominaisuuksia voivat olla vpn tunnelin käytön varmistaminen tai päätelaitteen sijainnin paikannus, jotta voidaan varmistaa laitteen luvallinen käyttö, jos etätyötä ei haluta mahdollistaa täysin vapaasti valittavassa paikassa. [21]

Laitteen valintaan suositellaan määrittämään yrityksen sisäiset vaatimuslistaukset. Yritysten on tarpeellista kartoittaa etätyövälineiden käyttötapauksia, joiden perusteella yritys voi valita itselleen sopivimmat työkalut. Välineiden oletusasetuksiin tutustuminen on tärkeää, jotta tietoturvallinen käyttö voidaan varmistaa luottamatta valmistajan omiin tietoturvamäärityksiin. Yrityksen on myös hyvä huomioida käytetäänkö etätyöhön hyödynnettävissä sovelluksissa pilvipalvelua vai yrityksen tiloihin asennettua järjestelmää. [24]

Työntekijöiden autentikointi on etätyössä erittäin tärkeää. Vuonna 2017 kaikista tietoturvaloukkauksista 81 prosenttia hyödynsi hyökkäyksessä varastettua tai heikkoa salasanaa ja 43 prosenttia loukkauksista olivat sosiaalisia käyttäjiin kohdistuneita hyökkäyksiä. Autentikointiin suositellaan siksi käytettävän monivaiheista autentikointia. Siinä salasanan lisäksi käytetään jotakin muuta käyttäjän todennustapaa samanaikaisesti. Tällainen tapa voi olla biometrinen tunnistus, älypuhelinsovellus tai tarkoitukseen suunniteltu erillinen laite, joka antaa yksilöidyn kirjautumiskoo-

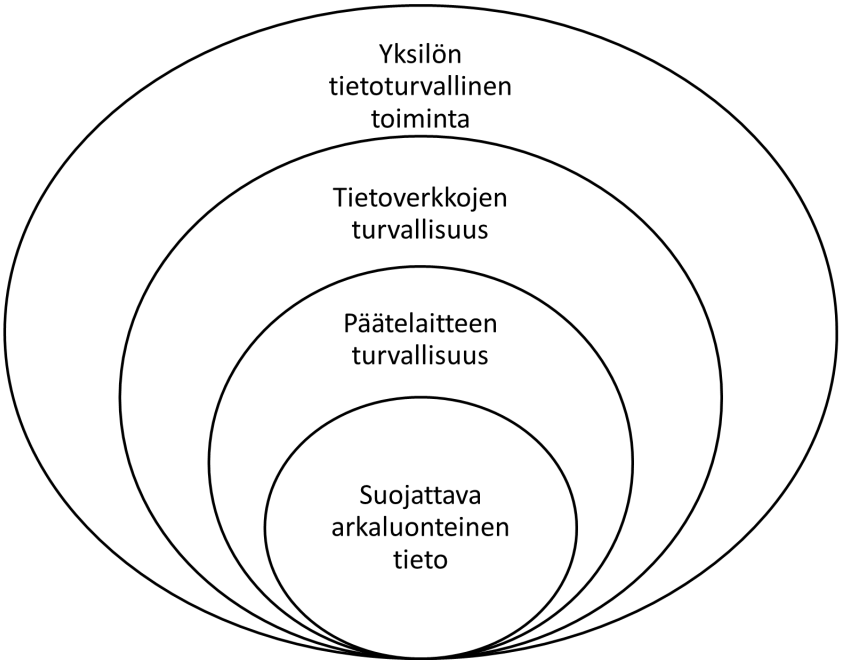
din jokaisen kirjautumisen yhteydessä. [21]

Myös yritysten tekemissä sopimuksissa asiakkaiden ja toimittajien kanssa on tärkeä mainita tietoturvavaatimuksista. Haastatellut yritysten edustajat pitivät tärkeänä, että tietoturvaan liittyvistä asioista on sovittu virallisesti sellaisiin projekteihin tai tuotteisiin liittyvissä sopimuksissa, joihin liittyy mahdollisia tietoturvauhkia. [22]

