Tietoturva etätyössä. Miten varmistetaan tiedon luottamuksellisuus?

Natalia Degen

Haaga-Helia ammattikorkeakoulu

Amk-opinnäytetyö

2021

Tradenomin tutkinto

Tiivistelmä

Tekijä(t)
Natalia Degen

Tutkinto
Tradenomi

Raportin/Opinnäytetyön nimi
Tietoturva etätyössä. Miten varmistetaan tiedon luottamuksellisuus?

Sivu- ja liitesivumäärä
43

Keväällä 2020 alkaneen maailmanlaajuisen pandemian seurauksena suuri määrä ihmisiä siirtyi tekemään etätyötä hyvin nopealla aikataululla. Aikaa siirtymän suunnitteluun oli vain vähän ja osalla työntekijöistä oli vain vähän tai ei lainkaan kokemusta etänä tehtävästä työstä. Opinnäytetyössä kartoitettiin, miten tietoturva toteutuu etätyössä tiedon luottamuksellisuuden säilyttämisen näkökulmasta.

Tietoperustassa käsiteltiin riskien arviointia, CIA-mallia, luottamuksellisuutta sekä erilaisia niin fyysiseen ympäristöön ja ihmiseen kuin ohjelmiin, laitteisiin sekä verkkoon liittyviä tietoturvariskejä.

Opinnäytetyössä kartoitettiin, millaista kirjallisuutta aiheesta on saatavilla ja millaisia toimintatapoja työpaikoilla yleisesti on käytössä tietoturvan parantamiseksi. Työssä käsiteltiin myös inhimillisten tekijöiden eli ihmisen toiminnan vaikutusta tietoturvan tasoon ja mahdollisiin riskeihin.

Menetelmäksi valikoitui kirjallisuuskatsaus ja sen periaatteita noudatetaan työssä soveltaen. Tässä tapauksessa kirjallisuuskatsauksen sovellettava muoto on kuvaileva kirjallisuuskatsaus.

Tietoturvasta oli saatavilla paljon materiaalia ja tietoturvaa oli tutkittu paljon. Saatavilla oli erityisesti paljon kaupallisia ja ei-kaupallisia ohjeita. Tutkimustietoa löytyi sekä englanninkielisenä että suomenkielisenä.

Tietoturvaa ja tiedon luottamuksellisuutta vaarantavat erityisesti ihmisen oma toiminta, tiedon puute sekä tietoturvalliseen työskentelyyn soveltumattomat laitteet ja ohjelmistot. Koulutus ja motivaatio nousivat avainasemaan tietoturvallisessa työskentelytavassa. Ennaltaehkäisyn merkitys oli suuri riskien realisoitumisen torjunnassa. Hyvin valitut, riittävän pitkät salasanat, tunnistautumismenetelmät sekä yksityisen erillisverkkojen (VPN) käyttö lisäsivät tietoturvallisuutta ja tiedon luottamuksellisuuden säilyttämistä. Myös organisaation sisäisellä ohjeistuksella olisi suuri merkitys.

Asiasanat
Tietoturva, etätyö, luottamuksellisuus, riski

Sisällys

1 Johdanto 1
1.1 Taustaa aiheenvalinnalle 1
1.2 Tutkimuskysymykset 3
2 Tietoperusta 6
2.1 Etätyö 6
2.2 Riskien arviointi 7
2.3 Tiedon luottamuksellisuus ja tietoturva 8
2.3.1 CIA-malli 9
2.4 Tietoturva työpaikalla 10
2.5 Fyysinen ympäristö 10
2.6 Verkon tietoturva 11
2.7 Tietoturvan kerroksellisuus 11
2.8 VPN 12
2.9 OSI-malli 13
2.9.1 Salasanat 14
2.9.2 Autentikointi ja auktorisointi 14
2.9.3 Kertakirjautuminen 15
2.10 Päätelaitteen suojaus 16
2.11 Tietoturvariskit verkossa 17
2.12 Kohdennetut hyökkäykset 18
2.13 WLAN-verkko 18
2.13.1 Tyypilliset hyökkäykset WLAN-verkossa 18
2.14 Tietoturvarike 19
2.15 Tietojenkalastelu 20
2.16 Kyberrikollisuus 20
2.17 Sosiaalinen media 21
2.18 GDPR 22
2.19 Tietoturvallisuuden lisääminen 22
3 Empiirinen osa 23
3.1 Menetelmäkuvaus 23
3.2 Tulokset 24
3.2.1 Salasanojen käyttö 25
3.2.2 Salasanojen hallinnointi 26
3.2.3 Kertakirjautuminen (SSO) 27
3.2.4 Kryptaus 29
3.2.5 RSA 30
3.2.6 VPN 31

3.2.7 Ihmisen toiminta 32
3.2.8 Kouluttautuminen 33
3.2.9 Kyberhyökkäysten torjunta 35
3.2.10 Zero trust -ajattelu 36
3.2.11 Automaatio ja tekoäly 37
3.2.12 Työskentely kotitoimistolla 38
3.2.13 Etätyöskentelyyn liittyvät riskit 38
3.2.14 Avoimet WLAN-yhteydet 40
3.2.15 Turvallinen etätyöympäristö 40
3.3 Johtopäätökset ja oppimisprosessi 42
3.4 Jatkotutkimusaiheet 43
Lähteet 45

1 Johdanto

Opinnäytetyöni aihe on tietoturva ja siihen liittyvät uhat etätyössä. Tarkoituksenani on tutkia, millä tavoin etätyö vaikuttaa yritysten, yrityksen asiakkaiden tietoturvaan sekä toisaalta työntekijöiden toimintaan. Rajaan työni koskemaan tiedon luottamuksellisuuden säilyttämisen näkökulmaa kartoittamalla keinoja, joita kirjallisuuden mukaan käytetään tietoturvallisuuden säilyttämiseen. Luottamuksellisen tiedon päätymistä vääriin käsiin on yritettävä estää kaikin käytössä olevin keinoin. Tietoturva on monitahoinen ja monimutkainen prosessi, jossa vuorovaikuttavat niin inhimillinen toiminta kuin pitkälle hiotut, modernit tekniset ratkaisut. Työssäni käsittelen tietoturvaa työntekijän ja yrityksen näkökulmasta tuoden esiin yleisimpi riskejä ja uhkia sekä keinoja siihen, ettei riski realisoituisi.

1.1 Taustaa aiheenvalinnalle

Etätyöskentelystä on tullut osa arkipäivää monen ihmisen elämässä koronapandemian puhjettua keväällä 2020. Taudin levittyä laajalle paineet saada mahdollisimman moni työskentelemään etänä kasvoi. Yritysten oli tehtävä toimintaansa nopeita muutoksia. Ratkaisuja jouduttiin tekemään muutaman viikon aikana ja osittain siirtymä erilaisiin etätyövälineisiin ei ollut enää hallinnassa. (Traficom 2020c, 6)

Tietoturva on yrityksen imagolle elintärkeä elementti ja toimivat ratkaisut vaikuttavat olennaisesti siihen, miten yritys menestyy kilpailussa muiden yritysten kanssa. (Teknologiateollisuus.) Pk-yrityksistä 60 % hakeutuu konkurssiin maaliin saadun kyberhyökkäyksen jälkeen. (Virkkunen 2020). Kyberrikolliset ovat nähneet pandemiatilanteessa mahdollisuutensa ja myös heidän toimintansa edellytyksen ovat kasvaneet, kun suuret määrät ihmisiä työskentelee verkon välityksellä. Eritoten palvelunestohyökkäysten määrä nousi vuonna 2020. (Traficom 2020c, 6)

Aihe on puhuttanut jo ennen koronapandemiaa ja etätyöskentelyä on harjoitettu edeltävästikin. Aiheesta on saatavilla runsaasti materiaalia niin koronapandemian edeltävältä ajalta kuin pandemian puhkeamisen jälkeiseltä ajalta. Vaikka pandemiatilanteen kanssa on eletty jo kohta kaksi vuotta, on tilanne nopean etätyöhön siirtymisnopeuden vuoksi osittain edelleen uusi.

Tietoturvan luottamuksellisuuden toteutuminen on tärkeää yksilön, yrityksen sekä esimerkiksi valtion oikeusturvan kannalta. Kaikilla on oikeus luottamukselliseen tietojen käsittelyyn ja toisaalta tietoa on käsiteltävä luottamuksellisesti. Tietojen käsittelyn on aina pohjattava tietosuojalainsäädäntöön. (Valvira 2020.)

Tietoturvallisuuden rikkoutuminen on aina vakava tilanne ja se voi vaarantaa yksilön turvallisuuden lisäksi kokonaisen valtion tai sen elimen turvallisuuden. Euroopan lääkevirasto EMA:aa vastaan hyökättiin tekemällä tietomurto juuri ennen, kun heidän piti hyväksyä koronarokote. Kybervakoilu kohdistuu niin valtioihin, poliittisiin elimiin kuin yksittäisiin yrityksiin. (Traficom 2020c, 6.)

Tietoturvalliseen työskentelyyn on kiinnitettävä huomiota ja oikeanlaiseen toimintatapaan voidaan tehdä ohjeistuksia. Ohjeistuksen tulee aina nojata tieteellisen tutkimuksen tutkimustuloksiin. Yritykset hyötyvät tutkimuksesta, kun tutkimusten pohjalta on mahdollista luoda uusittuja ohjeita uuden tilanteen edessä.

Nykyaikana tietoturva on todella tärkeä osa jokapäiväistä elämää. Teknologia tuo niin mahdollisuuksia kuin haasteitakin. Erityisesti on kiinnitettävä huomiota luottamuksellisuuteen ja yksityisyyden suojaan. (Järviö 2018, 3.) HP:n teettämän laajan tutkimuksen mukaan enemmän kuin puolet yritysten johtajista on havainnut, että esimerkiksi lunnasvaatimuksia sisältävien hyökkäysten määrä on kasvussa (Korkiakoski 2021.)

Korona-pandemian aikana tietojenkalasteluyritysten sekä varsinaisten kyberhyökkäysten määrät ovat kasvaneet kymmenillä prosenteilla. Organisaatioihin, jotka ovat aiemmin pääosin saaneet olla rauhassa hyökkäyksiltä, on nyt kohdistettu hyökkäyksiä. Näitä ovat pienet yritykset sekä teollisuusyritykset. Yritykset eivät ole riittävän valmistautuneita hyökkäysten varalta, aiemmin hyökkäyksiltä suojautuminen on ollut helpompaa yrityksen suljetun, oman sisäverkon ansiosta. Pandemian pitkittyessä on yrityksissä painetta päivittää tietoturvastrategioitaan suojautuakseen paremmin hyökkäyksiltä suuren osan työntekijöistä työskennellessä etänä. (Ahtokivi 2021.)

Pandemian aikana kyberturvallisuusuhissa ovat korostuneet työntekijöiden inhimilliset virheet, kun töitä tehdään kotoa käsin. Rikolliset pääsevät hyödyntämään tietoturva-aukkoja tehokkaasti esimerkiksi työntekijän huolimattomuuden tai peräti tietämättömyyden vuoksi. Erilaiset huijausviestit sekä hyökkäykset todennäköisesti jatkavat lisääntymistään jatkossakin. (Huhtaniitty 2021.) Kyberturvallisuuskeskus on koronavuoden aikana kertonut heille tulleen tietoon kaksinkertaisen määrän tietoturvaa uhkaavia riskejä aiempaan verrattuna. (Uitti 2021).

Pandemian jälkeenkin on todennäköistä, että etätyöskentely jää osaksi työkulttuuria paljon laajemmin kuin ennen pandemiaa on totuttu. Kuten jo edellä todettiin, etätyöskentely luo tietoturvalle uusia haasteita. Yritysten on tämän vuoksi keskityttävä henkilöstön

kouluttamiseen, hyökkäysten tunnistamiseen sekä jo toteutuneiden riskien torjuntaan. Rikolliset tuottavat niin sanottuja access-as-a-service-palveluja hyökäten yritysten järjestelmiin. Etä- ja lähityötä tehdään tulevaisuudessa todennäköisesti niin sanotun hybridimallin mukaan. Työntekijä, joka työskentelee kotikoneella, on erityisen hyvä kohde verkkorikolliselle, koska tämän laitteen kautta on mahdollista päästä käsiksi niin yrityksen kuin henkilön henkilökohtaisiin tietoihin. (Trend Micro 2020)

Tulevaisuuden IoT-laitteet ja tekoälytoteutukset vaativat entistä enemmän tietoturvaratkaisuja. Vuonna 2019 tuli voimaan EU:n kyberturvallisuusasetus, joka ottaa kantaa tietoturvan sertifiointijärjestelmään. Tulevaisuudessa tämän järjestelmän pohjalta suunnitellaan myös IoT-laitteille sertifiointijärjestelmä. IoT-laitteiden haavoittuvuudet mahdollistavat pelottavan usein sen, että hyökkääjä ottaa laitteen etähallintaansa. Haavoittuvuuksiin olisikin puututtava pikaisesti. (Traficom 2020c 15,18.)

1.2 Tutkimuskysymykset

Opinnäytetyöni tarkoituksena on selvittää, miten pandemiatilanne vaikuttaa yritysten tietoturvaratkaisuihin. Seuraaviin kysymyksiin on tarkoitus etsiä vastauksia:

1. Mitä keinoja yrityksillä on käytössään tietoturvalliseen työskentelyyn?
2. Mitä uusia uhkia pandemiatilanne on tuonut tietoturvalle yrityksissä?
3. Onko teoriatiedon ja siihen nojaavien käytäntöjen välillä ristiriitaisuuksia?

<u>Keskeisiä käsitteitä:</u>

Fyysinen ympäristö: ympärillämme olevat fyysiset asiat ja esineet. Tietoturvan yhteydessä laitteistot. Fyysiseen ympäristöön kuuluu paikka, jossa työtä tehdään, yleensä koti tai työpaikka.

GDPR: EU:n tietosuoja-asetus, joka on tullut sovellettavaksi keväällä 2018 kaikissa EU:n jäsenmaissa.

Kyberrikollisuus: tietoverkossa tapahtuva rikollisuus, jossa rikos voi tapahtua kokonaan tai vain osittain verkossa.

Oikeudet esimerkiksi tietokantaan: henkilölle myönnetty oikeus kirjautua järjestelmään tai järjestelmän osaan. Oikeuksia voidaan rajata tai laajentaa tarpeen mukaan.

Phishing: tietojenkalastelu tietoverkossa. Rikollinen pyrkii erehdyttämään uhria paljastamaan esimerkiksi käyttäjätunnuksia tai salasanoja päästäkseen niiden avulla käsiksi luottamukselliseksi tai salattavaksi luokiteltavaan tietoon.

Rikoslainsäädäntö: ajantasainen lainsäädäntö koskien rikoksia sekä niistä langetettavia rangaistuksia. Lainsäädäntö sisältää myös ennakkotapauksia rikoksista.

Riskinhallinta: prosessit ja niihin sisältyvät toiminnot ja toimintatavat haitallisten asioiden estämiseksi tai niiden vaikutusten minimoimiseksi.

Salasanat: henkilökohtaiset, salassa pidettävät merkkijonot, joilla käyttäjä pääsee kirjautumaan järjestelmiin tai sen osiin.

Salaus: menetelmät ja toimenpiteet, joilla salassa pidettävän tiedon joutuminen ulkopuolisten saataville estetään.

Salausmenetelmät: sisältyy salaukseen. Sisältää ne toimintatavat, joilla salataan tietoverkossa olevat data.

Tiedon jakaminen: tässä asiayhteydessä tiedon jakamisella tarkoitetaan datan jakamista asiakkaan tai kollegojen kanssa. Tiedon jakaminen voi tapahtua reaaliajassa esimerkiksi Teams-kanavan välityksellä tai tietoa voi jakaa chatissa tai sähköpostissa ja erilaisilla foorumeilla ja verkkosivuilla. Tiedon jakaminen voi olla tarkoituksenmukaista tai tahatonta, viimeksi mainittuun liittyy aina tietoturvariski.

Tietomurto: verkossa tai fyysisessä ympäristössä tehtävä rikos, jossa rikollinen pääsee käsiksi häneltä salattavaksi tarkoitettuun tietomateriaaliin.

Tietoturvapoikkeama: tilanne, jossa riskinhallinta on pettänyt täysin tai osittain. Saattaa johtaa siihen, että salattavaa tietoa päätyy henkilöille, joille se ei kuulu. Tietoturvapoikkeama ei välttämättä johda tietovuotoon vaan muodostaa sille riskin.

Tietovuoto: tiedon päätyminen vääriin käsiin tietoturvapoikkeaman seurauksena. Tietovuoto luokitellaan riskinhallinnassa riskin realisoitumiseksi.

Tunnistautuminen: sisältää erilaisia menetelmiä ja protokollia, joilla varmistutaan siitä, että henkilö on juuri se, joka kertoo olevansa. Tunnistautumisella voidaan lisätä tiedon luottamuksellisuutta ja tunnistautuminen on usein moniportaista usein kolmannen

osapuolen varmentamaa. Tunnistautuminen on kriittinen tekijä luottamuksellisen tiedon välittämisessä verkon yli oikeille tahoille.

Verkon suojaus: sisältää kaikki fyysiset suojausmenetelmät, virustorjunnan sekä tunnistautumisen ja salauksen, joilla suojataan verkko ulkopuolisilta tunkeilijoilta. Suojauksessa käytetään erilaisia tasoja ja toteutustapoja.

Virustorjunta: liittyy läheisesti sekä sisältyy verkon suojaukseen, kattaa sekä palomuurin että virustorjuntaohjelmistot, joilla pyritään estämään haittaohjelmien ja viruksien pääsy järjestelmään

.

VPN: virtuaalinen, yksityinen erillisverkko, joka toimii julkisen tietoverkon sisällä sisältäen erilaisia salausmenetelmiä. Erilaisia VPN-ratkaisuja on käytössä esimerkiksi yrityksillä, ja tunnistautumismenetelmät sallivat työntekijän liittymisen yrityksen erillisverkkoon julkisen verkon yli vaikkapa kotoa käsin.

2 Tietoperusta

Tietoturvasta yleisellä tasolla on saatavilla paljon materiaalia ja sitä on myös tutkittu paljon. Saatavilla on erityisesti paljon kaupallisia ja ei-kaupallisia ohjeita. Tutkimustietoa on saatavilla niin englanninkielisenä kuin suomenkielisenäkin. Tämän opinnäytetyön pohjana käytän pääosin ei-kaupallista materiaalia sen vuoksi, että kaupallisen aineisto voi joskus koostua osin puolueellisestä sisällöstä. Jonkin verran mukana on myös kaupallista aineistoa. Käytäntöön sovellettava, toiminnan suunnittelu vaatii pohjalle tutkittua tietoa.

Vaikka etätyötä ja siihen kiinteästi liittyvää tietoturvaa on tutkittu paljon, on poikkeustila tuonut molempiin aivan uusia ulottuvuuksia. Etätyötä tekivät ennen pandemiaa pääosin henkilöt, jotka olivat siihen halukkaita tai olosuhteiden pakosta sitä syystä tai toisesta joutuivat tekemään. Valtaosa työstä tehtiin kuitenkin työpaikan tiloissa. Pandemiatilanne aiheutti sen, että suuret määrät etätyöhön tottumattomia henkilöitä siirtyi nopealla tahdilla kotiin tekemään töitä (Traficom 2020, 6). Yritykset ja työpaikat olivat aivan uuden tilanteen edessä. Oli kehiteltävä toimintatapoja ja menetelmiä, joilla tieto ei vaarannu. Dataa liikkuu verkossa huomattavasti enemmän etätyön aikana kuin pandemiaa edeltävänä aikana. (Yli-Korhonen 2020.)

Ennakointi on yksi tärkeimpiä asioita niin kriisitilanteiden aikana kuin normaalitilassakin. Ilman suunnittelua ja huolellista perehtymistä asiaan ajaudutaan nopeasti ongelmiin. Laadunvalvonta nousee tärkeäksi elementiksi. (Tulevaisuusvaliokunta 2020, 233.) Ennakointiin ja näyttöön perustuvaan toimintaan tarvitaan tueksi tutkittua tietoa.

Aiheesta tietoturva etätyössä löytyy muutamia tutkimuksia sekä pro-gradu -tutkielmia. Opinnäytetyöni tavoitteena on tuottaa koottu tutkimus kirjallisuuskatsauksen periaatteita soveltaen, millaista tietoa on saatavilla ja mitä käytännön toimia voidaan hyödyntää pandemiatilanteessa turvallisen etätyöskentelyn mahdollistamiseksi. Tuloksia voidaan hyödyntää laajemmin yrityksissä sekä jokainen yksilö omassa etätyöskentelyssään.

2.1 Etätyö

Etätyö on työtä, jota voidaan tehdä työpaikan tilojen ulkopuolella sovitusti. Etätyössä paikka ja aika eivät ole sidoksissa työpaikan tiloihin tai kaikissa tilanteissa edes säännölliseen työaikaan. Työtä voidaan tehdä joko kokonaan etänä tai sitten käytössä voi olla niin sanottu hybridityö, jossa tehdään osanaikaa etätyötä, osan aikaa lähityötä.

Etätyö on sanan perinteisen merkityksen mukaisesti työmuodon osalta vapaaehtoisuuteen perustuvaa ja joustavaa työtapaa, jota ohjaavat yhteiset säännöt ja ohjeistukset. Säännöt ja ohjeistukset sovitaan ennalta ja töitä voidaan tehdä paikasta riippumatta jopa perinteisestä toimistotyöajasta joustaen. (Työsuojelu 2020.) Keväällä 2020 etätyö sai perinteisen määritelmänsä lisäksi uuden määritelmän maailmanlaajuisen pandemian vuoksi, kun siitä poistui perustuvuus vapaaehtoisuuteen. Työnantajat määräsivät etätyöhön suuren määrän henkilöstöään. Yksi neljäsosa henkilöstöstä ei ollut tehnyt etätyötä aiemmin ja siihen liittyvät käytänteet ovat ennestään vieraita. Tämä toi suuren riskin yritysten tietoturvalle. (Heljaste 2020.)

Lainsäädännöllisesti etätyö on vieras käsite, eikä etätyötä määritellä Suomen laissa. Työsuhteisiin liittyvä lainsäädäntö on kuitenkin pohjana myös etätyössä. Työntekoa sääteleviä lakeja ovat työsopimuslaki, työaikalaki ja työturvallisuuslaki. (Työsuojelu 2020.)

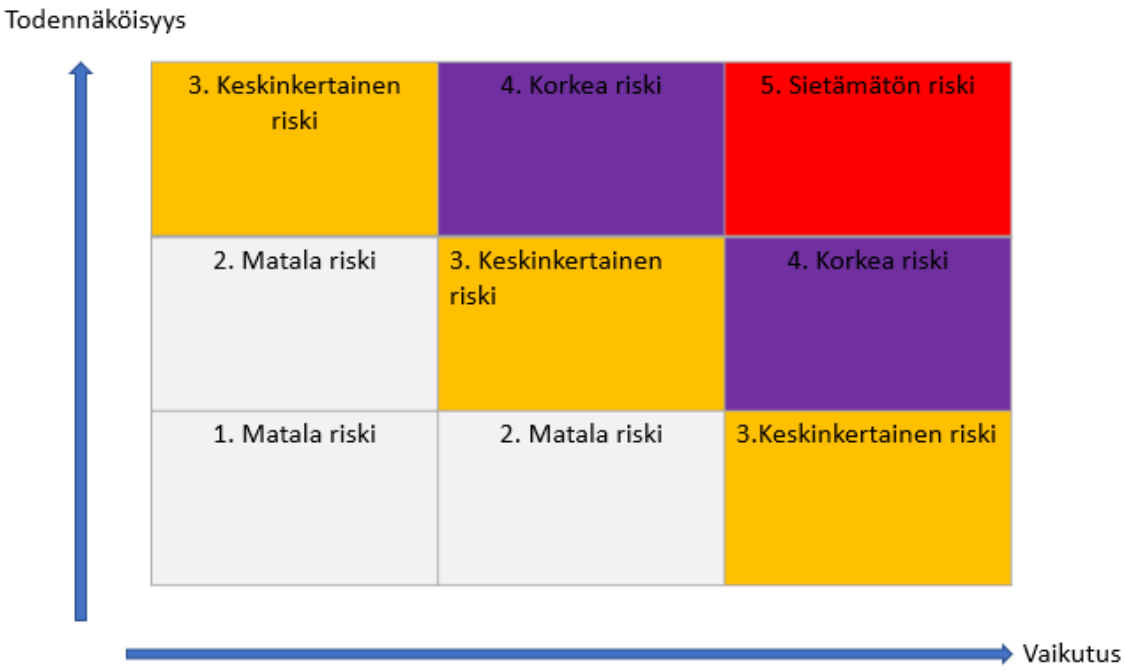
Etätyön yleistyessä ovat muodostuneet myös erilaiset hyväksi havaitut toimintatavat, joita noudatetaan joustavasti työnteossa. Käytännöistä on apua arjen työtilanteissa ja ne lisäävät työn sujuvuutta. Etätyöhön liittyviä käytäntöjä sovitaan monesti kirjallisessa muodossa. Sovittavia asioita ovat muun muassa etätyön tekemisen edellytykset, työaika, tulosten seuranta, sairasloma- ja muut poissaolokäytännöt, tietoturvaan liittyvät asiat sekä kustannuskysymykset. On tärkeää sopia etukäteen, miten toimitaan esimerkiksi tietoturvapoikkeamatilanteissa (Työsuojelu 2020.)

2.2 Riskien arviointi

Riskien suuruuden tai todennäköisyyden arviointi ei ole aina helppoa. Apuna voidaan kuitenkin käyttää erilaisia mittareita. Riskin arviointi ei ole aukotonta tai helppoa mutta yleisesti hyväksytyn taulukon tai muun mittarin käyttö tekee arvioinnista helpompaa. (Meurman 2021.)

Yleisesti käytössä on riskitaulukko, jossa on vaihteleva määrä ruutuja. Riskin riskiluku voidaan määrittää kertomalla keskenänsä riskin vaikuttavuus ja riskin todennäköisyys. Riskiluvun kasvaessa riskiin täytyy reagoida ja mahdollisesti ryhtyä toimenpiteisiin. Toimenpiteillä riskilukua voidaan madaltaa. (Meurman 2021.)

Kaikkia riskejä ei voida poistaa eikä siihen pyritä, mutta riskinhallinnalla voidaan kartoittaa ne riskit, jotka ovat vaikuttavuudeltaan tai todennäköisyydeltään suurimpia ja voisivat realisoituessaan aiheuttaa mittavia vahinkoja esimerkiksi yritykselle tai yhteisölle. (Meurman 2021.)



Kuva 1. Taulukko riskin arvioinnin avuksi (mukaillen Saarola)

Yllä oleva taulukko on tyypillinen riskien arviointiin käytettävä taulukko. Vaakasuunnassa on merkitty kasvavaksi riskin vaikutus luvulla 1–3. Pystysuunnassa on merkitty kasvavaksi riskin todennäköisyys luvuilla 1–3. Pienin mahdollinen riski on vasemmalla alhaalla ja suurin mahdollinen riski oikealla yläkulmassa.

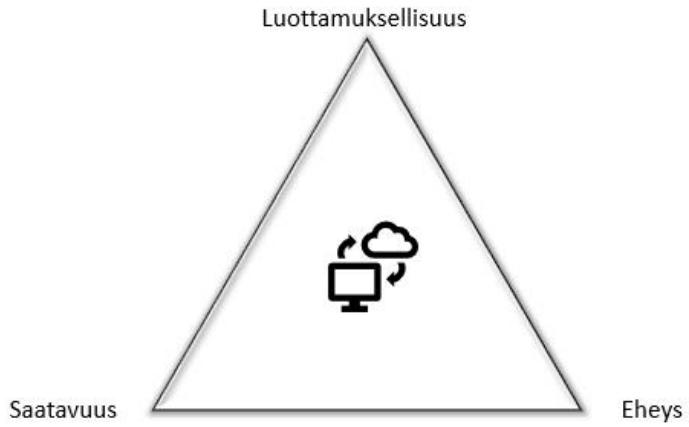
Taulukko perustuu brittiläiseen BS8800 menetelmään. Riskejä arvioidaan sen mukaan, mikä niiden todennäköisyys ja vaikuttavuus on. (Saarola.)

2.3 Tiedon luottamuksellisuus ja tietoturva

Tietoturvan yksi osa-alue on tiedon luottamuksellisuuden säilyttäminen. Teknologiset ratkaisut eivät yksin riitä ratkaisemaan tietoturvaan liittyviä ongelmia, vaan tietoturvaan liittyy erilaisia prosesseja, toimintatapoja sekä inhimillisiä tekijöitä. Tietoturvaa voidaan kuvata CIA-mallin avulla, jossa tietoturva jaetaan tiedon luottamuksellisuuteen, tiedon saatavuuteen sekä tiedon yhteneväisyyteen. Tietoturva edellyttää hyökkääjien identifioimista, hyökkääjien motiivien selvittämistä sekä tietoisuutta siitä, mitä mahdolliset riskit ovat. On myös tiedostettava ja huomioitava mahdolliset haavoittuvuudet järjestelmissä. (Livinus 2017, 1.)

2.3.1 CIA-malli

CIA-mallissa kuvaillaan tietoturvan kolmea tärkeää osa-aluetta, luottamuksellisuus, eheys sekä saatavuus. Tiedon luottamuksellisuuden näkökulmasta tiedon liikkuessa verkossa vain tietyillä tahoilla on oikeus päästä tietoon käsiksi, ja lopuilla siihen ei ole oikeutta. Oikeudet voivat olla rajattuja ja jollakin taholla voi olla vain oikeus osaan tiedosta. Mikäli väärät tahot pääsevät käsiksi tietoihin, voi seurauksena olla suuria ongelmia. Tiedon eheyden näkökulmasta tarkasteltuna tiedon tulee pysyä sellaisena, kuin se on alkuperäisestikin ollut eli muutokset tiedoissa ovat vain tarkoituksenmukaisia. Eheys tarkoittaa siis sitä, että asiaankuulumattomat tahot eivät pääse tietoa muokkaamaan. Eheyteen kuuluu myös se, ettei tieto muutu vahingossa. Tiedon saatavuus tarkoittaa sitä, että tieto on saatavilla silloin, kun sitä tarvitaan. (Livinus 2017, 1)



Kuva 2. CIA-malli (mukaillen Wesley 2021)

2.4 Tietoturva työpaikalla

Tietoturvan tavoitteena on suojata järjestelmiä ja tietoaineistoja ja sen keinoja ovat erilaisen tekniset sekä hallinnolliset ja toiminnalliset ratkaisut organisaation sisällä, joilla varmistetaan tiedon luottamuksellisuuden, eheyden sekä tiedon saatavuuden säilyttäminen. (Tietosuojavaltuutetun toimisto.) Tietoturva voidaan jakaa karkeasti kahteen osaan: organisaation hallinnollisiin menettelytapoihin sekä teknisiin toimenpiteisiin. Tekniset toimenpiteet tukevat työntekijöiden tietoturvallista toimintaa mahdollistamalla tarvittavat puitteet. (Järvinen& Rousku 2017.) Organisaatiossa on tärkeää jakaa vastuut niin, että ne ovat kaikille selkeitä ja hyvin jaettuja. (BLC 2018).

Yritysten liiketoiminnan laajetessa ja digitalisaation edetessä kyberturvallisuusriskit kasvavat väistämättä. Kyberturvallisuus tulisikin olla osa liiketoimintastrategiaa automaattisesti eikä siitä erillinen osa-alue. Kokonaisvaltainen tietoturva on kaiken keskiössä eikä pelkkä palomuuri ratkaise ongelmaa. (Korkiakoski 2021.)

2.5 Fyysinen ympäristö

Fyysinen ympäristö on perusta tietoturvallisen työskentelyn toteuttamiselle. Fyysinen ympäristö suojaa yrityksen omaisuutta ja tiloja ulkopuolisilta. Fyysisiä suojattavia tiloja ovat ne, joihin ulkopuolisilla henkilöillä ei tule olla pääsyä. Fyysiseen turvallisuuteen kuuluvat muun muassa tilat, kulunvalvonta sekä kameravalvonta. (Heljaste 2020.)

Kotona työskentely tekee fyysisen turvallisuuden toteuttamisen hankalammaksi kuin työpaikalla. Kotien turvallisuus vaihtelee paljon. Muut perheenjäsenet kotona aiheuttavat riskin tietoturvalliselle työskentelylle. Työssä käsiteltävät luottamukselliset asiat eivät kuulu ulkopuolisille, joihin työn tekemisen kannalta kuuluvat muut perheenjäsenet. Tietokoneelta on mahdollista päästä halutessaan käsiksi salassa pidettäviin tietoihin, ellei tehokkaasta suojauksesta pidetä huolta. (Heljaste 2020.)

Asianmukaisia työtiloja voi olla hankala järjestää esimerkiksi pienissä kerrostaloasunnoissa ja riskit monikertaistuvat, kun kotitoimistoja on valtaosan tehdessä etätyötä jopa tuhansia. Työpaikalla fyysiset tilat ovat helppo tarkastaa, mutta työnantajalla ei ole oikeutta eikä mahdollisuuksia puuttua kodin ympäristöön. Tilanne on uusi, koska siinä joudutaan pakon edessä yhdistämään yksityinen elämä ja työelämä.

2.6 Verkon tietoturva

Kun töitä tehdään työpaikan tiloissa, on työn tekemiseen tarkoitetut koneet liitetty samaan työpaikan verkkoon suoraan. Etätyötä tehdessä koneet liitetään työntekijän kotiverkon avulla yrityksen yksityiseen sisäverkkoon erilaisia suojaus- ja autentikointimenetelmiä hyödyntäen VPN-yhteyden avulla. Yritykset yleensä huolehtivat koneittensa ja verkkojensa tietoturvaohjelmistoista. (Heljaste 2020.) Kotiverkon turvallisuus on kuitenkin työntekijän omien toimenpiteiden ja ratkaisujen varassa ainakin osittain.

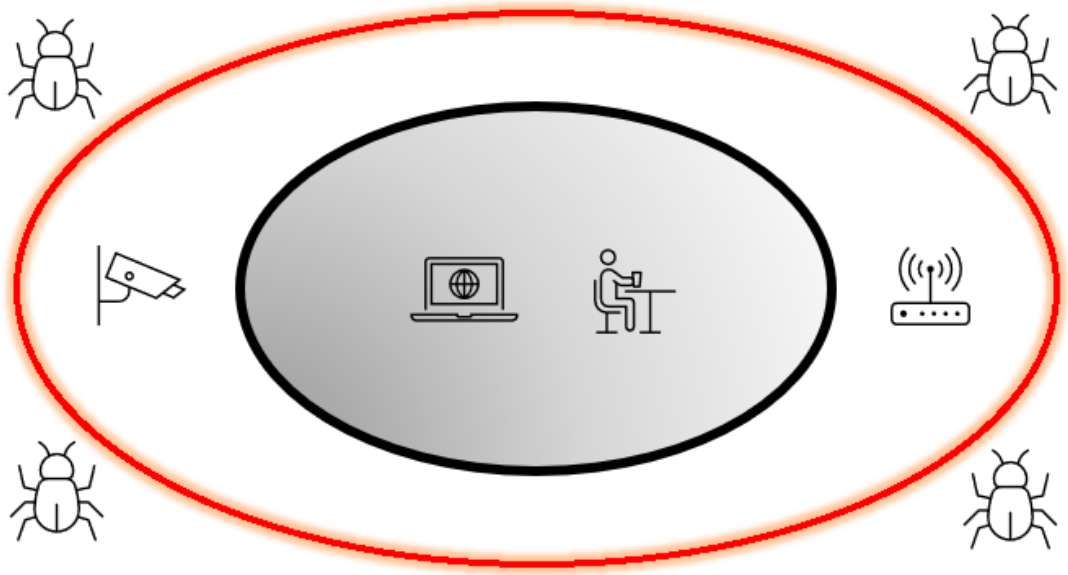
Etätyö on erityisen riskialtista, jos sitä tehdään avoimissa, julkisissa verkoissa. Mikäli jostain syystä oma kone pitäisi liittää julkiseen, langattomaan verkkoon, suositellaan rakennettavaksi oma suojattu sisäverkko eli VPN (virtual private network). VPN-ratkaisussa tietoliikenne ohjataan oman väliaseman kautta ja verkkoliikenteen pitäisi olla ainakin ulkopuolisilta salattua. (BLC 2018.)

2.7 Tietoturvan kerroksellisuus

Tämän päivän työntekijöillä on usein käytössään monia eri päätelaitteita, joiden kautta on mahdollista päästä käsiksi työhön liittyviin sovelluksiin ja dokumentteihin. Käytössä on myös usein suuri määrä erilaisia sovelluksia. Monien sovellusten ja useiden päätelaitteiden kautta rikollisten reitit kohteeseen ovat moninkertaiset. Ei riitä, että pelkkä päätelaite suojataan. On muistettava suojata esimerkiksi sähköpostipalvelut sekä tiedostojen jakamiseen tarkoitetut palvelut. (Vesajoki 2018.)

Tietoturvan kerroksellisuudesta puhutaankin silloin, kun uhat pyritään estämään jo ennen kuin ne päätyvät päätelaitteelle. Päätelaite on yhteydessä työpaikan sisäverkkoon ja aiheuttaa uhan tietoturvalle, mikäli uhka pääsee laitteelle saakka. Suojauksen tulisi olla kerroksellista. Suuri osa uhkista eli haittaohjelmista, huijauksista ja kiristyksistä päätyy päätelaitteelle sähköpostin kautta. Sähköpostiin tulevat tietojenkalasteluviestit ovat hankalia siinä mielessä, etteivät ne aina sisällä haitalliseksi luokiteltavaa linkkiä tai liitettä ja näin ollen sähköpostivistit pääsevät perinteisen suojauksen läpi. Sähköpostin tietoturvaan tuleekin yrityksissä kiinnittää huomiota. (Vesajoki 2018.)

Kerroksellinen tietoturva on monitahoinen järjestelmä, jota voitaisiin kuvata esimerkiksi kehämallin avulla (BLC 2018).