Työntekijät ovat yritykselle yhä tärkein investointikohde tietoturvallisuuden toteutumisen kannalta. Jopa 53 prosenttia etätyöntekijöistä ei ollut saanut mitään etätyöskentelyn tietoturvaan liittyvää ohjeistusta työnantajaltaan. Niistä työntekijöistä, joilla ei ollut mahdollisuutta etätöihin ennen koronapandemian mahdollistamaa muutosta 44.44 prosenttia ei saanut mitään ohjeita tietoturvaan liittyen etätyöskentelyyn siirtyessä [23]. Ohjeistusten laadinnassa onkin tärkeää huomioida työntekijöiden koulutuksen tärkeys. Tietoturvallisuus vaatii enemmän huomiota jokaisella osa-alueella. Suurin osa yrityksistä, jotka olivat luoneet käytäntöjä ja ohjeistusta etätyöskentelyyn keskittyivät enemmän yrityksen sisäisen verkon turvaamiseen tiedon turvaamisen sijasta. Teknisiin toimintoihin, kuten VPNn käyttöön keskityttiin enemmän kuin salasanojen hallintaan tai kalasteluhyökkäysten torjuntaan. [23].

Suosituksia on siis tehty useita erilaisia, joista osa keskittyy tietoturvallisuuteen yleisesti, osa etätyön tietoturvaan ja osa johonkin sen osa-alueeseen. Toistuvia teemoja suosituksissa ovat yrityksen toimintaympäristön ja suojattavien tietojen kartoitus ja dokumentointi, tietoliikenneyhteyksien suojaus sekä työntekijöiden opastus ja koulutus. Sisäisten tietoturvaohjeiden ja määräysten merkitys nousee myös esille monessa suosituksessa. Suositusten pääsanoma on yleensä usean eri keinon hyödyntäminen tietoturvauhkien minimointiin, jotta puolustus ei jäisi vain yhden minimointikeinon varaan.

Tutkimuskysymykseen kaksi vastauksena löytyy suosituksia laajasti ja erilaisiin yrityksiin organisaatioihin suunnattuina. Suosituksia on julkaistu monien eri tahojen, kuten valtiollisten tietoliikennevirastojen toimesta. Suosituksissa korostuu eten-



Kuva 4.2: Esimerkki usean tietoturvakeinon yhtäaikaisesta käytöstä

kin tietoturvasuunnitelman tekeminen ja sen noudattaminen sekä usean tietoturvaratkaisun yhtäaikainen käyttö. Usea ratkaisu parantaa tietoturvaa merkittävästi. Parhaita teknisiä käytänteitä on myös koottu suosituksiin, mutta tekninen toteutus on jätetty pieneen osaan yritysten ja teknisten ympäristöjen moninaisuuden vuoksi. Parannusta tietoturvakulttuuriin tarvitaan usealla eri osa-alueella ja laajasti. Suositukset on julkaistu pääosin valtiollisten organisaatioiden toimesta tai tieteellisen tutkimusten pohjalta tehtyjen julkaisujen ohessa.

5 Yhteenveto

Tietoturvan osalta etätyössä kohdataan laajalti samoja haasteita kuin työnantajan tiloista tehtävässä toimistotyössäkin. Yleisesti hyväksi todetut tietoturvakäytänteet pätevät niin lähityössä, kuin etätyöskentelyssäkin. Etätyön ainutlaatuinen ympäristö tuo kuitenkin lisähaasteita tietoturvaan. Etätyössä liikutaan paljon ja töitä voidaan tehdä monenlaisessa ympäristössä ja monenlaisilla välineillä. Toimistotyössä työvälineitä ja ympäristöä on usein mahdollista valvoa ja suojata paremmin tietoturvauhkia vastaan.

Etenkin valvomattomien tietoverkkojen ja työntekijöiden käyttämien omien laitteiden tietoturvaan on kehitetty useita suosituksia ja käytänteitä. Tietoturvallisin ratkaisu on välttää näiden laitteiden käyttöä mahdollisimman paljon ja suosia yrityksen omistamia ja hallinnoimia ratkaisuja. Toinen mahdollisuus tällaisten laitteiden suojaamiseen ovat tietoturva ja hallintasovellukset, jotka antavat yrityksen it-osastolle mahdollisuuden seurata ja hallita kyseisiä laitteita.

Työntekijöille etätyössä tärkeää on työympäristön huomiointi, sekä mukana kuljetetun informaation suojaus. Etätyötä voidaan tehdä paikoissa, jotka ovat julkisia ja vartioimattomia, joka altistaa työntekijöitä tietoturvauhille. Työntekijöille tärkeimpiä suosituksia onkin työympäristön tarkkailu. Julkisilla paikoilla työskenneltäessä on oltava tarkkana siitä, mitä tietokoneen näytöllä näkyy. Yrityksen informaation päätymistä muiden kuin sallittujen käyttäjien haltuun on tärkeä varoa etenkin silloin, kun liikutaan hallitun toimistoympäristön ulkopuolella.

Etätyöskentelyyn on yritysten avuksi luotu useita suosituksia. Suosituksia on niin yleisellä tasolla kuin yksityiskohtaisesti tietyille osa-alueille. Suomessa Kyberturvakeskus on luonut etätyöskentelyyn liittyviä suosituksia. Yksi suosituksista käsittelee turvallisten etätyövälineiden valintaa, jossa käsitellään työskentelyssä käytettäviä sovelluksia ja niiden turvallisia valintakriteerejä. Kyberturvallisuuskeskus on myös julkaissut ohjeen turvalliseen etätyöhön, jossa on avattu teknisiä ja toiminnallisia käytänteitä tietoturvallisuuden varmistamiseksi. Myös muiden maiden kansalliset tietoturvatoimijat ovat julkaisseet omia suosituksiaan tietoturvalliseen etätyöhön.

Suosituksissa korostuu usean tietoturvaratkaisun yhtäaikainen käyttö ja puolustuksen kerroksittainen rakennus. Nämä ovat etätyössä vähintään yhtä tärkeitä kuin toimisto-olosuhteissakin. Yritysten ei tule luottaa siihen, että yksittäinen etätyöhön suunniteltu tietoturvaratkaisu tekee etätyön täysin tietoturvalliseksi. Turvallisuuden maksimoinniksi on myös etätyöhön rakennettava tehokas tietoturvajärjestelmä ja toimintatavat yrityksen sisällä. Suositusten seuraamiseen liittyy myös haasteita. Suosituksien päällekkäisyys ja joidenkin suositusten ristiriitaisuus keskenään voi vaikeuttaa yrityksen valintaa siitä mitä suosituksista on kannattavaa seurata. Joidenkin käytäntöjen seuraamisella on myös suuret taloudelliset kustannukset, jotka voivat vaikuttaa yrityksen päätökseen toteuttaa suositusten vaatimuksia.

Tärkeimpänä keinona yrityksille tietoturvauhkien minimoinnissa on työntekijöiden tietoturvataitojen kehitys ja varmistus. Käyttäjät ja käyttäjien toiminta on todettu suurimmaksi tietoturvapoikkeusten aiheuttajaksi. Yrityksen tietoturvaympäristö paranee huomattavasti, kun työntekijöillä on tarpeeksi osaamista havaita tietojenkalasteluyrityksiä tai muita tietoturvauhkia. Teknisesti tietoturvaympäristöä on mahdollista vahvistaa yrityksen IT- tai tietoturvaosaston hallinnoimien päätelaitteiden ja hallitun verkkoympäristön avulla. Erilaiset tekniset ratkaisut, kuten VPN-ratkaisut etätyöskentelijän laitteiden yhdistämiseksi yrityksen sisäverkkoon tuovat lisäturvallisuutta siihen verrattuna, että liikenne kulkee julkisen internetin yli. Hal-

linnollisesti tärkeitä ovat vahvat yrityksen sisäiset tietoturvakäytännöt, joiden noudattamista valvotaan. Tutkimuskysymykseen kolme vastatessa löytyy siis useita erilaisia teknisiä ja hallinnollisia keinoja, joita on järkevä käyttää mahdollisimman laajasti.