Kuva 3. Kerroksellinen tietoturva

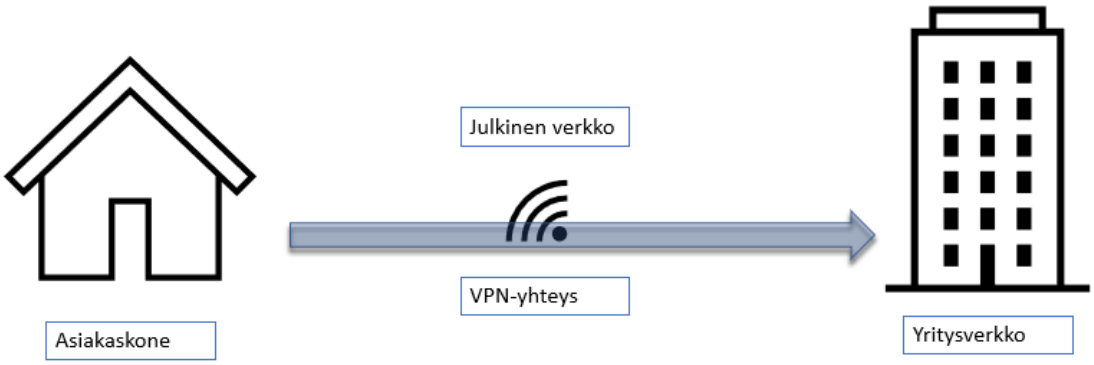
Kehän sisäosassa ovat työntekoon tarkoitetut laitteet sekä työntekijät. Uloimmalla kehällä sijaitsee verkon tietoturva. Riskien realisoitumista tulee pyrkiä estämään suojaamalla sisintä kehää eli päätelaitetta ja työn tekijää ulkoa tulevilta uhkatekijöiltä. Uloimman kehän eli verkon tietoturvan avulla tulisi uhat torjua ennen, kun ne pääsevät kehän sisempiin osiin. (BLC 2018.)

2.8 VPN

VPN-yhteydellä tarkoitetaan näennäisesti yksityistä erillisverkkoa, johon käyttäjä saa yhteyden julkisen internetin kautta. VPN on yksityinen vain virtuaalisesti koska siinä kulkeva data liikkuu julkisen verkon ylitse. VPN käyttää alustana julkista internetverkkoinfrastruktuuria ja yhteyden suojaus tapahtuu tunneloinnin kautta esimerkiksi L2TP-protokollan läpi. L2TP tapahtuu OSI-mallin siirtoyhteyskerroksessa yhdessä IPsec-protokollan kanssa, joka sijaitsee OSI-mallissa verkkokerroksessa. (IPSec/L2TP) kryptaa lähetetyn datan ennen lähetystä ja dekryptaa datan tunnelin toisessa päässä. (Bhattrai & Nepal 2016.)

VPN:n suosio on kasvanut sitä mukaa, kun etätyönteko on yleistynyt. VPN tarjoaa yrityksille yksityisiä verkkoja edullisemman ratkaisun vaikkakin VPN tuo myös mukanaan tietoturvariskejä. (Bhattrai, & Nepal 2016.) Eritoten ilmaiset VPN-ratkaisut voivat olla merkittäviä tietoturvariskejä. Osa VPN-ratkaisusta ovat sellaisia, että oikeuksia on annettava

kohtalaisen paljon ja VPN:n tarjoaja saa haltuunsa paljon sellaista tietoa, joka ei ole välttämätöntä palvelun toiminnan kannalta. Osa ilmaisista VPN-ratkaisuista sisältää haittaohjelmakoodia. Tietoja voi vuotaa esimerkiksi dns-haun kautta, jos tämän suojaus on puutteellinen. (Mikrobitti 2019.)



Kuva 4. VPN-yhteys julkisen verkon yli

2.9 OSI-malli

OSI-malli on viitekehys, joka kuvaa verkkoyhteyksien toimintamallia. Mallissa kuvataan seitsemän kerrosta, joita ovat alhaalta ylöspäin luetellessa fyysinen kerros, siirtokerros, verkkokerros, kuljetuskerros, istuntokerros, esitystapakerros ja sovelluskerros. Malli visualisoi muutoin abstraktia asiaa havainnollistaen sen toimintaa. OSI-mallin ymmärtäminen on tärkeää järjestelmiä ylläpitäville tahoille sekä esimerkiksi kehittäjille. (Shaw 2020.)

Sovelluskerroksella tarkoitetaan sovellustasoa, joka on käyttäjälle näkyvä taso. Tämä taso sijaitsee lähimpänä loppukäyttäjää. Esitystapakerros määrittää sen, missä muodossa data esitetään käyttäjälle. Tiedon kryptaaminen ja purku tapahtuvat tällä tasolla. Istuntokerroksella tarkoitetaan yhteyden muodostavaa kerrosta eri laitteiden välillä. Istuntokerroksessa luodaan yhteys kahden eri laitteen, vaikkapa työaseman välille. (Shaw 2020.)

Kuljetuskerros huolehtii kahden työaseman, työaseman ja palvelimen tai kahden palvelimen välisestä datan pilkkomisesta sopivan kokoisiin osiin eli IP-paketeiksi. Verkkokerros huolehtii pakettien toimittamisesta oikeisiin osoitteisiin erilaisten verkkoprotokollien esimerkiksi TCP tai UDP välityksellä. (Shaw 2020.)

Siirtokerros on läheisessä yhteydessä fyysiseen kerrokseen ja huolehtii datan siirtymisestä toisiinsa välittömässä yhteydessä olevalta solmulta toiselle. Se myös korjaa fyysiseltä kerrokselta tulevia virheitä. Suurin osa verkon kytkimistä sijaitsee tässä kerroksessa. Fyysisellä kerroksella sijaitsevat erilaiset liittimet, käytettävät taajuudet, jännitetason sekä määrittää muista fyysisiä vaatimuksia verkon toiminnalle. (Shaw 2020.)

Kuva 5. OSI-malli (mukaillen Shaw 2021)

2.9.1 Salasanat

Salasana on käyttäjän itsensä valitsema tai tietojärjestelmän generoima yhdistelmä merkkejä, joiden perusteella jokin järjestelmä päästää käyttäjän sisään järjestelmään. Salasanan pituus voi vaihdella yhdestä merkistä pitkiin lauseisiin. Salasanan tarkoituksena on tunnistaa käyttäjä. (Bosworth & Wayne 2004, 2.) Salasanat ovat erittäin tärkeä osa tietoturvaa. Salasana on kuin jokaisen järjestelmän käyttäjän henkilökohtainen avain järjestelmään (TCJN).

2.9.2 Autentikointi ja auktorisointi

Työpaikan verkoissa käytetään yleensä vahvaa tunnistautumista vaativia kirjautumismenetelmiä. (Heljaste 2020.) Autentikoinnilla tarkoitetaan henkilöllisyyden tai tiedon alkuperän varmistamista. (Suomalainen 2013, 8). Tietojärjestelmä varmistaa erilaisin keinoin, että henkilö on todellisuudessa se, joka kertoo olevansa. Käyttäjälle on luotu järjestelmään identiteetti ja käyttäjän syöttämien tietojen on vastattava järjestelmään syötettyjä,

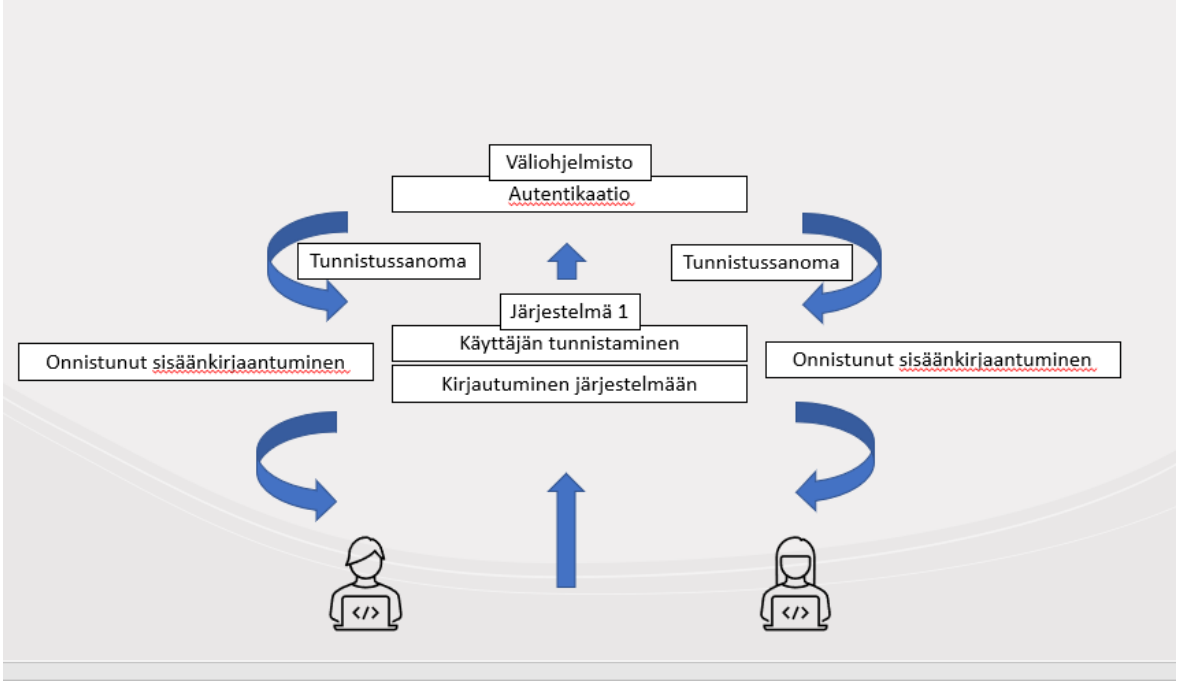
identiteettiin liitettyä tietoa. Menetelmiä autentikointiin on erilaisia. Se voi pohjata salasanaan tai koodiin, toimikorttiin tai toimiavaimeen tai niiden yhdistelmään, kertakäyttösalasanaan tai biometriseen tunnistustapaan. (Linden 2015, 16–17.)

Autentikointi voi olla vahvaa tai heikkoa. Vahvoihin menetelmiin lukeutuvat ne tunnistautumismenetelmät, jotka ovat sisältävät kaksi tai useampia tunnistautumismenetelmiä yhdessä. Esimerkkinä tästä voisi olla toimikorttikirjautuminen työpaikan järjestelmään niin, että tunnistautumisessa käytetään sekä salasanaa että itse toimikorttia. Verkkopankkiin kirjautuessa tarvitaan sekä salasana että kertakäyttökoodi. (Linden 2015,17.)
Auktorisoinnilla eli valtuutuksella tarkoitetaan käyttövaltuuksien hallintaa eli sitä, onko käyttäjällä oikeus pyytämänsä toiminnon suorittamiseen. Auktorisoinnissa suoritetaan käyttöoikeuksien hallintaa. (Linden 2012, 29.)

2.9.3 Kertakirjautuminen

Kertakirjautumisella (single sign-on) tarkoitetaan kirjatumista, jossa käyttäjä tunnistautuu vain kerran ja kertakirjautumisella voidaan päästä useisiin eri järjestelmiin eikä käyttäjätunnusta ja salasanaa tarvitse syöttää uudelleen joka järjestelmään. (Linden 2015, 28–29.) SSO-kirjautumistapoja erilaisiin extranet-ympäristöihin ovat yksinkertainen SSO-arkkitehtuuri sekä monimutkainen SSO-arkkitehtuuri. Yksinkertainen SSO-arkkitehtuuri tarkoittaa sitä, että käyttäjä kirjautuu järjestelmään esimerkiksi käyttäjätunnuksella ja salasanalla. Monimutkainen SSO-arkkitehtuuri tarkoittaa sitä, että käyttäjä kirjautuu järjestelmään yksinkertaisen valtuutuksen tai kaksitasoisen valtuutuksen avulla. Yksitasoinen valtuutus voi olla joko token-pohjainen tai PKI-pohjainen eli sertifikaatteihin pohjautuva valtuutus. (Radha & Reddy 2012.)

SSO-kirjautuminen on voimassa siihen saakka, että käyttäjä lopettaa istunnon. Aidossa kertakirjautumisessa käyttäjän tunnistaa väliohjelmisto, joka välittää tunnistussanoman tunnistettuaan käyttäjän identiteetin varsinaiselle ohjelmistolle. Tunnistusohjelmisto on joko käyttäjän laitteessa tai se voi sijaita erillisellä palvelimella. Aidon kertakirjautumisen lisäksi voidaan käyttää näennäiskertakirjatumista, jossa ohjelmistoon kirjautujan ja itse ohjelmiston välissä on ohjelmisto, joka varastoi salasanan ja käyttäjätunnuksen istunnon alussa. Kerran ne syötettyään käyttäjän ei itse tarvitse käyttäjätunnusta ja salasanaa enää syöttää vaan väliohjelmisto syöttää ne käyttäjän puolesta järjestelmään, johon kirjaudutaan. (Linden 2015 28–29.)



Kuva 6. Kertakirjautuminen (mukaillen Forcepoint)

2.10 Päätelaitteen suojaus

Päätelaite, mobiililaite tai palvelin, jota työnteossa käytetään, tulee aina suojata asianmukaisesti virustorjuntaohjelmalla ja palomuurilla. Näiden avulla voidaan mahdollisesti havaita työasemaan kohdistuvat hyökkäysyritykset tai muut uhat tietoturvallisuudelle. (BLC 2018.)

Tietoturvan perusta on uhkien torjunnassa ennen, kun uhka realisoituu eli saavuttaa verkon ja tunkeutuu tai ujuttautuu itse päätelaitteeseen. Sähköpostissa on virustorjunta, joka pyrkii estämään haitallisten sähköpostien tai sähköpostin osien pääsyn sähköpostilaatikon kautta itse päätelaitteeseen. (BLC 2018.) DNS eli Domain Name System -palvelimelle voidaan määrittää sallitut verkko-osoitteet ja uhkaa voidaan yrittää torjua sillä, etteivät tietyt verkkosivut ole sallittujen osoitteiden joukossa. (Rasmussen 2018a).

Sovellukset tulee aina päivittää uusimpaan versioon tietoturva-aukkojen tilkitsemiseksi. Tämä toimenpide on olennainen osa tietoturvaa. Päivittämättä jätettävä sovellus tarjoaa hyökkääjille hyökkäyspintaa-alaa haavoittuvuuksien kautta. (BLC 2018.) Päivityksiä ei saisi ladata laitteille avoimissa, suojaamattomissa verkoissa vaan päivityksiin tulee aina käyttää suojattua yhteyttä (Järvinen & Rousku 2017).

Uhan tietoturvalle aiheuttavat tilanteet, joissa päätelaite katoaa tai unohtuu jonnekin epähuomiossa. Mikäli tiedetään, missä laite on, tulisi se noutaa välittömästi pois, kun katoaminen huomataan. Käytettäville laitteille olisi hyvä sallia etäseuranta. Mikäli laite katoaa eikä katoamispaikka ole tiedossa, voi organisaation it-tuki yrittää selvittää laitteen sijaintia etähallinnan avulla. (Järvinen & Rousku 2017.)

Päätelaitteet itsessään voivat aiheuttaa riskin tietoturvalle (Traficom 2020a). Verkkorikollisten on mahdollista hyödyntää verkkoyhteyttä ja itse laitetta esimerkiksi palvelunestohyökkäyksen tekemiseen. Koneeseen tulisikin asentaa ohjelmia vain harkiten. Tarpeettomien ohjelmia asentamisesta on syytä pidättäytyä, koska näiden mukana koneelle voi päästä erilaisia haittaohjelmia. Erityistä varovaisuutta tulee noudattaa Java-sovellusten kanssa, Adoben Flash-laajennuksen sekä Silverlightin kanssa. Riskialttiita ovat myös erilaiset selaimen ladattavat lisäosat. (Järvinen & Rousku 2017.)

2.11 Tietoturvariskit verkossa

Tietoturvaan voi ihminen itse vaikuttaa paljon omalla toiminnallaan. Ihminen voi olla tietoturvan heikoin lenkki tietoturvassa. On houkuttelevaa ihmiselle uskoa erilaisiin verkossa oleviin ilmaistarjouksiin, kilpailuihin ja lupauksiin suurista tuotoista. Nämä ovat käytännössä aina huijausyrityksiä ja niiden klikkailu aiheuttaa riskin tietoturvalle. *(*Järvinen & Rousku 2017.)

Ongelmallista on myös se, että monet luotettavaksikin luokiteltavista verkkosivuista voivat sisältää verkkosivun ylläpitäjän siitä tietämättä arveluttavaa sisältöä kuten esimerkiksi mainontaa. Mainostilaa myyvät erilaiset kansainväliset toimistot, joiden intresseissä ei ole mainostajien taustojen selvittäminen. (Järvinen & Rousku 2017.)

Verkossa törmää erilaisiin nettitesteihin sekä kyselyihin, jotka itsessään saattavat vaikuttaa kohtalaisen harmittomilta. Kuitenkin niiden kautta saattaa välittyä arkaluontaistakin tietoa esimerkiksi mainostajille. (Järvinen & Rousku 2017.)

Sähköpostilaatikkoon voidaan lähettää epäilyttäviä viestejä, joiden tarkoituksena on tiedustella esimerkiksi tunnusten kalastelu. Tästä yksi tunnetuin muoto ovat nigerialaiskirjeet, joissa voidaan pyytää rahallista apua erilaisiin tekaistuihin ahdinkotilanteisiin. Monimutkaisen prosessin aikana uhri saattaa lopulta päätyä maksamaan suutia summia rikollisjärjestöille. Tämänkaltaisia huijausyrityksiä kohdistetaan toisinaan myös yrityksiin. (Järvinen & Rousku 2017.)

2.12 Kohdennetut hyökkäykset

Ransomware-as-service-hyökkäykset ovat lisääntymässä. Hyökkäys kohdennetaan kriittiselle toimialalle kuten terveydenhuoltoon sekä mielenterveyspalveluihin sekä muihin julkisen puolen palveluihin. Tietoja varastetaan ja sen lisäksi tietoa julkaistaan kaikille nähtäväksi julkiseen verkkoon. Hyökkäyksistä seuraa paljon julkisuutta ja huomiota. Tiedot voidaan kopioida ennen varastamista ja silti varastetuista tiedoista pyydetään lunnaita. Lunnaiden maksaminen ei takaa sitä, että tiedot olisivat lunnaiden maksamisen jälkeenkään turvassa. Terveydenhuolto on hyökkääjille siinäkin mielessä hyvä hyökkäyskohde, koska pulaa tietoturvaosaamisesta usein on ja järjestelmät voivat olla vanhoja huonosti suojattuja. (Huhtaniitty 2021.) Ikävä tosielämän esimerkki tiedon luottamuksellisuuden rikkoutumisesta oli psykoterapiakeskus Vastaamon tietomurto, joka tuli ilmi syksyllä 2020. Potilastietoja oli päässyt julkisuuteen jo tätä aiemmin ja yksi suurimmista syistä tietovuodolle oli se, että palomuurilta oli porttiohjaus, joka johti suoraan tietokantapalvelimelle, jonka salasana pystyttiin selvittämään. Tiedot oli hyökkääjien toimesta ensin kopioitu. Tapaus aiheutti valtavasti inhimillistä kärsimystä sekä valtavia tappioita liiketoiminnalle. (Palmu 2021.)

2.13 WLAN-verkko

WLAN-verkko on langaton sisäverkko, joka on käytössä nykyään lähes kaikilla työpaikoilla ja lähes jokaisessa kodissa. Langaton verkko on haavoittuvainen hyökkäyksille ja langattomassa verkossa on käytössä erilaisia suojausmenetelmiä ulkoisia uhkia vastaan. Hyökkäyksiä pyritään estämään salausprotokollien avulla. Protokollan on tarkoitus tunnistaa ja valtuuttaa verkossa toimiva käyttäjä sekä salata liikkuvien IP-pakettien sisältö. Näitä protokollia ovat mm. WEP, WPA sekä WPA2. WLAN-tukiaseman kautta on mahdollista liittää laitteita verkkoon. Protokolliin liittyy salausmenetelmiä, autentikointiin ja autorisointiin liittyviä prosesseja sekä erilaisia avaimia. Varmaa suojausmenetelmää langattomalle verkkoliikenteelle ei toistaiseksi ole olemassa. (Leinonen 2021 1–2, 7.)

2.13.1 Tyypilliset hyökkäykset WLAN-verkossa

Langattomaan verkkoon kohdistuu lukuisia erilaisia hyökkäystyyppejä. Tavallisimpia ovat Brute force ja erilaiset palvelunestohyökkäykset. Brute force – hyökkäys tähtää WLAN-verkon salasanan murtamiseen. Aluksi hyökkääjä kartoittaa ne verkot, joiden nimi on avoimesti näkyvissä ja ottaa selvää, onko mikään laite yhdistyneenä kyseiseen verkkoon. Salausprotokollalla suojattuun verkkoon hyökkääminen vaatii sen, että hyökkääjä pääsee kuuntelemaan protokollan käsittelyn, kun verkkoon yhdistyy jokin päätelaite. Hyökkääjä pyrkii saamaan selville reitittimen sekä pseudosatunnaisluvun, salasanan sekä

avainarvon. Näiden tietojen avulla hyökkääjä yrittää rakentaa avainarvon ja tämän onnistuessa hyökkääjä on selvittänyt WLAN-verkon salasanan. Salasanan avulla hyökkääjä pääsee kuuntelemaan WLAN-verkossa liikkuvaa liikennettä. Brute force -hyökkäyksestä toinen yleinen variaatio on sanakirjahyökkäys, jossa hyökkääjä kokeilee lukuisia salasanoja, jotka koostuvat kohtuullisen tavallisista sanoista. (Leinonen 2021, 9.)

Palvelunestohyökkäys (Denial of Service) on usein seurausta Brute force -hyökkäyksestä Hyökkääjä ottaa haltuunsa WLAN-verkon liikenteen niin, että pyrkii tukkimaan sen suurella määrällä IP-paketteja lähetettyinä hyvin lyhyen ajan sisällä. Palvelu estyy, kunnes kaikki IP-paketit on käsitelty. Brute force -hyökkäyksen jälkeen reititin hyväksyy IP-paketit verkkoliikenteeseen. (Leinonen 2021, 10.)

Rikolliset pyrkivät hyötymään hyökkäyksistä taloudellisesti ja tietomurrot aiheuttavat taloudellisia tappioita sekä vaarantavat hyökkäyksen kohteena olevan yrityksen maineen. Kun sivustolle tehdään onnistunut tietomurto, sen maine heikkenee ja erilaiset tietoturvaohjelmat sekä hakukoneet saattavat estää pääsyn kyseisille verkkosivuille. Onnistunutta tietomurtoa voi seurata tietovuoto, mikä vararantaa tiedon luottamuksellisuuden. Pahimmassa tapauksessa ovat vaarassa esimerkiksi ihmisten henkilötiedot sekä muut arkaluontoiset tiedot (Traficom 2020b.)

2.14 Tietoturvarike

Tietoturvarike on ihmisen toimintaa, jossa esimerkiksi yrityksen tiedot vaarantuvat ja muodostuu riski. Tietoturvarikkeet voidaan jaotella sisäpiirin toimiin, jossa esimerkiksi yrityksen jäsen syyllistyy rikkomukseen. Organisaation ulkopuolinen henkilö, esimerkiksi hakkeri, muodostaa yritystä sen ulkopuolelta uhkaavan tietoturvarikkeen. (Järviö 2018, 6–7.)

Tietoturvarike voi olla tarkoituksellinen tai vahingossa tehty ja rikkeitä on kolmenlaisia. Salassa pidettäviä tietoja voi päästä ulkopuolisille vaikkapa sen vuoksi, että yrityksen työntekijällä ei ole riittävästi tietoa tai kokemusta tietoturvallisesta toiminnasta ja esimerkiksi paljastaa salasanan yrityksen ulkopuoliselle taholle. Rikkeeseen voi syyllistyä myös tahallaan mutta ilman varsinasta pahaa tarkoitusta esimerkiksi toimimalla huolimattomasti. Tästä esimerkkinä on tilanne, jossa työntekijä ei toimi yrityksessä annettujen ohjeiden mukaisesti ja aiheuttaa riskin. Kolmantena riketyyppinä on tahallinen, pahassa tarkoituksessa toteutettu teko, joka aiheuttaa riskin. Tästä esimerkkinä tilanne, jossa työntekijä pyrkii ohjeita tahallaan rikkomalla hyötyä tilanteesta jollakin tavalla (Järviö 2018, 6–7.)

2.15 Tietojenkalastelu

Sähköpostiin tulevilla phishing-viesteillä rikolliset kalastelevat salasanoja ja käyttäjätunnuksia harhauttamalla käyttäjän klikkaamaan viestissä olevaa linkkiä. Linkki ohjaa käyttäjän esimerkiksi pankin sivuston kanssa lähes identtiselle huijaussivustolle, joka todellisuudessa on tietojenkalastelusivusto. Kalastelua kohdistetaan niin yrityssähköposteihin kuin yksityisiin sähköposteihin. Joissain viesteissä pyydetään uhria kertomaan esimerkiksi pankkitunnuksensa tai jonkin muun palvelun tunnukset. (Järvinen & Rousku 2017.)

Jokaisen on hyvä oppia tunnistamaan merkit, jotka voivat viitata tietojenkalasteluun. Tietojenkalastekuun viittaavia tunnusmerkkejä voivat olla epäilyttävän näköiset linkit sähköpostiviestissä ja epämääräinen sähköpostiosoite. Verkkorikolliset ovat taitavia väärennöksissä ja linkit ja osoitteet voivat muistuttaa paljon alkuperäisiä sähköpostiosoitteita ja linkkejä. On parasta olla klikkaamatta linkkiä, ellei tiedä tarkalleen, minne se johtaa. Palvelun osoite on hyvä kirjoittaa selaimeen suoraan erityisesti pankki- ja muiden kriittisten palvelujen kohdalla. (Järvinen & Rousku 2017.) Tietojenkalasteluviestin tunnistaminen voi kuitenkin olla todella haasteellista, koska kalastelua tehdään muun muassa soluttautumalla mukaan sähköpostiketjuun ja sähköpostit voivat olla hyvin aidon kaltaisia ulko- ja kieliasultaan koneoppimisen mahdollistaessa näiden tuottamisen. (Huhtaniitty 2021).

Selainta käytettäessä on hyvä varmistaa, että selaimessa on väri osoiterivin pohjassa ja/tai lukon kuva. Lukon kun ja osoitekentän pohjan väri viittaavat SSL-suojaukseen. SSL-suojaukseton sivu voi olla huijaussivu tai muuten tietoturvan kannalta epäilyttävä sivu. SSL-varmenne salaa liikenteen selaimen ja palvelimen välillä ja kertoo palvelimen aitoudesta. (Järvinen & Rousku 2017.)

Sosiaalinen media on hyvä alusta rikollisille tietojenkalasteluun. Sosiaalisen median kautta käyttäjiltä on helppo saada arkaluontoista tietoa esimerkiksi päällepäin viattomilta vaikuttavien kyselyjen muodossa. Yrityksessä tulisi ohjeistaa henkilöstöään turvalliseen verkon käyttöön. Linkit tulee jättää avaamatta, ellei ole täysin varma linkin sisällöstä. (Valtionvarainministeriö 2010b.)

2.16 Kyberrikollisuus

Kyberrikollisuuden esiintyvyys on kasvussa. Monissa valtioissa kyberrikollisuuden torjunta on otettu keskeiseksi osaksi turvallisuusstrategioita. Kyberrikollisuus aiheuttaa maailmanlaajuisesti valtavia kustannuksia. Kustannukset saattava yltää 600 miljardiin dollariin

vuositasolla mitattuna. Interpol ilmoitti tietojenkalastelun ja haittaohjelmien esiintyvyyden nousseen 569 % pelkästään yhden kuukauden aikana vuonna 2020. Keskimäärin kiristyssumma oli 180 000 dollaria. (Paasonen 2021.)

Kyberhyökkäykselle tyypillistä on se, että hyökkääjä tekee ensin tiedustelutyötä, jossa kartoitetaan mahdollisia rikoksen kohteita. Kohteen valinnan jälkeen rikollinen valitsee tilanteeseen sopivan tavan hyökkäykselle. Seuraavassa vaiheessa rikollinen toteuttaa itse hyökkäyksen esimerkiksi tunkeutumalla kohteen sisäverkkoon. Hyökkääjä voi tässä vaiheessa varmistaa pääsyn järjestelmään ja järjestelmän hallinnan esimerkiksi lataamalla kohteeseen etähallintaohjelman. Hyökkääjä pyrkii saamaan hallintaansa mahdollisimman monen käyttäjän käyttäjätilejä. Usein kaapattujen tilien määrä on valtava, jopa useita tuhansia. Hyökkäyksen viimeisessä vaiheessa hyökkääjä pääsee käsiksi tietoon, jonka avulla hän voi hyötyä taloudellisesti. (Brewer 2017.)

2.17 Sosiaalinen media

Sosiaalisessa mediassa moni tulee tahtomattaan paljastaneeksi itsestään paljon. Henkilökohtaiset kuvat, mielenilmaistut ja videot ovat julkisesti nähtävillä kaiken aikaa. Sosiaalisen median käytössä on hyvä harkita, mitä uhkia sosiaalisen median käyttöön voisi liittyä, jos julkaistusta materiaalista voi päätellä esimerkiksi sijaintitietoja tai muuta arkaluonteista. Sosiaalisen median käyttöohjeet on hyvä lukea tarkasti läpi. (Järvinen & Rousku 2017.)

Työtehtävät ja vapaa-aika on hyvä pitää erillään toisistaan niin, ettei tule paljastaneeksi julkisesti mitään sellaista, mikä voisi olla haitallista työpaikan organisaatiolle tai yksilölle itselleen. Sosiaalisessa mediassa on usein hankalaa täysin erottaa toisistaan yksityishenkilön ja yrityksen edustajan rooli etenkin, jos työskentelyorganisaatio mainitaan sosiaalisen median profiilissa. Kannanotot voivat helposti ulkopuolisesta vaikuttaa yrityksen kannanotoilta ja siksi onkin syytä pidättäytyä sellaisten mielipiteiden, joista voi yhdistää henkilön ja organisaation negatiivisessa valossa, julkaisemisesta. (Järvinen & Rousku 2017.)

Tietoturvariskit sosiaalisessa mediassa koostuvat pääosin tietoturvauhkien, toimintatapojen sekä palvelukonseptien yhdistelmistä. Ongelmia aiheuttavat sekä käyttäjien toiminta että toisaalta rikolliset, jotka kalastelevat tietoa saadakseen sen avulla taloudellista tai muuta hyötyä. (Järvinen & Rousku 2017.)

Salaiseksi tai arkaluontoiseksi luokiteltavaa tietoa voi päätyä sosiaalisen median välityksellä epähuomiossa julkisuuteen. Tietoa voi olla vaikea poistaa ja usein poistaminen on mahdotonta. Pienistä tiedon osasista muilla on mahdollisuus koota yhteen kokonaiskuva

tilanteesta ja esimerkiksi valokuvat ja videomateriaalit voivat sisältää tietoja, joka leviää vahingossa julkisuuteen. (Valtionvarainministeriö 2010.)

2.18 GDPR

EU:n yleistä tietosuoja-asetusta alettiin soveltaa yleisesti käytäntöön Euroopan unionin jäsenvaltioissa keväällä 2018. Henkilötietojen suoja on tärkeä osa länsimaista oikeusjärjestelmää ja tämä tulisi sisällyttää osaksi elinkeinonharjoittamista yksilön tietoturvan turvaamiseksi. Tietosuoja-asetuksen yksi keskeinen osa korostaakin juuri riskien ennaltaehkäisyä ja riskin mahdollisuuden arviointia. Rekisterinpitäjän ja henkilötietojen käsittelijän on aina varmistuttava siitä, että käytännöt ovat yrityksessä tai yhteisössä sellaiset, että tietoturva on hyvällä tasolla. (Korpisaari, Pitkänen & Warma-Lehtinen 2018.)

Henkilötietojen väärästä ja huolimattomasta käsittelystä voi aiheutua suuria uhkia yksilöille ja organisaatioille. GDPR-asetusta noudattamalla voidaan varmistaa se, että henkilötietoja käsitellään tarkoituksenmukaisesti eikä turhaa tietoa tallenneta. Kaikki tämä edellyttää taustalle toimivan tietoturvasuunnitelman. (Järvinen & Rousku 2017.)

GDPR:n lisäksi tietoturvallisuutta käsitellään esimerkiksi perustuslaissa, jossa turvataan yksityisyyden suoja ja viestinnän luottamuksellisuus. Julkisen vallan tehtävänä on huolehtia siitä, että nämä toteutuvat monimutkaistuvassa digitalisoituvassa ympäristössä. (Liikenne- ja viestintäministeriö 2018.)

2.19 Tietoturvallisuuden lisääminen

Kuten jo edellä olevassa luvussa todettiin, tietoturvan heikoimmat lenkit ovat verkon käyttäjät eli ihmiset. Omaksumalla tietoturvalliset toimintatavat voidaan tietoturvaa parantaa merkittävästi. Tiedon turvalliseen tallennuspaikkaan on hyvä kiinnittää huomiota. Kaikkein kriittisempää tietoa ei ole tarkoituksenmukaista tallentaa esimerkiksi pilvipohjaiseen palveluun. Jokaisen tietoa käsittelevän ihmisen on osaltaan huolehdittava siitä, ettei kriittistä tietoa pääse katoamaan tai vääriin käsiin. (Järvinen & Rousku 2017.) Käsiteltävä tieto olisi hyvä luokitella eri tavoin sen mukaan, onko tieto julkista, vai salassa pidettävää materiaalia. Henkilötietoja tulee aina käsitellä erityistä huolellisuutta noudattaen ja GDPR huomioiden. (Digitaalinen Helsinki.)

3 Empiirinen osa

3.1 Menetelmäkuvaus

Tutkimusmenetelmänä käytän soveltaen kirjallisuuskatsausta. Opinnäytetyössäni kartoitan etätyön vaikutusta tietoturvaan tiedon luottamuksellisuuden säilyttämisen näkökulmasta. Kirjallisuuskatsauksen menetelmin on tarkoitus selvittää, millaista tietoa valitsemastani aiheesta on saatavilla tällä hetkellä, vertailla tietoa ja pohtia, kuinka tietoa sovelletaan käytäntöön. Tässä tapauksessa kirjallisuuskatsauksen sovellettava muoto on kuvaileva kirjallisuuskatsaus.

Etätyöstä, tietoturvasta sekä niiden yhdistelmästä löytyy verkkohaulla paljon kirjallisuutta ja tutkimuksia ajalta ennen koronapandemiaa. Julkaisuja löytyy myös monia korona-ajalta. Korona-ajan etätyö ja tietoturva ovat luonteeltaan erilaisia kuin perinteiseen toimistolla tapahtuvaan työhön liittyvät vastaavat. Suuri määrä ihmisiä siirtyi etätöihin nopealla aikataululla lähes olemattomalla varoitusajalla. Halukkuus työskennellä etänä ei kaikilla työntekijöillä ollut sisäsyntyistä, vaan tilanteeseen oli pakko sopeutua. Tilanne aiheutti luonnollisesti haasteita myös tietoturvatoteutuksille ja niiden toimivuutta oli pakko tarkastella uudelleen kriittisesti.

Tietoturva on nykyajan tietoyhteiskunnassa yksi merkittävimmistä riskeistä yritysten liiketoiminnalle ja vakavan tietoturvauhan realisoituessa tuhot ovat usein suuria. Realisoituneet uhat voivat uhata jopa liiketoiminnan olemassaolon perusteita, koska tietoturva on elintärkeää asiakaskontakteille sekä heidän asiakkailleen. Yrityksen mainetta voi olla mahdotonta palauttaa, jos se kerran on menetetty.

Työssäni kartoitan mahdollisia tiedon luottamuksellisuuteen liittyviä uhkia tietoturvan näkökulmasta. Pääasiallisesti keskityn työssäni keinoihin, joilla tietoturvaa pyritään parantamaan kuten fyysiseen ympäristöön sekä turvalliseen työskentelyyn verkon välityksellä. Ennakkoasetelma on, että tietoturva on hoidettu varsin tehokkaasti yrityksissä, mutta ongelmakohtia on siitä huolimatta. Ongelmakohtiin on kirjallisuudessa esitetty useita eri ratkaisumalleja ja tietoturvaa voidaan näiden mallien avulla pyrkiä parantamaan.

3.2 Tulokset

Etätyötä tekevät tällä hetkellä suuri osa työntekijöistä siitä riippumatta, onko henkilöllä itsellään tosiasiallisesti motivaatiota etätyön tekemiseen. Valmistautumiseen on ollut vain vähän aikaa niin työntekijä- kuin työantajapuolella. Nopeita siirtoja tehtäessä riskit kasvavat merkittävästi, kun kaikkea ei ole mahdollisesti pystytty ottamaan huomioon.

Yritysten on koronapandemian alkaessa pitänyt kartoittaa uusia kyberturvallisuutta uhkaavien riskien tyypit ja yritysten on pitänyt päivittää koko tietoturvastrategiansa uudelle tasolle. Työntekijöitä on alusta saakka ohjattava ja koulutettava toimimaan oikein, muutoin etätyöstä voi pitkässä juoksussa tulla merkittävä hankaluus työnteolle tietoturvan näkökulmasta. (Brandenburg & Mee 2020.) Verkossa työntekijä saattaa etsiä työnteon lisäksi tietoa, pitää yhteyttä muihin ja hoitaa henkilökohtaisia asioitaan. Työpaikoilla tulisikin laatia netinkäytön periaatteista säännöt ja netinkäytöstä on hyvä keskustella työpaikalla avoimesti. Ohjeistus tulisi suullisen oheistuksen lisäksi olla kirjallisessa muodossa. Työntekijöiden omien verkkojen kautta tapahtuvaa netinkäyttöä on työnantajan hankala rajoittaa, koska aika monella on käytössään langattomassa älylaitteessa kuten puhelimessa oma langaton verkko. (Järvinen & Rousku 2017.)