Jatkossa tutkimuksen pohjalta olisi mielenkiintoista tutkia yleisimpien käytäntöjen tehokkuutta uhkien minimoinnissa. Käytäntöjen olemassaolon perustelu on tärkeää, jotta käytettävät resurssit voidaan suunnata oikein mahdollisimman tehokkaan uhkien minimoinnin onnistumiseksi. Yritysten monimuotoisuuden vuoksi eri kokoisten yritysten tietoturvavalmiuksien ja käytäntöjen seuraamisen kartoittaminen voisi olla kiinnostava aihe tehdä tarkempaa tutkimusta.

Lähdeluettelo

[1] H. Koyama, Y. Nakagawa, S. Tanimoto, T. Endo, T. Hatashima ja A. Kanai, "Risk Assessment of Telework for the New Normal Era", teoksessa *2021 IEEE 10th Global Conference on Consumer Electronics (GCCE)*, 2021, s. 496–497. DOI: 10.1109/GCCE53005.2021.9621909.

[2] J. Morales-Arilla ja C. Daboin, "Is Remote Work in High Demand? Evidence from Job Postings during COVID-19", teoksessa *ACM SIGCAS Conference on Computing and Sustainable Societies*, sarja COMPASS '21, Virtual Event, Australia: Association for Computing Machinery, 2021, s. 27–37, ISBN: 9781450384537. DOI: 10.1145/3460112.3471984.

[3] M. H. Olson, "Remote Office Work: Changing Work Patterns in Space and Time", *Commun. ACM*, vol. 26, nro 3, s. 182–187, maaliskuu 1983, ISSN: 0001-0782. DOI: 10.1145/358061.358068.

[4] D. Ford, M.-A. Storey, T. Zimmermann et al., "A Tale of Two Cities: Software Developers Working from Home during the COVID-19 Pandemic", *ACM Trans. Softw. Eng. Methodol.*, vol. 31, nro 2, joulukuu 2021, ISSN: 1049-331X. DOI: 10.1145/3487567.

[5] L. Yang, D. Holtz, S. Jaffe ja S. Suri, "The Future of Information Work", *Commun. ACM*, vol. 65, nro 7, s. 27–29, kesäkuu 2022, ISSN: 0001-0782. DOI: 10.1145/3538638.

[6] J. M. Barrero, N. Bloom ja S. Davis, ”60 Million Fewer Commuting Hours Per Day: How Americans Use Time Saved by Working from Home”, Becker Friedman Institute for Research In Economics, Working Papers 2020-132, 2020. url: https://EconPapers.repec.org/RePEc:bfi:wpaper:2020-132.

[7] C. Weinert, C. Maier, S. Laumer ja T. Weitzel, ”Does Teleworking Negatively Influence IT Professionals? An Empirical Analysis of IT Personnel's Telework-Enabled Stress”, teoksessa *Proceedings of the 52nd ACM Conference on Computers and People Research*, sarja SIGSIM-CPR '14, Singapore, Singapore: Association for Computing Machinery, 2014, s. 139–147, ISBN: 9781450326254. DOI: 10.1145/2599990.2600011.

[8] C. P. Ruppel ja S. J. Harrington, ”Telework: An Innovation Where Nobody is Getting on the Bandwagon?”, *SIGMIS Database*, vol. 26, nro 2–3, s. 87–104, toukokuu 1995, ISSN: 0095-0033. DOI: 10.1145/217278.217288.

[9] J. C. Messenger ja L. Gschwind, ”Three generations of Telework: New ICTs and the (R)evolution from Home Office to Virtual Office”, *New Technology, Work and Employment*, vol. 31, nro 3, s. 195–208, 2016. DOI: https://doi.org/10.1111/ntwe.12073.

[10] A. Verma, R. Surendra, B. Reddy, P. Chawla ja K. Soni, ”Cyber Security in Digital Sector”, teoksessa *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, 2021, s. 703–710. DOI: 10.1109/ICAIS50930.2021.9395933.

[11] E. Kritzinger ja S. von Solms, ”Home user security- from thick security-oriented home users to thin security- oriented home users”, teoksessa *2013 Science and Information Conference*, 2013, s. 340–345.