Pandemiatilanteen puhjettua rikolliset ovat aktivoituneet hyödyntämään heille edullista tilannetta ja kyberhyökkäysten määrä on monikertaistunut. Rikolliset ovat löytäneet uusia verkkorikollisuuden muotoja, ja heille on avautunut lisää kanavia rikoksiin. FBI:lle ilmoitetaan päivittäin useista tuhansista kyberhyökkäyksistä. Työympäristön nopea muutos on tuonut uusia haavoittuvuuksia ja hyökkäysalustoja on tullut lisää. Yrityksillä on hankaluuksia pysyä ajan tasalla nopeassa muutoksessa. (Brandenburg & Mee 2020.)

On mielenkiintoista, että iso osa tapahtuneista hyökkäyksistä liittyy jollakin lailla inhimilliseen virheeseen. Ihminen onkin tietoturvaketjussa usein heikoin lenkki. Arvion mukaan vuonna 2019 jopa 90 % kyberhyökkäyksistä mahdollistuu ihmisen toiminnasta. Kyberhyökkäyksen onnistumisen todennäköisyys kasvaa, kun tarkkaavaisuus syystä tai toisesta vähenee. Esimerkiksi stressi lisää virheen mahdollisuutta. (Brandenburg & Mee 2020.)

Koronapandemian aikana esiin tulleista tietoturvauhista ei moni ole täysin uusi. Kun kuitenkin suuret määrät ihmisiä työskentelee etänä verkossa, verkkorikollisille avautuu paremmat mahdollisuudet hyödyntää tilannetta aiempaa paremmin. Toisaalta aktiivisuus verkossa on välttämätöntä siksi, että työ tapahtuu suurilta osin etänä. Verkkorikolliset etsivät huonosti suojattuja tai suojaamattomia verkkoyhteyksiä etsien niistä haavoittuvuuksia.

Ennen varsinaista hyökkäystä rikolliset usein kartoittavat huolellisesti tilannetta. (Okereafor & Manny 2020)

3.2.1 Salasanojen käyttö

Salasanatunnistus on edelleen käytössä oleva menetelmä heikkouksistaan huolimatta. Henkilön voidaan antaa itse valita salasanansa tai järjestelmä voi generoida sattumanvaraisen salasanan käyttäjälle. (Linden 2015, 21.) Yleisimmin käyttäjä määrittelee salasanansa itse. (Kyberturvallisuuskeskus).

Hyvä salasana on helposti muistettava mutta samalla salasanan arvaaminen tulisi olla vaikeaa. Hyvä tapa on opetella ulkoa lause, josta salasana koostuu. Lause on helppo muistaa. Perinteisesti hyvä salasana on sisältänyt erikoismerkkejä. Kuitenkin tämä vaatimus tulisi poistaa hyvän salasanan määritelmästä, koska erikoismerkit lisäävät riskiä kirjoitusvirheille. (Siltainsuu 2020, 10.) Salansanan ominaisuudet vaikuttavat suoraan tietoturvan tasoon etenkin sellaisissa järjestelmissä, jossa käytetään heikkoa tunnistamista. Heikolla tunnistamisella tarkoitetaan sitä, että tunnistaminen ja todentaminen tapahtuvat vain yhden menetelmän avulla. (Kyberturvallisuuskeskus.)

Järjestelmän tulisi sallia vähintään 64 merkkiä pitkät salasanat, parhaimmassa tapauksessa pituusrajoitusta ei olisi ollenkaan. (Siltainsuu 2020, 10.) Lyhyt salasana altistaa sille, että salasana voidaan helposti selvittää esimerkiksi ns. brute force -menetelmällä (Burr ym. 2017, 67). Salasanan kopiointi salasanakenttään tulisi mahdollistaa. Lisäksi Siltainsuun mukaan olisi luovuttava vaatimuksesta, että salasana pitäisi vaihtaa tietyin aikavälein. (Siltainsuu 2020, 10.)

Wayne ja Bosworth sen sijaan ovat sitä mieltä, että vahvassa salasanassa on mukana erikoismerkkejä. Hyvässä salasanassa tulisi olla vähintään 6–10 merkkiä ja numeroiden, erikoismerkkien ja kirjainten pitäisi olla toistensa lomassa. Tavallisia sanoja on hyvä välttää. (Bosworth & Wayne 2004, 5.) Riittävän pitkä salasana tulisi olla vähintään 15 merkkiä pitkä (Kyberturvallisuuskeskus).

Lyhyet salasanat eivät ole lähteiden valossa suositeltavia ja niiden käyttö tulisi lopettaa välittömästi ja vaihtaa vahvempiin, koska tietomurtojen yhteydessä paljastuvat etenkin käyttäjätunnukset ja salasanat. Näitä voi rikollinen sitten hyödyntää muissakin järjestelmissä, esimerkiksi uhrin työpaikalla ja päästä käsiksi yritysten järjestelmiin. Tämä tilanne muodostuu erityisen vaaralliseksi silloin, kun tietomurto kohdistuu sellaisiin järjestelmiin

kuten Google tai Facebook. Näiden kautta yksittäisestä käyttäjästä on mahdollista selvittää suuri määrä tietoa. (Isotalo.)

Salasanan kryptografisen tiivisteen ansiosta tietojärjestelmässä salasana ei välity koskaan sellaisenaan, joten erikoismerkkien vaatimus salasanoissa on kyseenalainen. Tutkimusten mukaan vaatimus erikoismerkeistä voi johtaa siihen, että käyttää valitsee salasanan näennäisesti monimutkaisempana mutta hyvin arvattavana. Esimerkkinä tästä salasana, jonka käyttäjä olisi asettanut muotoon ”aurinko” mutta erikoismerkki- ja numerovaatimuksen vuoksi koostaa sen esimerkiksi näin ”Aurinko1!”. Käänteisesti monimutkainen salasana tuo mukanaan toisenlaisen riskin. Liian monimutkainen salasana on vaikea muistaa ja se kirjoitetaan mahdollisesti muistiin vaikkapa paperille. Muistiin kirjoitettu salasana altistuu paljastumiselle. (Burr ym. 2017, 68.)

Salasanojen hallinnoimiseen on olemassa erilaisia järjestelmiä, joihin käyttäjä voi syöttää salasanansa ja hakea sen silloin, kun sitä tarvitsee. Salasanojen hallintamenetelmät mahdollistavat monimutkaisten ja hankalasti muistettavien salasanojen käytön järjestelmissä. Hallintajärjestelmät voivat olla työasemalla, puhelimessa tai ulkoisesti USB-liitännällä tietokoneeseen liitettynä. (Ambarish, Nicolas & Nitesh 2014, 2.)

Hyvä ja vahva salasana ei kuitenkaan aina merkitse huonoa käytettävyyttä. Käytettävyys ja salasanan vahvuus eivät ole välttämättä käänteisesti verrannollisia toisiinsa. Bauer ym. teettämien laajojen kyselytutkimusten mukaan hyviä tuloksia on saatu sillä, että organisaatioissa järjestelmissä on tiettyjä vaatimuksia salasanoille kuten pituus ja erikoismerkit sekä pienet ja isot kirjaimet. Hyödyllisiksi todettiin tiettyjen merkkijonoyhdistelmien mustat listat organisaatioiden järjestelmissä. Käyttäjiä ohjattiin järjestelmän toimesta vahvempien salasanojen valintaan. Käyttäjän taakka keveni, kun järjestelmä ohjasi käyttäjää valitsemaan vahvan salasanan. (Bauer ym. 2016.)

3.2.2 Salasanojen hallinnointi

Siltainsuu tutki pro gradu -tutkimuksessaan sitä, minkälaisia tapoja ihmisillä on hallinnoida ja muistaa salasanoja. Tapoja oli kolmenlaisia. Salasana voidaan muistaa, se voidaan kirjoittaa ylös paperille tai voidaan käyttää salasanojen hallintajärjestelmää. Muistamisen ongelmana on muistin rajallinen kapasiteetti. Ongelmat salasanojen ulkoa muistamisessa johti siihen, että salasanoja käytettiin uudelleen eri järjestelmissä. Tämä toimintatapa aiheuttaa riskin sille, että yhden järjestelmän paljastunut salasana paljastaa myös muiden järjestelmien salasanoja aiheuttaen näin tietoturvariskin. (Siltainsuu 2020, 59–60.)

Siltainsuun haastattelututkimuksen mukaan toinen tapa hallinnoida salasanoja oli kirjoittaa salasanat ylös paperille. Tämän menetelmän vahvuutena on se, että uniikkien salasanojen käyttäminen on mahdollista, koska niitä ei tarvitse muistaa ulkoa. Esille tuli myös se, että salasanoja käytettiin muistiin kirjoittamisesta huolimatta jonkin verran uudelleen. Ongelmallista on myös se, että salasanat ovat mahdollisesti myös muiden henkilöiden saatavilla ollessaan paperilla selkokielisenä. (Siltainsuu 2020, 59–60.)

Kolmas tapa hallinnoida salasanoja olivat erilaiset digitaaliset salasananhallintajärjestelmät. Tässä menetelmässä erottui kaksi erilaista tapaa. Osa tallensi salasanoja omalle koneelleen, osa käytti ulkopuolisen palveluntarjoajan tietokantaa. Vahvuutena salasanahallintajärjestelmässä oli se, että salasanat tallennetaan salatussa muodossa eikä käyttäjällä ole tarvetta muistaa salasanoja ulkoa. Hallintajärjestelmä mahdollisti täysin erilaisten salasanojen keksimisen eri järjestelmiin. (Siltainsuu 2020, 59–60.)

Salasanaohjelmistoissa on kuitenkin omat riskinsä ja niiden taso vaihtelee suuresti. Salasanojen hallintajärjestelmät sisältävät erittäin arkaluontoista dataa ja hallintajärjestelmän kautta voi vuotaa valtavan määrän tietoa, jos master-salasana eli palveluun kirjautumissalasana paljastuu. (Kasunic, 2021.) Master-salasanan tulisi olla vahva, vaikka käyttäjä sen kokisikin hankalana ja epämukavana koska master-salasanan avulla paljastuvat muut järjestelmään syötetyt salasanat esimerkiksi brute force – hyökkäyksen yhteydessä. (Elizarraras, Hirschi, Luevanos, Yeh 2017, 8)

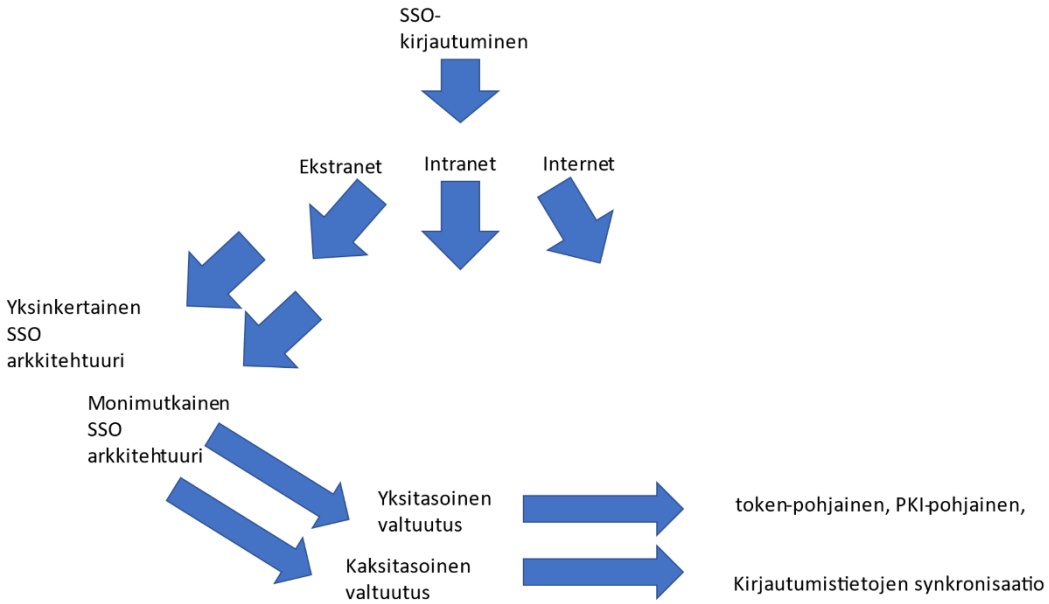
Hyvän salasanan hallintajärjestelmän ominaisuutena on se, että turvallisuus menee käytettävyyden edelle. Läpinäkyvyys on tärkeää, jotta käyttäjä tietää, miten hänen tietojaan käsitellään. Hallintajärjestelmän tulisikin vaatia käyttäjältä vahvaa salasanaa ja näin ohjata käyttäjää salasanan valinnassa. (Elizarras ym. 2017, 8.)

Suositeltavaa olisi, että kaikissa järjestelmissä olisi oma uniikki salasanansa. Mikäli samaa salasanaa käytetään useissa eri järjestelmissä, pääsee hyökkääjä kerralla käsiksi mahdollisesti henkilön kaikkeen digitaliseen dataan mukaan lukien työpaikan järjestelmät. Joidenkin tietoturva-asiantuntijoiden mukaan salasanojen uudelleenkäyttö on jopa suurin yksittäinen uhka tietoturvalle. (Lord, 2020.)

3.2.3 Kertakirjautuminen (SSO)

Single-sign-on-kertakirjautuminen eli SSO-kirjautuminen on menetelmä, jossa käyttäjä pääsee kirjautumaan useisiin eri palveluihin yhdellä kertaa. Hyvänä puolena tässä menetelmässä on se, että kirjautumistiedot sijaitsevat vain yhdessä paikassa. Myös oikeudet

järjestelmiin esimerkiksi työpaikalla voidaan lakkauttaa yhdestä paikasta. (Kuparinen, 2019.) SSO-kirjatumista voidaan käyttää niin internet-palveluissa kuin intranet- ja extranet-palveluissa. (Radha, Reddy 2012.)



Kuva 7. SSO-kertakirjautuminen (mukaillen Radha, Reddy 2012)

SSO-pohjaisen kirjautuminen vähentää phishing-yritysten onnistumisen todennäköisyyttä, kun kirjautumiseen moniin eri järjestelmiin käytetään vain yhtä tunnusta ja salasanaa. (Radha, Reddy 2012.) Todennäköisyys sille, että käyttäjä valitsee riittävän monimutkaisen salasanan, kun salasanoja on vain yksi, on suurempi kuin silloin, kun eri järjestelmiin on käyttäjällä monta eri salasanaa. (Bazaz & Khalique 2016.)

Toisaalta SSO-kirjautumiseen liittyy kuitenkin myös tietoturvaongelmia. Mikäli hyökkääjä pääsee käsiksi SSO-istuntoon, pääsee hän käsiksi mahdollisesti useisiin eri järjestelmiin ja niiden sisältämiin tietoihin yhdellä kertaa. Kertakirjautumisella käyttäjä pääsee käsiksi useisiin eri järjestelmiin näin ollen hyökkäyspinta-ala on laajempi (Belloni.) Riskinä on myös se, että käyttäjä lähtee työpisteeltään vaikkapa käymään wc:ssä ja jättää työasemansa lukitsematta. Tässä tilanteessa toinen henkilö pääsee helposti käsiksi kerralla moniin eri järjestelmiin ja siellä sijaitseviin tietoihin. Tämä riski ei toki ole SSO-spesifinen, mutta riskin realisoituessa tuhot voivat olla monikertaiset. (Bazaz & Khalique 2016.)

SSO-kirjautumiseen liittyviä riskejä ja toisaalta siitä saatavia hyötyjä on punnittava organisaatioissa tarkkaan ennen SSO-pohjaisten kirjautumistapojen käyttöönottoa.

Pahimmillaan SSO voi aiheuttaa valtavan tietoturvariskin, jos sen hallintaa ja käyttöönottoa ei ole harkittu tarkoin. (Radha, Reddy 2012.)

3.2.4 Kryptaus

Kryptaus tarkoittaa salausta. Kun jokin tieto on salattua tietojenkäsittelyn yhteydessä, selkokielellä kirjoitettu sisältö kryptataan eli muutetaan salattuun muotoon matemaattisella menetelmällä. Sisällön saa takaisin selkokieliseksi vain salausavaimen avulla. Kryptausta on käytetty hyödyksi jo toisen maailmansodan aikana, joten tekniikka ei ole uusi. Tietokoneiden alati paraneva laskentateho parantaa myös salaustehokkuutta. Tavallinen käyttäjä ei tule välttämättä salausta ajatelleeksi ja salaus on osa tietojärjestelmää. Järjestelmien tehtävänä varmistaa, että yhteyttä työasemalta ei voida murtaa. Järjestelmissä käytetään erilaisia salaustekniikoita. Hyvä esimerkki salaustekniikasta on Windows 10 pro version ominaisuus eli BitLocker-laitesalaus. (Rasmussen 2018b.)

Salausmenetelmiä tarvitaan digitaalisen viestinnän yhteydessä sähköpostikeskusteluissa, chateissa, videoneuvotteluissa sekä erilaisten digitaalisten palvelujen yhteydessä. Nykyaikana salausta tarvitaan entistä enemmän myös erilaisten älylaitteiden yhteydessä. Salaus tapahtuu eri verkon tasoilla salaustekniikasta riippuen. Tärkeimmät salaustasot ovat sovellus- ja verkkokerros OSI-mallin mukaan. Viestit tulee vastaanottajalle mahdollisimman pitkän matkan salattuna, jos salaus sijaitsee niin ylhäällä verkon kerroksella kuin mahdollista. (Liikenne- ja viestintäministeriö 2018.)

Päästä päähän salauksella tarkoitetaan sitä, että viesti muutetaan selkokieliseksi vasta vastaanottajan laitteessa. SS eli secure shell -protokolla tähtää päästä päähän tapahtuvaan salaukseen. Tästä hyvä esimerkki on laitteen käyttö etänä. (Liikenne- ja viestintäministeriö 2018.)

Salausmenetelmät jaotellaan muun muassa symmetrisiin ja epäsymmetrisiin eli asymmetrisiin menetelmiin. Asymmetrisellä menetelmällä tarkoitetaan julkisen salauksen menetelmää. Salaus tapahtuu tässä vastaanottajan julkisella avaimella. Lähettäjä saa tämän avaimen käyttöönsä eri menetelmin. Usein tämä tapahtuu ohjelmiston kautta niin, että avain välitetään automaattisesti vastaanottajalle. Varmentaminen hoituu usein myös automaattisesti. Joskus avain voi olla osana sertifikaattia tai avain haetaan keybase-luetteloista. Julkinen avain voi pohjata myös käyttäjään yksilöivään tunnistukseen esimerkiksi sähköpostiosoitteeseen. Vastaanottajalla on salattu, yksityinen avain, jonka avulla salauksen purkaminen onnistuu. Julkista avainta käyttävissä järjestelmissä voidaan käyttää digitaalista allekirjoitusta. Järjestelmä tarkistaa allekirjoituksen ja hyväksyy tai hylkää sen. Julkisen

avaimen yhteydessä käytetyt menetelmät ovat monimutkaisia matemaattisia menetelmiä ja ne ovat turvallisuustasoltaan vaihtelevia. (Liikenne- ja viestintäministeriö 2018.)

Salaukselle suurena uhkana voidaan nähdä tulevaisuudessa mahdollisesti valmistuvat äärimmäisen tehokkaat kvanttitietokoneet, jotka voivat murtaa lähes kaikki tämänhetkiset julkiseen salausavaimeen perustuvat salausmenetelmät. Tallaisen kvanttitietokoneen valmistuminen ei tällä hetkellä ole vielä kovin ajankohtainen mutta tämä voisi olla todellisuutta vaikkapa kymmenen vuoden kuluttua. Kvanttitietokoneen saapumiseen olisi kuitenkin hyvä valmistautua ennakkoon, koska sen saapuminen voi mullistaa kyberturvallisuutta merkittävästi. (Liikenne- ja viestintäministeriö 2018.)

Symmetrisellä salauksella tarkoitetaan salausta, jossa on käytössä yksi salainen avain, joka on käytössään sekä vastaanottajalla että viestin lähettäjällä. Yhteisellä, salaisella avaimella onnistuu niin viestin kryptaus kuin viestin purkukin. Symmetrisen salauksen menetelmiä ovat jono- ja lohkosalausalgoritmit. Ongelmallista näissä on se, että molemmissa voi olla turvallisia sekä turvattomia vaihtoehtoja. (Liikenne- ja viestintäministeriö 2018.)

Salausmenetelmänä mielenkiintoinen ROT13 on helposti murrettavissa oleva turvaton salausmenetelmä. Siinä aakkoset muunnetaan niin, että salakirjoituskirjain vastaa oikeasti 13 kirjaimen päässä olevaa kirjainta aakkosissa. Salaus voidaan murtaa todella helposti ilman suurta vaivannäköä. (Ekdeeps 2021.)

3.2.5 RSA

RSA-menetelmään käytetty kryptaamisessa ja digitaalisissa allekirjoituksissa jo todella kauan 70-luvulta lähtien. RSA:ta pidetään kohtalaisen turvallisena menetelmänä mutta RSA:han liittyy myös ongelmia. Ongelmat liittyvät siihen, että RSA:n turvallisuutta ei olla voitu todistaa luotettavasti ja objektiivisesti. Pitkä käyttöaika ilman suurempia ongelmia toki tukee ajatusta siitä, että RSA on kohtalaisen turvallinen menetelmä. Tutkimukset aiheesta ovat kuitenkin empiirisiä tutkimuksia ja vahva tutkimusnäyttö puuttuu edelleen. Avoimeksi jäänyt kysymys on matemaattisten mallien tasolla ja todistusaineisto puuttuu. RSA on kuitenkin edelleen säilyttänyt asemansa ja sen avulla pyritään säilyttämään tiedon luottamuksellisuus, aitous sekä muuttumattomuus. RSA on ratkaisu tilanteeseen, jossa symmetrinen avain pitäisi saada vastapuolelle verkon yli. (Lindberg 2020)

RSA-tekniikassa käytetään kahta toisiinsa liittyvää erillistä salausavainta, joista toinen on julkinen avain ja toinen yksityinen avain. Salaus puretaan yksityisellä avaimella ja salaus tapahtuu julkisella avaimella. Yksityinen avain on vain salauksen purkajan tiedossa.

Salaaminen onnistuu tekniikassa myös yksityisen avaimen avulla ja silloin salauksen voi purkaa vastaavan julkisen avaimen avulla. (Lindberg 2020)

RSA:n tekniikka perustuu yksisuuntaiseen funktioon, jossa jokin asia voidaan suorittaa helposti yhteen suuntaan mutta käänteinen suunta on erittäin hankala. Hyvä mutta yksinkertaistettu esimerkki tästä on se, että suurilla luvuilla kertolaskujen laskeminen on helppo toimenpide mutta jakolasku on jo vaikeampi samoilla luvuilla käänteiseen suuntaan. RSA-tekniikan tulevaisuus riippuukin mahdollisesti pitkälti siitä, milloin jokin taho onnistuu kehittämään RSA-tekniikan murtamiseen tarvittavan algoritmin. Niin kauan tekniikan käyttö onnistuu, koska murtaminen tällä hetkellä on laskennalliselta kannalta katsottuna erittäin haastavaa. (Lindberg 2020)

3.2.6 VPN

VPN:n eli virtuaalisen erillisverkon käyttö esimerkiksi työpaikalla on yleensä tietoturvallisuuden kannalta järkevää. (Soon 2019.) Monet yritykset käyttävät VPN-tekniikkaa etätyön järjestämiseen niin, että työntekijä pääsee työpaikan verkkoon VPN-yhteyden avulla kotoa käsin. Myös monet yksityishenkilöt käyttävät erillisverkkoja omiin tarkoitusperiinsä. Yksityiskäyttäjät ostavat VPN-ratkaisuja tyypillisesti sovelluskaupasta. (Yle 2017).

VPN:n avulla yhteys voidaan piilottaa muilta ja toimiminen internetin yli on ainakin periaatteessa turvallisempaa. VPN muodostaa niin sanotun tunnelin verkkoyhteyden ympärille niin, ettei yhteyden fyysinen sijainti ole näkyvä muille verkon käyttäjille. VPN:n avulla on mahdollista saada yksi kerros lisää turvallisuuteen mutta toisaalta käyttäjän pitää luottaa VPN-ratkaisun tarjoajaan, koska periaatteessa paljastaa tälle tietonsa. (Yle 2017.) VPN:n käytössä on kuitenkin omat hankaluutensa ja riskinsä käyttäjälle ja yrityksen liiketoiminnalle. VPN mahdollistaa teknisesti sen, että sitä käyttävän tiedot paljastuvat VPN:n tarjoajalle. Yrityksissä käytettävät ratkaisut ovat yleensä luotettujen palveluntarjoajien maksullisia palveluja, ja riski tietojen paljastumiselle on täten pienempi muttei olematon. Maksuttomissa VPN-ratkaisuissa riski on suurempi. (Soon 2019.) Kuitenkin myös maksullisissa versioissa on paljastunut tietoturva-aukkoja (Yle 2017).

VPN-ratkaisuja on useita satoja ja vuonna 2015 paljastui esimerkiksi Hola! -sovellus vaaralliseksi VPN-ratkaisuksi. Vuonna 2017 tehtiin laaja tutkimus, jossa paljastui useiden palveluntarjoajien VPN-ratkaisujen turvattomuus tietovuotojen kannalta. Sovelluksiin liittyi myös ikäviä väärinkäytöksiä. Ongelmallista on se, että viranomaiset eivät valvo yritysten toimintaa. Luotettavalta kuulostava nimi tai edes suomen kieli ole takeita palvelun turvallisuudelle. (Yle 2017.)

VPN on laajassa käytössä yrityksissä matalien kustannustensa ansiosta verrattaessa kokonaan yksityisiin verkkoratkaisuihin. (Bhattrai & Nepal 2016.) Koronaviruspandemian alussa VPN-ratkaisujen kanssa oli ajoittain kapasiteettiongelmia, jotka sittemmin saatiin ratkaistua esimerkiksi split tunnel -tekniikan avulla. Etätyöpöytäratkaisut toivat myös tietoturvariskejä silloin, kun niiden käyttöönotto oli toteutettu huolimattomasti. (Traficom 2020c)

3.2.7 Ihmisen toiminta

Ihmisen inhimillisen toiminnan vaikutus tietoturvaan on aiheena mielenkiintoinen. Järviö kuvailee pro gradu -tutkielmassaan personallisuuden eri piirteiden vaikutusta tietoturvalliseen toimintaan. Sellaiset persoonallisuudenpiirteet kuten pahantahtoisuus ja epärehellisyys liittyvät jossakin määrin tutkimusten mukaan siihen, miten henkilö toimii työpaikalla tietoturvan suhteen. Tutkimustietoa on olemassa vain vähän mutta olemassa olevien tulosten perusteella esimerkiksi pahantahtoisuus persoonallisuuden piirteenä voi vaikuttaa tietoturvalliseen toimintaan työpaikalla hyvin suurella todennäköisyydellä. (Järviö 2018, 3,8.)

Mielenkiintoista Järviön tutkielmassa on se, että persoonallisuuden piirteillä on vaikutusta siihen, miten yrityksessä voitaisiin parhaiten estää tietoturvarikkeitä. Tämän vuoksi, ehkä hieman yllättäen, persoonallisuuden piirteitä tulisi tutkailla mietittäessä tietoturvallista toimintaa työpaikalla. Persoonallisuuden piirteet ihmisessä ovat yleensä kohtalaisen pysyviä ominaisuuksia. Pysyvyys mahdollistaa ihmisen toiminnan ennustettavuuden ainakin jollain tasolla. Toki tällöin on tunnettava muut tilanteeseen vaikuttavat taustamuuttujat. Persoonallisuutta ja sen piirteiden vaikutusta on tähän saakka tutkittu erittäin vähän suhteessa tietoturvaan. (Järviö 2018, 7.)

Tunnollisuuden ja sopuisuuden persoonallisuuspiirteiden on yhdistetty tutkimusten mukaan liittyvän hyviin tietoturvakäytäntöihin. Tunnollisuuden luonteenpiirteen oletetaan ohjaavan ihmistä tekemään tietoturvan kannalta hyviä ratkaisuja. Mielenkiintoista kyllä, iän ja sukupuolen merkitys tietoturvakäyttäytymisessä näyttäisi olevan marginaalinen. (Dawson, Debb & Shappie 2015, 2)

Oletusarvoisesti ihminen haluaa toimia sääntöjen ja ohjeiden mukaisesti. Ihminen on kuitenkin taipuvainen toimimaan toisella tavalla kuin oli alun perin suunnitellut. Ihmiselle on luonteenomaista olla huolissaan tietoturvallisuudesta mutta kuitenkin todellisuudessa toimia riskialttiilla tavalla esimerkiksi olemalla huolehtimatta omien tietojensa suojaamisesta.

Tämä voi olla yhteydessä siihen, että tahtotila on todellisuudessa kognitiivinen prosessi, kun taas todellista käyttäytymistä saattavat ohjata enemmänkin kussakin tilanteessa osin impulsiiviset ja suunnittelemattomat, alitajuiset prosessit. Toiminta ei näin ollen välttämättä perustu pelkkään kognitiiviseen prosessiin. (Dawson, Debb & Shappie 2015,1)

Mielenkiitoista oli Behaviour and Information Technology -lehden artikkelin mukaan se, että ihmisille vallitseva ajatusrakenne on se, että tietoturva on tärkeä asia ja tietoturvarikkeiden aiheuttamat seuraukset voivat olla katastrofaaliset mutta ei tällaisia katastrofeja osu minun kohdalleni. Tässä kyse vääränlaisesta optimismista, jossa takana on ajatus siitä, että ikäviä asioita tapahtuu vain muille ihmisille. Yleinen tietämys siitä, millainen on esimerkiksi hyvä ja vahva salasana, ei johda välttämättä käytännön tekoihin omien salasanojen parantamiseksi niin, että niitä olisi vaikeampi murtaa. (Glassman, Tam & Vandewauver 2010.) Samalla kun tietoisuus tietoturvallisista toimintatavoista lisääntyy, lisääntyvät myös käytössä olevat digitaaliset alustat ja käytännöllisyys menee usein tietoturvan edelle (Lord 2020).

3.2.8 Kouluttautuminen

Pandemian aikana monet tietoturvauhat korostuvat ihmisten työskennellessä kotoa käsin. Kouluttamisen ja informoinnin merkitys on tilanteessa ensiarvoisen tärkeää, koska moni tietoturvariski realisoituu juuri henkilön huolimattomuuden tai tietämättömyyden vuoksi. (Huhtaniitty 2021.) Tietoturvaan kohdistuvat uhat muuntautuvat ja uusia tapoja tehdä kyberhyökkäyksiä tulee jatkuvasti lisää. Tekniikan ollessa kunnossa hyökkäyksiä tapahtuu ihmisen tekemien inhimillisten virheiden takia. Tutkimusten mukaan kolmasosa etätyötä tekevistä ihmisistä myöntää vierailevansa aikuisviihdesivustoilla, joiden kautta koneelle voi päätyä haitallista materiaalia ja voi levitä sieltä myös yrityksen muihin järjestelmiin. (Uitti 2021.)

Lapin maakunnassa koulutettiin sosiaali- ja terveydenhuollon henkilöstöä tietoturva-asioissa verkkokoulutuksen avulla. Koulutuksen takana on UULA-projekti yhdessä Granite Partners Oy:n kanssa. Koulutus suoritettiin verkkoalustalla, jonne koulutukseen osallistuvat kirjautuvat käyttäjätunnuksen ja salasanan avulla. Koulutuksessa käytiin läpi teoriaa tietoturvasta ja tietosuojasta, tietojen käsittelystä, tietoturvallisesta toiminnasta sekä tietosuojan rikkomisesta. Koulutus sisälsi myös välitestejä sekä loppukokeen. (Anttila & Liimatta 2011, 30.)

Koulutukseen osallistuneille tehtiin jälkeenpäin kysely verkkokoulutuksen sisällöstä. Kolme neljäsosaa vastanneista koki, että he olivat oppineet uutta koulutuksen aikana.

Lähestulkoon puolet vastaajista kertoi, että olivat muuttaneet omia toimintatapojaan koulutuksen jälkeen. Muuttuneet toimintatavat olivat esimerkiksi salasanojen vaihtamista tietoturvan kannalta vahvemmiksi, varovaisuutta sähköpostin käsittelyssä sekä tietokoneen lukitsemista työasemalta poistuttaessa. Nämä kaikki ovat pieniä arkisia toimintatapoja, joilla voi kuitenkin olla suuri merkitys tietoturvan kannalta. (Anttila & Liimatta 2011, 30–31.)

Vastauksista oli kuitenkin havaittavissa myös se, että henkilökunnalle ei ollut kerrottu riittävän selvästi, miksi kouluttautuminen on tärkeää ja perusteltu koulutuksen sisällön tarpeellisuutta jokapäiväisessä työelämässä. Hankaluutena osalla oli myös ajan löytäminen koulutuksen käymiseen työpäivän aikana. Kyselystä selvisi myös, että vastaajien mielestä esimiesten tulisi enemmän tukea alaisiaan ja kannustaa koulutuksen suorittamiseen perustelemalla, miksi koulutus on tarpeellinen sekä järjestämällä tarvittavat puitteet koulutuksen suorittamiseen. (Anttila & Liimatta 2011,32.)

Yhdessä oppiminen on tehokas menetelmä ja sitä voisi kyselyn tulosten mukaan hyödyntää koulutuksen jälkeen keskustelemalla koulutuksen sisällöstä ja sen soveltamisesta käytäntöön. (Anttila & Liimatta 2011, 31–32.)

Vaikka koulutuksen ja informoinnin merkitystä tuodaan esiin yhtenä keinona parantaa tietoturvallisuutta, tieto siitä, mikä on esimerkiksi mahdollisimman turvallinen salasana ei kuitenkaan aina johda toiminnan muuttumiseen. Behaviour and Information Technology -lehden artikkelin mukaan kyky erottaa hyvä ja huono salasana ei johda toimintaan ja mukavuus ratkaisee. (Glassman ym. 2010.)

Monimutkaisen salasanan valinta ei ole mukavaa, koska sen käyttö koetaan haastavana ja samoja salasanoja käytetään mukavuussyistä eri palveluissa uudelleen. Osa jopa paljastaa salasanan läheisimmille ihmisille kuten läheisille ystäville ja perheenjäsenille. Mukavuudenhalu näyttää olevan yhteinen nimittäjä edellä mainituille tavoille toimia. Tietoturvallinen, monimutkainen salasana näyttää assosioituvan monelle mukavuuden vähentymiseen. Artikkelin mukaan lisäkoulutus ei välttämättä johda toimintaan eikä vahvempien salansanojen valintaan, koska mukavuustekijät menevät ihmisen mielessä tietoturvallisuuden edelle. (Glassman ym. 2010.)

Mielenkiintoista on se, että tutkimusten mukaan jopa tietoturvan parissa työskentelevillä on taipumus käyttää salasanoja uudelleen eri järjestelmissä. Salasanojen uudelleen käyttö on suuri tietoturvariski. Tämä seikka puhuu sen puolesta, että tietoisuus riskistä ei johda toimintaan vaan valintoja ohjaa jokin muu asia. Ihmisen omilla sisäisillä malleilla vaikuttaisi olevan suuri vaikutus ihmisen toimintaan, vaikka tietoa on runsaasti saatavilla.

(Bauer ym. 2016, 6.) Toisaalta koulutusta ja informointia pidetään tärkeänä osana kyberturvallisuutta ja tietoisuuden lisäämisen katsotaan parantavan kyberturvallista toimintaa. (Khalid, Rahman, Sairi, Zizi 2020).

3.2.9 Kyberhyökkäysten torjunta

Avainasemassa kyberhyökkäyksien torjunnassa on ennaltaehkäisy sekä mahdollisimman aikainen hyökkäyksen havaitseminen. Perinteisesti kyberrikollisuuden torjunnassa on keskitytty hyökkäysten torjuntaan. (Brewer 2017.) Palomuurit toimivat hyvin suomalaisyrityksissä. Ongelmana onkin se, että jo hyökkäyksen tapahtuessa ovat vastatoimet puutteelliset eikä toipumissuunnitelma ole riittävän kattava. Riskienhallintaa on hyvä suunnitella ja harjoitella ennalta. (Ahtokivi 2021.) Useat hyökkäykset ovat älykkäästi toteutettu niin, että niiden huomaaminen voi olla vaikeaa. Tärkeää olisi panostaa myös mahdollisesti jo tapahtuneiden hyökkäysten eliminointiin mahdollisimman aikaisessa vaiheessa, jotta taloudellinen vahinko voidaan minimoida. (Brewer 2017.)

Täydellistä suojaa hyökkäyksiä vastaan on mahdotonta rakentaa. Hyvistäkin toimenpiteistä ja toimintatavoista huolimatta uhkat voivat realisoitua ja haitta voi saavuttaa yrityksen sisäverkon vaikkapa päätelaitteen kautta. Koska resurssit ovat usein rajalliset tietoturvankin suhteen, olisi hyvä keskittyä havainnointiin, havaitsemiseen sekä jo realisoitujen uhkien tehokkaaseen ja nopeaan eliminointiin. Organisaatioiden tulee huolehtia siitä, että resurssit tietoturvan tason ylläpitoon ovat riittävät, jotta havainnointi ja aikainen puuttuminen olisivat mahdollisia. (Vesajoki 2018.)

Tietoturvaa ajatellaan perinteisesti monessa yrityksessä erillisenä lisäosana ja tietoturvalle annetaan oma budjettinsa. Toimivat tietoturva tulee kytkeä osaksi kaikkea toimintaa ja osaksi yrityksen identiteettiä. Tietoturvan tarve on ymmärrettävä, jotta se voidaan mitoittaa oikein kullekin yritykselle sopivalle tasolle. Uhkat tulisi ensin tunnistaa, sitten voidaan suojautua. Jatkuva havainnointi on suojauksesta huolimatta ensiluokkaisen tärkeää, jotta uhkin realisoituessa osataan toimia ja torjua mahdolliset uhat. Toipumissuunnitelma tulisi olla osa yrityksen tietoturvastrategiaa. (Korkiakoski 2021.)