[12] S. L. Jones, E. I. M. Collins, A. Levordashka, K. Muir ja A. Joinson, ”What is 'Cyber Security'? Differential Language of Cyber Security Across the Li-

fespan", teoksessa *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, sarja CHI EA '19, Glasgow, Scotland Uk: Association for Computing Machinery, 2019, s. 1–6, ISBN: 9781450359719. DOI: 10.1145/3290607.3312786.

[13] J. Malgeri, "Cyber Security: A National Effort to Improve", teoksessa *2009 Information Security Curriculum Development Conference*, sarja InfoSecCD '09, Kennesaw, Georgia: Association for Computing Machinery, 2009, s. 107–113, ISBN: 9781605586618. DOI: 10.1145/1940976.1940998.

[14] L. Li, L. Xu, W. He, Y. Chen ja H. Chen, "Cyber Security Awareness and Its Impact on Employee's Behavior", teoksessa *Research and Practical Issues of Enterprise Information Systems*, A. M. Tjoa, L. D. Xu, M. Raffai ja N. M. Novak, toim., Cham: Springer International Publishing, 2016, s. 103–111, ISBN: 978-3-319-49944-4.

[15] J. Srinivas, A. K. Das ja N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations", *Future Generation Computer Systems*, vol. 92, s. 178–188, 2019, ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2018.09.063.

[16] N. Kesswani ja S. Kumar, "Maintaining Cyber Security: Implications, Cost and Returns", teoksessa *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, sarja SIGMIS-CPR '15, Newport Beach, California, USA: Association for Computing Machinery, 2015, s. 161–164, ISBN: 9781450335577. DOI: 10.1145/2751957.2751976.

[17] M. Barrett, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, en, huhtikuu 2018. DOI: https://doi.org/10.6028/NIST.CSWP.04162018.

[18] L. Li, W. He, L. Xu, A. Ivan, M. Anwar ja X. Yuan, "Does Explicit Information Security Policy Affect Employees' Cyber Security Behavior? A Pilot Study", teoksessa *2014 Enterprise Systems Conference*, 2014, s. 169–173. DOI: 10.1109/ES.2014.66.

[19] H. Koyama, Y. Nakagawa, S. Tanimoto, T. Endo, T. Hatashima ja A. Kanai, "A Study of Risk Assessment Quantification for Secure Telework", teoksessa *2022 12th International Congress on Advanced Applied Informatics (IIAI-AAI)*, 2022, s. 574–580. DOI: 10.1109/IIAIAAI55812.2022.00115.

[20] Huoltovarmuuskeskus, *Ohjeita turvalliseen etätyöhön*, https://www.huoltovarmuuskeskus.fi/files/7f58b0da92e4f19003e0c4a7337c71c8c37c5bef/ohjeita-turvalliseen-etatyohon.pdf, Luettu: 11.1.2023.

[21] K. Bicakci, Y. Uzunay ja M. Khan, "Towards Zero Trust: The Design and Implementation of a Secure End-Point Device for Remote Working", teoksessa *2021 International Conference on Information Security and Cryptology (ISCTURKEY)*, 2021, s. 28–33. DOI: 10.1109/ISCTURKEY53027.2021.9654298.

[22] L. Bodsberg, T. O. Grøtan, M. G. Jaatun ja I. Wærø, "HSE and Cyber Security in Remote Work", teoksessa *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 2021, s. 1–8. DOI: 10.1109/CyberSA52016.2021.9478249.

[23] A. Georgiadou, S. Mouzakitis ja D. Askounis, "Working from home during COVID-19 crisis: a cyber security culture assessment survey", *Security Journal*, vol. 35, s. 486–505, 2022, ISSN: 1743-4645. DOI: https://doi.org/10.1057/s41284-021-00286-2.

[24] Huoltovarmuuskeskus, *Ohjeita turvallisten etätyövälineiden valintaan*, https://www.huoltovarmuuskeskus.fi/files/62f911a5aca6873bb95053068d4dc3bb92c50801/turvalliset-etatyovalineet-2021.pdf, Luettu: 7.1.2024.