Kaikki kyberhyökkäykset eivät tähtää välittömään taloudelliseen hyötyyn, vaan pohjatyötä saatetaan tehdä pitkään tarvittavan informaation kokoamiseksi. Tiedon osista hyökkääjät saavat rakennettua itselleen kokonaiskuvan, jonka kautta he voivat saavuttaa lopulta taloudellista tai muuta hyötyä. Joskus merkityksettömältä vaikuttava tieto voi olla osa

palasista rakentuvaa kokonaisuutta. Tämän takia kaikkea salassa pidettävää tietoa on syytä varjella tarkoin. Joskus motiivina voi olla myös pelkkä kiusanteko. (Korkiakoski 2021.)

Onnistunut kyberhyökkäys aiheuttaa usein maineen menetyksen ja suuri osa kyberhyökkäyksistä jää ilmoittamatta kokonaan. Osa kyberhyökkäyksistä jaa ilmoittamatta myös sen vuoksi, että niitä ei havaita. Kyberhyökkäysten todellista määrää on vaikea ilmoittaa ja tarve mittaamiselle ja raportoinnille on todellinen. Taloustieteilijät ovat kokeilleet koneoppimista ja tietokonelingvistiikkaa löytääkseen ratkaisun sille, että yhä useampi kyberhyökkäys tulisi julki. (Paasonen 2021)

3.2.10 Zero trust -ajattelu

Zero trust -ajattelu tarkoittaa yksinkertaisimmillaan verkkoympäristössä toimimisessa sitä, että kaikki, mitä ei ole erikseen sallittu, on kielletty. Nykyajan monimutkaistuvissa ympäristöissä toimiminen edellyttää uudenlaista ajattelutapaa aiemman sijaan, jossa kaikki mitä ei ollut erikseen kielletty, oli lähtökohtaisesti sallittua. Vanhalle ajattelumallille oli ominaista se, että ajateltiin yritysverkon sisäpuolen olevan turvallinen. Verkon sisällä toimijat ovat luotettavia, verkon ulkopuolella toimijat ovat epäluotettavia lähtökohtaisesti. Esimerkiksi palomuuri on jakanut verkon sisä- ja ulkopuolen turvalliseen ja ei-turvalliseen alueeseen. (Rokka 2021.)

Zero trust on toimintamalli, jossa käyttäjän autentikointi tehdään monitasoisesti. Kun henkilö kirjautuu vahvan tunnistautumisen vaativalla menetelmällä, sen lisäksi tunnistetaan käytössä oleva laite ja/tai laitteen sijainti. Mikäli samaan järjestelmään yritetään kirjautua hetken päästä esimerkiksi toisesta maasta ja toisella laitteella, voidaan tietoturvarike mahdollisesti havaita. (Huhtaniitty 2021.)

Palomuurille määritetään säännöt pääsynhallinnalle IP-avaruuksia, osoitepareja sekä porttisääntöjä OSI-mallin kolmannella eli verkkotasolla tasolla hyödyntäen. Tietoturva tulisi kuitenkin ulottaa OSI-mallin seitsemännelle tasolle eli sovellustasolle saakka. Yrityksissä ympäristöt ovat usein siroteltu monen eri toimijan konesaleihin ja palveluihin. Ympäristöt ovat erittäin monitasoisia ja monimutkaisia. Istuntoja voi olla yhtaikaa monessa maassa eikä tällaisen ympäristön hallinta ole enää kovin yksinkertaista. Verkko kyllä osaa suodattaa IP-paketteja mutta kun mukana voi olla satoja eri sovelluksia, ei tietoturvallinen työskentely perinteisillä tietoturvaratkaisuilla välttämättä ole enää mahdollista. (Rokka 2021.) Tietoturvan on ulotuttava päätelaitteelle saakka loppukäyttäjiä myöden. Suojauksen kokonaisvaltaisuuteen on panostettava. (Huhtaniitty 2021).

Zero trust -ajattelu lähtee ajatuksen tasolta ja lähestymistapa pohjaa osittain ihmisen omaan käyttäytymiseen. Kaikkea ja kaikkia epäillään ja jokainen on potentiaalinen riski verkon toimintaympäristössä. Nimensä mukaisesti kehenkään ei ole luottamista. Toiminen verkkoympäristöissä perustuu verifikaatioon ja tässä kohtaa mukaan tulevat tekniset ratkaisut ajattelumallin tueksi. Luottaa ei voi pelkkiin teknisiin ratkaisuihin vaan fokus on ihmisen ajattelussa. (Hood 2021.)

Zero trust -ajattelu ei kuitenkaan ole tällä hetkellä vielä kovin helposti toteutettavissa ja esteenä on muun muassa vanha, zero trust -ajattelua tukematon infrastruktuuriympäristö. Ympäristön päivittäminen on monesti kallista. (Hood 2021.) Tietoturvasta puhuttaessa on kuitenkin muistettava se, että mahdollinen tietomurto voi tulla yritykselle todella kalliiksi ja jälkien korjaaminen on hankalampaa kuin tapahtuman ehkäiseminen. Rahallisen menetyksen rinnalla uhkana on lisäksi aina maineen menetys. Maineen menetys voi johtaa asiakkaiden siirtymisen kilpailijoille. (Högmander 2019.)

Zero trust -ajattelu on perusteltua, kun yritykset ovat entistä monikansallisempia eikä työpaikan sijainnilla ja asuinpaikalla ole välttämättä enää merkitystä yhtä paljon kuin ennen. Pandemia on osaltaan kiihdyttänyt tätä kehitystä ikään kuin sivutuotteena. Työntekijöitä kirjautuu yrityksen verkkoon eri puolilta maailmaa, eikä toiminta ole enää osin ollenkaan yrityksen turvallisuusosaston hallinnassa. Zero trust -ajattelu on viitekehys, jossa pyritään suojautumaan niin yrityksen sisä- kuin ulkopuolelta tulevia uhkia vastaan. (IBM 2021.)

3.2.11 Automaatio ja tekoäly

Automaation avulla voidaan mahdollisesti estää verkkohyökkäyksiä esimerkiksi reitittimen avulla oikeanlaisten konfiguraatioiden kautta. Automaatio mahdollistaa toistettavissa olevien prosessien rakentamisen. Automaatiolla voidaan varmistaa, ettei mahdollisia tietoturva-aukkoja jää huomaamatta. Esimerkki tällaisesta tietoturva-aukosta voisi olla yksi reititin, joka on inhimillisestä syystä jäänyt suojaamatta ja muodostaa riskin myös muille samassa verkossa oleville laitteille. Automaatiolla tällainen inhimillinen unohdus on mahdollista estää. Automaatio tarkistaa kaikki laitteet määriteltyjen asetusten kautta ja huomaa mahdolliset poikkeavuudet. (Slattery 2021.)

Huomionarvoista on myös se, että vain osa kyberhyökkäyksistä on toteutettu ihmisen toimesta. Hyökkäysten takana voivat olla automatisoidut botit, jotka on ohjelmoitu levittämään haittaohjelmia sekä tekemään tietomurtoja. (Korkiakoski 2021.) Nykyään monet tietoturvaratkaisut tallentavat dataa, jonka avulla voidaankin saada tekoäly mukaan

tietoturvaratkaisujen toteuttamiseen. Tekoäly voidaan valjastaa esimerkiksi tunnistamaan poikkeavia tapahtumia, joiden voidaan katsoa ennakoivan tai tarkoittavan tietoturvapoikkeamaa. Tekoälyä voidaan opettaa olemaan huomioimatta epäolennaisia asioita, jotka kuormittaisivat tietoturvan parissa työskenteleviä henkilöitä turhaan. Tekoälyn havaitessa jotakin poikkeavaa, asiantuntija voi ottaa tapahtuman tarkempaan tarkasteluun. Näin tekoälyä voidaan käyttää apuna havainnoinnissa ja ennakoinnissa. Koneoppimista on hyödynnetty jo usean vuoden ajan tietoturvaratkaisuissa. (Högmander 2019.)

3.2.12 Työskentely kotitoimistolla

Etätyön myöstä erilaiset viestintään tarkoitetut sovellukset on otettu osaksi jokapäiväistä työtä. Kun sovelluksen kautta jaetaan arkaluontoista ja salassa pidettävää tietoa, on varmistuttava sovelluksen tietoturvan tasosta. Olennaista on, välittyykö viesteistä jotakin kolmansille osapuolille ja kulkevatko viestit jonkin toisen valtion läpi. Olennaista on myös se, tallennetaanko viestit jonnekin, siirtyykö metatietoa jonnekin. (Valonen 2020)

Kotitoimiston ongelmana on se, että kotona liikkuu työntekijän lisäksi työntekijän perheenjäseniä. Kulunvalvontaa ei yleensä ole ja joskus työskennellään samassa tilassa muiden perheenjäsenten kanssa. Kotona työskennellessä tulee muistaa työhön kuuluvien luottamuksellisten asioiden salassapito ja se, etteivät muut kuule esimerkiksi puheluja. Kun työkoneelta lähdetään vaikkapa syömään tai wc:hen, tulee näyttö lukita kuten työpaikallakin tehtäisiin. Myös tietoturvaan liittyvät perusasiat on pidettävä kunnossa kuten reitittimen asianmukainen konfigurointi, VPN-yhteyden käyttö, palomuuri ja virusturva. Käytettävän pilvipalvelun turvallisuudesta on varmistuttava. (Valonen 2020)

3.2.13 Etätyöskentelyyn liittyvät riskit

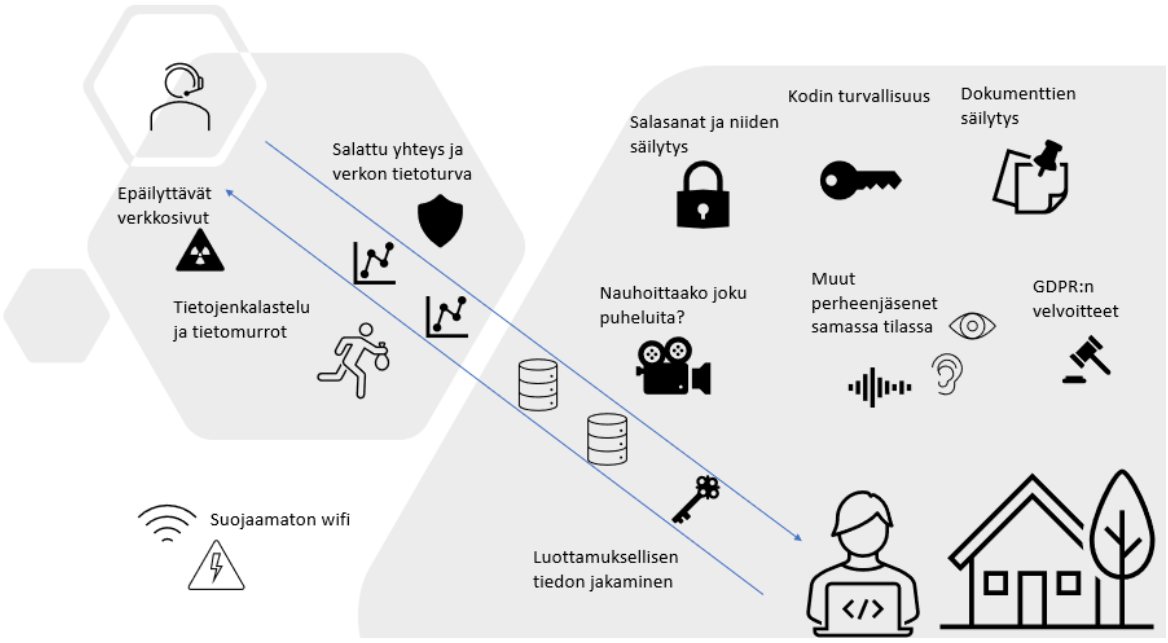
HP on teettänyt tutkimuksen etätyöhön liittyvistä riskeistä ja tuloksia käsitellään Security-lehden artikkelissa keväältä 2021. Tutkimuksen mukaan työtapojen muutos lisää uusia kyberriskejä yrityksille, yksilöille ja salattavalle tiedolle. Jopa 70 % työntekijöistä myönsi ajoittain käyttävänsä työkonettaan omiin, henkilökohtaisiin asioihinsa kun taas 69 % tutkimuksessa mukana olleista käytti omia henkilökohtaisia tietokoneitaan työtehtäviensä hoitamiseen. 30 % tutkimuksessa mukana olleista antoi jonkin toisen henkilön käyttää omaa työkonettaan. (Security 2021.) Mikäli henkilö käyttää omia laitteitaan työtehtäviensä hoitamiseen, tulisi laitteet varustaa työpaikan viruksentorjuntaohjelmistoilla sekä turvallisilla kirjautumiskäytännöillä. (Crossland, Ertan & Michaelides 2021,11). Työkoneen käyttäminen esimerkiksi henkilökohtaisen sähköpostin lukemiseen voi aiheuttaa tietoturvauhan. Yksityisen sähköpostilaatikon kautta rikollinen voi päästä suoraan yrityksen tietoihin käsiksi. (Huhtaniitty 2021.)

Etätyöskentelyssä erilaiset tietoturvauhat korostuvat, kun työskentely tapahtuu etänä ja käytössä on paljon erilaisia alustoja. Alustojen määrän kasvaessa kasvaa myös hyökkäyspinta-ala rikollisille. Tietoturva-aukkoja voi olla yrityksen vpn-yhteydessä kuten myös laitteissa. (Huhtaniitty 2021.)

Kuva 8: Top 6 tietoturvauhat (mukaillen Huhtaniitty 2021)

Suurimmat tietoturvauhat tällä hetkellä liittyvät tietojenkalasteluun, kiristys- ja haittaohjelmiin, uhkiin yrityksen sisältä, GDPR-rikkeisiin sekä vanhentuneisiin ohjelmistoihin. (Huhtaniitty 2021).

Etätyöskentely ja työntekijöiden oma toiminta ovat lisänneet kyberhyökkäyksiä, ja pandemian aikana ne ovat lisääntyneet jopa 238 % maailmanlaajuisesti tarkasteltuna. Vapaa-ajan ja työajan rajat ovat hämärtyneet ja hyökkäysrajapinta on kasvanut. Epäilyttävän sähköpostliitteen avaaminen voi tuoda mukanaan suuria ongelmia. Työpaikkojen it-osastot, joiden tehtävänä on pitää huolta yrityksen kyberturvallisuudesta, joutuvat osin työskentelemään tavallaan sokkona, koska näkyvyyttä ei ole työntekijöiden koteihin saakka. Valvonta on hankalaa ja periaatteessa joku muu voi käyttää laitteita kuin työntekijä itse. (Security 2021.)



Kuva 9. Tietoturvariskit kotitoimistolla

3.2.14 Avoimet WLAN-yhteydet

Avoimia, langattomia verkkoyhteyksiä voidaan pitää perustellusta syystä suurena riskinä tietoturvallisuudelle. Monissa julkisissa tiloissa tarjotaan niiden käyttäjille avoimia verkkoja. On kuitenkin tiedostettava, että verkkorikolliset saattavat luoda väärennetyn verkon, joka näyttäytyy käyttäjälle päällisin puolin samanlaisena kuin esimerkiksi kauppakeskuksen WLAN-verkko. Nimi voi olla sama ja käyttäjä helposti erehtyy liittymään tällaiseen väärennettyyn avoimeen verkkoon. Rikollinen pääsee verkkoon kirjautumisen kautta käsiksi käyttäjän yksityisiin tietoihin. Wifi-toiminto olisi hyvä pitää pois käytöstä omalla laitteella, jottei laite pääse avoimiin verkkoihin kirjautumaan. (Lorentsen 2020.)

3.2.15 Turvallinen etätyöympäristö

Etätyötä tehdessä työtilan tulee olla turvallisesti sijoitettu niin, etteivät ulkopuoliset pääse näkemään tietokoneen näyttöä. Tietojenkäsittelyn pitää tapahtua niin, että tiedon luottamuksellisuus saadaan säilytettyä. Tietokonetta ei pidä laittaa ikkunan eteen niin, että ikkunasta voisi edes teoriassa kukaan nähdä näyttöä. Nykytekniikalla on mahdollista kameran avulla nähdä tietokoneen näyttö hyvinkin kaukaa. Hyvästä äänieristyksestä on myös huolehdittava niin, etteivät ulkopuoliset kuule luottamuksellisia puhelinkeskusteluja. Tietokoneen verkkolevylle kannattaa tallentaa mahdollisimman vähän luottamuksellista materiaalia ja työaseman levyn suojauksesta on huolehdittava (Pitkänen 2021.)

Etätyössä toimintatavat ovat tutkimusten mukaan jonkin verran erilaiset kuin toimintatavat toimistolla tietoturvallisen työskentelyn suhteen. Tämän vuoksi kouluttaminen ja informointi ovat ensiarvoisen tärkeitä. Myös esimiehen tuki on tärkeää. Tuen puute voi johtaa siihen, että sääntöihin ja ohjeisiin ei sitouduta ja toimintatavat muuttuvat niin, että tietoturvan taso heikentyy. Toisaalta saadun informaation määrä ei aina takaa sitä, että itse toimintatavat muuttuisivat. Tietoisuuden lisääntyminen ei välttämättä johda muutokseen. (Michaelides 2021.)

3.3 Johtopäätökset ja oppimisprosessi

Kun luottamuksellista tietoa päätyy vääriin käsiin, ovat vaarassa sekä yrityssalaisuudet sekä yksilön henkilökohtaiset, salassa pidettävät tiedot. Yrityksen tiedon vaarantuessa vaaratuvat luonnollisesti myös asiakkaiden tiedot.

Tietoturvapoikkeamatilanteiden hallintaan ja tietoturvapoikkeaman estoon on käytössä monia keinoja. Kuitenkin ihminen on tutkimusten mukaan suuri riskitekijä tietoturvassa. Teknisten ratkaisujen tarjoaman hyöty on vähäinen tai olematon, jos ihmisten toiminta ei ole tietoturvallista.

Kaikki työntekijät eivät välttämättä ole motivoituneita etätyön tekoon, kun tilanteeseen on jouduttu pandemiatilanteen vuoksi ja etätyö on välttämätön toimenpide vähentää tartuntojen leviämistä. Työntekijät saattavat kokea stressiä tilanteen edessä, tilat ja olosuhteet kotona eivät aina ole optimaaliset etätyön tekemiselle. Negatiivinen stressi voi entisestään vähentää motivaatiota ja tarkkaavaisuus alenee. Tämänkaltainen tilanne aiheuttaa sen, ettei tietoturvaan jakseta paneutua niin paljon, kun tilanne sitä edellyttäisi. Joskus pieni virhe voi johtaa ikäviin seurauksiin yksilön itsensä, yrityksen ja asiakkaiden kannalta ja vaikuttaa yksilön työnteon edellytyksiin sekä yrityksen perusteisiin olla olemassa.

Erittäin mielenkiintoinen näkökulma on se, että ihmisen toiminta on erittäin vahvassa roolissa tietoturvallisuudessa. Yllättävää on se, että koulutuksen oletetaan tuovan hyötyjä tietoturvallisemmalle toiminnalle mutta vastakkaisiakin tuloksia on. Ihmiselle tyypillinen mukavuudenhalu menee tietoturvallisen toiminnan edelle. Onko tietoturvallinen toiminta osin persoonakysymys?

Nykyajan jatkuvasti monimutkaistuvissa it-toimintaympäristöissä tietoturvaan liittyviä toiminta- ja ajatusmalleja on välttämätöntä päivittää. Palomuureihin nojaavat turvallisuustoimet eivät pelkästään enää riitä globaalissa toimintaympäristössä, jossa ohjelmistoja on suuri määrä ja istunnot voivat sijaita vaikkapa vastakkaisella puolella maapalloa. Tekninen kehitys luo uusia mahdollisuuksia myös rikollisille ja tuhot moninkertaistuvat. Tekoäly tulee tulevaisuudessa eittämättä vaikuttamaan tietoturvaympäristöihin. Herää kysymys, missä vaiheessa ihmisen kapasiteetti hallita monimutkaisia ympäristöjä loppuu. Vai onko väistämätön jo osittain tapahtumassa?

Ennen opinnäytetyön aloittamista oma ennakkokäsitykseni tietoturvasta oli teknologia- ja tekniikkakeskeinen. Uskoin suurimpien uhkien kohdistuvan teknisiin ratkaisuihin ja uskoin myös tietoturvaongelmien ratkeavan pääosin teknisin keinoin. Työn myötä käsitykseni on

muuttunut. Teknisillä ratkaisuilla on eittämättä oma paikkansa ja roolinsa tietoturvassa mutta ihmisen toiminnalla on tutkimusten mukaan yllättävän suuri rooli tietoturvan toteutumisessa. Kyberturvallisuuden merkitys tulee varmasti korostumaan tulevaisuudessa, kun suuri osa palveluista siirtyy verkkoon ja informaation ja datan valta on suuri. Vanha sanonta, tieto on valtaa, pitää paikkaansa jopa pelottavan hyvin. Tietoturvallisuudessa yhdistyvät teknologia ja ihmisen psykologia sekä biologia hyvin mielenkiintoisella tavalla. Inhimillinen kohtaa äärimmäisen loogisen laskentatehon. Inhimillisen toiminnan ja laskentatehon yhdistelmä voi parhaimmillaan lisätä tietoturvaa mutta voi pahimmillaan myös johtaa katastrofeihin. Kyse on yhteisvaikutuksesta, joka on kuin arvaamaton kemiallinen reaktio. Laskentateho on kohtalaisen ennustettavaa, inhimillinen ihmismieli ei.

Opinnäytetyön tekeminen on ollut erittäin mielenkiintoinen prosessi alusta loppuun saakka ja aihevalinta on ajankohtainen ja tulevaisuudessa entistä tärkeämpi. Olen oppinut paljon uutta tietoa, jota työssäni olen käsitellyt objektiiviselta kantilta, mutta jota voin soveltaa myös käytäntöön.

3.4 Jatkotutkimusaiheet

Tulevaisuudessa tarvitaan lisää tutkimusta siitä, kuinka paljon tietoturva on heikentynyt laajamittaisen etätyöskentelyn aikana ja toisaalta siitä, paljonko uusia tilanteen seurauksena syntyneitä uhkia on vielä huomaamatta. Rikolliset ovat valitettavan usein askeleen edellä turvallisuusstrategioista. Valppaus on tarpeen kaikilla yrityksen tasoilla työntekijöistä johtoportaaseen ja tietoturvayksikköön. On hyvä epäillä jossain määrin kaikkea. Näin saattaa esiin tulla seikkoja, jotka voivat johtaa tietoturvapoikkeamiin. Verkossa ei saa luottaa kritiikittä mihinkään.

Tutkimusta tarvitaan lisää myös ihmisen toiminnan vaikutuksista kyberturvallisuuteen ja olosuhteista, joissa nämä turvallisuusuhat syntyvät. Iso osa näistä turvallisuusuhista, kun tutkimusten mukaan syntyy ihmisen toiminnan seurauksesta. Teknisten toteutusten rinnalla pitäisi miettiä tilanteita, jotka voivat suoraan tai välillisesti johtaa ongelmiin tietoturvan kanssa. Tärkeää on sitoutettava tietoturvalliseen toimintaan, työntekijät tarvitsevat tiedon ja sääntöjen lisäksi tukea ja keskustelua.

Lisätutkimusta tarvitaan koulutuksen ja informoinnin merkitysestä tietoturvalliselle toiminnalle. Tulokset näiden kahden merkityksestä ovat tutkimusten valossa ristiriitaiset. Toisaalta koulutuksella ja informoinnilla on suuri merkitys kyberturvallisuuteen mutta toisaalta

tutkimusten mukaan ihmisen toimintaa ohjaavat muun muassa mukavuudenhalu ja ihmisen omat sisäiset mallit.

Tietoturva etätyössä on erittäin kiinnostava ajattomuutensa ja toisaalta ajankohtaisuutensa vuoksi. Tieto yhdistyy tässä hyvin käytännönläheisesti reaalimaailmaan ja tutkittu tieto on konkreettista. Hyödynnettävän tutkimustiedon pitää olla saavuttanut hyvä reliabiliteetti sekä olla ajankohtaista.

Pandemia ei mahdollisesti ole täysin ohi vielä pitkää aikaan. Tilanne voi pahimmillaan jatkua useiden vuosien ajan jollain tasolla. Myös uuden pandemian riski on mahdollinen tulevaisuudessa. Yritysten ja yksilöiden on kehitettävä kestävät toimintatavat ja vakinaistettava ne käytäntöön, vaikka tarve uudistuksille on osittain tullut pandemian myöstä. Uusi normaali tarvitsee uutta ja vanhaa tietoa, joidenka pohjalta voidaan kehitellä uusia toimintatapoja myös pitkälle tulevaisuuteen.

Koronarokotusten yleistyessä monet yritykset siirtyvät pikkuhiljaa hybridityöskentelyyn, joka on uusi toimintamalli kaikille. Hybridimallissa työskennellään osaksi kotona, osaksi yrityksen toimitiloissa. Hybridityöskentelyn vaikutuksista tietoturvaan ja luottamuksellisuuden säilyttämiseen tarvitaan lisätutkimusta.

Lähteet:

Ahtokivi, I. 2021. Hybridityö lisännyt yritysten tietoturvan riskejä.
Luettavissa: https://www.verkkouutiset.fi/hybridityosta-lisaa-riskeja-yritysten-tietoturvalle/#07a3137a. Luettu 12.9.2021.

Ambarish, K., Nicolas, C. & Nitesh, S. 2014. A Comparative Usability Evaluation of Traditional
Password Managers. Luettavissa: https://www.researchgate.net/publication/220833967_A_Comparative_Usability_Evaluation_of_Traditional_Password_Managers. Luettu 13.11.2021

Anttila, L. & Liimatta, S. 2011. Tietoturva- ja tietosuojaosaaminen koko henkilöstön perustaidoksi.
Finnish Journal of eHealth and eWelfare, 3, 1, s. 29-32.

Bauer, L., Blase, U., Christin, N., Cranor, L., Durity, A., Huh, P., Komanduri, S., Mazurek, M., Sean, S., Shay, R., 2016
Designing Password Policies for Strength and Usability. ACM Journals Luettavissa: https://dl.acm.org/doi/abs/10.1145/2891411. Luettu 13.11.2021

Bazaz, T.& Aqeel, K. 2016. A Review on Single Singn
on Enabling Technologies and Protocols. International Journal of Computer Applications, 151,11, s.18-22.

Belloni, C. Is SSO Secure? Luettavissa: https://www.getkisi.com/academy/lessons/is-sso-secure. Luettu 19.9.2021.

Bhattrai, S. & Nepal, S., 2016. VPN research (Term Paper).
Luettavissa: https://www.researchgate.net/publication/289120789_VPN_research_Term_Paper. Luettu 2.10.2021.

BLC, tietoturvaopas, 2018. Montako tietoturvan kehää suojelee liiketoimintaasi? Luettavissa: https://cdn2.hubspot.net/hubfs/2067663/Ladattavat%20oppaat%20pdf/BLC-Tietoturvaopas.pdf. Luettu 11.3.2021.

Brandenburg, R. & Mee, P., 2020. Cybersecurity for a Remote Workforce. Luettavissa: https://sloanreview.mit.edu/article/cybersecurity-for-a-remote-workforce/. Luettu 15.2.2021.

Burr, W., Grassi, P., Fenton, J., Newton, E., Perlner, R., Regenscheid, A. & Richter, J., 2017.
Digital Identity Guidelines Authentication and Lifecycle Management. NIST Special Publication 800-63B, U.S Department of Commerce. Luettavissa: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf. Luettu: 9.9.2021.

Crossland, G., Ertan, A. & Michaelides, N., 2021 Remote Working and Cyber Security, Literature Review. Research Institute for Sociotechnical Cyber Security, Lontoo.
Luettavissa: https://www.researchgate.net/publication/349396561_Remote_Working_and_Cyber_Security_Literature_Review. Luettu 13.9.2021

Dawson, C., Debb, S. & Shappie A., 2015. Personality as a Predictor of Cybersecurity Behavior. Psychology of Popular Media Culture. Luettavissa: www.researchgate.net/publication/333326382_Personality_as_a_Predictor_of_Cybersecurity_Behavior. Luettu 10.9.2021.

Digitaalinen Helsinki. Luokittelu datan käsittelysääntöjen näkökulmasta.
Luettavissa: https://digi.hel.fi/esittely/helsinki-datastrategia/helsinki-datastrategia-luku-4/luku-43/. Luettu 12.11.2021.

Ekdeeps, 2021. This is ROT13, an encryption algorithm so simple that it has been revived to hide spoilers.
Luettavissa: https://tekdeeps.com/this-is-rot13-an-encryption-algorithm-so-simple-that-it-has-been-revived-to-hide-spoilers/.
Luettu: 12.11.2021

Elizarraras, J., Hirschi, K., Luevanos, C., Yeh, J., 2017. Analysis on the Security and Use of Password Managers.
Luettavissa: https://www.researchgate.net/publication/324096476_Analysis_on_the_Security_and_Use_of_Password_Managers.
Luettu 13.11.2021.

Forcepoint, How single sign-on works. Luettavissa: https://www.websense.com/content/support/library/web/hosted/sso_guide/how_sso_works.aspx. Luettu: 12.11.2021.

Glassman, M., Tam, L.& Vandenwauver, M., 2010. The psychology of password management: A tradeoff between security and convenience.
Luettavissa: https://www.researchgate.net/publication/220208616_The_psychology_of_password_management_A_tradeoff_between_security_and_convenience
Luettu: 30.10.2021.

Heljaste, J-M., 2020 Tietoturva etätöissä ei ole yksinkertainen asia edes etätyön konkareille. Luettavissa: https://www.mpy.fi/yritykset/blogi/tietoturva-etatoissa-ei-ole-yksinkertainen-asia-edes-etatyon-konkareille. Luettu: 10.2.2021.

Hood, L., 2021. Zero-trust security: Assume that everyone and everything on the internet is out to get you – and maybe already has.
Luettavissa: https://theconversation.com/zero-trust-security-assume-that-everyone-and-everything-on-the-internet-is-out-to-get-you-and-maybe-already-has-160969.
Luettu 16.10.2021.

Huhtaniitty, J., 2021. Tietoturvauhat vuonna 2021–5 isoa trendiä.
Luettavissa: https://www.bonfire.fi/tietoturvauhat-vuonna-2021-5-isoa-trendia/.
Luettu 17.10.2021

Högmander, J., 2019. Tekoäly on mullistanut tietoturvan - ihmistäkin tarvitaan vielä.
Luettavissa: https://blog.f-secure.com/fi/tekoaly-mullistanut-tietoturvan-ihmistakin-tarvitaan-viela/.
Luettu: 16.10.2021.

IBM, 2021. What is zero trust? Luettavissa https://www.ibm.com/topics/zero-trust.
Luettu 16.10.2021.

Isotalo, V., Vahva salasana on avain turvalliseen netin käyttöön.
Luettavissa: https://lounea.fi/yrityksille/ajankohtaista/artikkelit-yritysasiakkaille/vahva-salasana-avain-turvalliseen-netin. Luettu:30.10.2021

Järvinen, P. & Rousku K. 2017. Työpaikan tietoturvaopas: tunnista uhat, hallitse riskit. Alma Talent Oy. Helsinki.

Järviö, H. 2018. Ihminen osana tietoturvaa: persoonallisuus ja perusteltu toiminta tietoturvakäyttäytymisen taustalla. Pro gradu -tutkielma. Lääketieteellinen tiedekunta / psykologian ja logopedian osasto. Luettavissa: https://helda.helsinki.fi/bitstream/handle/10138/236391/Gradu_HJ.pdf?sequence=2&isAllowed=y. Luettu 10.9.2021.

Kasunic, K., 2021. 9 parasta turvallista salasanojen hallintaohjelmaa 2021. Luettavissa: https://fi.vpnmentor.com/blog/parasta-turvallista-salasanojen-hallintaohjelmaa/
Luettu: 30.10.2021

Khalid, F., Rahman, N., Sairi, I., Zizi, N., 2020. The Importance of Cybersecurity Education in School.
International Journal of Information and Education Technology, 10, 5. Luettavissa: https://dl.acm.org/doi/pdf/10.1145/2891411.
Luettu 13.11.2021.

Korkiakoski, M., 2021. Kyberhyökkäyksen motiivi ei aina ole suora taloudellinen hyöty, vaan motiiviksi riittää myös kiusanteko.
HP Finland Oy & Netox Oy. Luettavissa: https://www.tivi.fi/kumppanisisallot/hp-netox/kyberhyokkaysten-motiivi-ei-aina-ole-suora-taloudellinen-hyoty-vaan-motiiviksi-riittaa-myos-kiusanteko/. Luettu 15.10.2021.

Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. 2018. Uusi tietosuojalainsäädäntö. Alma Talent Oy. Helsinki.

Kuparinen, K., 2019, Kertakirjautumisen hyödyt. Luettavissa: https://www.vitecsoftware.com/fi/tuotealue/avoine/blogi/kertakirjautuminen/. Luettu: 30.9.2021.

Kyberturvallisuuskeskus, Salasanat haltuun. Neuvoja salasanojen käyttöön ja hallintaan. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Salasanat_haltuun.pdf Luettu: 30.10.2021.

Leinonen, A., 2021. WLAN-verkkojen tietoturva. Kandidaattitutkielma. Tampereen yliopisto. Informaatioteknologian ja viestinnän tiedekunta. Luettavissa: https://trepo.tuni.fi/bitstream/handle/10024/133875/LeinonenAarre.pdf?sequence=2&isAllowed=y. Luettu: 11.9.2021.

Liikenne- ja viestintäministeriö, 2018. Sähköisen viestinnän salaus- ja suojausmenetelmät.
Luettavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160614/LVM_02_2018_Sahkoisen_viestinnan%20salaus_ja_suojaus.pdf
Luettu: 30.10.2021.

Lindberg, H., 2020. RSA:n kryptoanalyysi.
Luettavissa: https://tivia.fi/2020/06/15/rsan-kryptoanalyysi/
Luettu 30.10.2020.

Linden, M., 2015. Identiteetin- ja pääsynhallinta. Tampereen teknillinen yliopisto. Tietotekniikan laitos. Luettavissa: https://trepo.tuni.fi/bitstream/handle/10024/116698/linden_identiteetin_ja_paasynhallinta.pdf?sequence=1&isAllowed=y. Luettu 9.9.2021.

Linden, M.,2012, Identiteetin- ja pääsynhallinta. Luentomoniste.
Luettavissa: https://docplayer.fi/1405611-Identiteetin-ja-paasynhallinta.html.
Luettu 14.10.2021.

Livinus, O., 2017, Using the CIA and AAA Models to explain Cybersecurity Activities.
PM World Journal. Luettavissa: https://www.researchgate.net/publication/334029877_Using_the_CIA_and_AAA_Models_to_explain_Cybersecurity_Activities.
Luettu 13.10.2021.

Lord, N. 2020. Uncovering Password Habits: Are Users' Password Security Habits Improving?
Luettavissa: https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic.
Luettu: 30.10.2021.

Lorentsen, M., 2020. Ilmainen netti voi tulla kalliiksi.
Luettavissa: https://kotimikro.fi/tietoturva/tietomurrot/ilmainen-netti-voi-tulla-kalliiksi.
Luettu 30.10.2021.

Meurman, M. 2021, Arvioi riskejä tehokkaasti - Käytä asteikkoa! Luettavissa:
https://www.arter.fi/arvioi-riskeja-tehokkaasti/.
Luettu 9.10.2021.

Michaelides, N., 2021. Remote Working and Cyber Security Literature Review. Luettavissa: https://www.researchgate.net/publication/349396561_Remote_Working_and_Cyber_Security_Literature_Review.
Luettu: 16.10.2021.

Mikrobitti, 2019. Mikä on VPN? Luettavissa: https://www.mikrobitti.fi/neuvot/mika-on-vpn/61708851-881b-435a-ab31-4164c58eaa69.
Luettu 12.11.2021.

Okereafor, K., Manny, P., 2020. Understanding Cybersecurity Challenges of Telecommuting and Video Conferencing Applications in the Covid-19 Pandemic. International Journal in IT & Engineering (IJITE), 8, 6, s. Luettavissa: https://www.researchgate.net/publication/341895001_Understanding_Cybersecurity_Challenges_of_Telecommuting_and_Video_Conferencing_Applications_in_the_COVID-19_Pandemic. Luettu 15.2.2021.

Paasonen, J. 2021. Kyberrikollisuuden kustannuksista ja seurannasta. Luettavissa: https://jyripaasonen.fi/tag/kyberhyokkays/. Luettu 12.9.2021.

Palmu, P., 2021. Vastaamo - Tietomurto, joka kaatoi koko yrityksen. Luettavissa: https://www.etevat.fi/blogi/valta-vastaamon-kohtalo
Luettu 17.10.2021

Pitkänen, M., 2021, Tietoturvallinen etätyö - mitä kaikkea se on? Luettavissa: https://yrityksille.elisa.fi/ideat/tietoturvallinen-etatyo-mita-kaikkea-se-on/.
Luettu 16.10.2021

Radha, V., Reddy, H. 2012. SciVerse ScienceDirect: A Survey on Single Sign-On Techniques. Procedia Technology 4, s.134–139.

Rasmussen, H. 2018a, Mikä on DNS-palvelin? Luettavissa: https://kotimikro.fi/internet/mika-on-dns-palvelin. Luettu 11.10.2021.

Rasmussen, H.,2018b. Mitä salaus tarkoittaa? Luettavissa: https://kotimikro.fi/tietoturva/tietosuoja/mita-salaus-tarkoittaa.
Luettu: 30.10.2020.

Rokka, H., 2021, Onko Zero Trust Network kyberturvan pelastusrengas? Luettavissa: https://www.5feetnetworks.com/2021/03/09/onko-zero-trust-network-kyberturvan-pelastus-rengas/
Luettu: 16.10.2021.

Saarola, J., Riskin arviointi työympäristössä. Luettavissa: https://www.blueplan.fi/riskin-arviointi-tyoymparistossa/.
Luettu: 11.11.2021

Shaw, K., 2020. The OSI model explained and how to easlily remember its 7 layers. Luettavissa https://www.networkworld.com/article/3239677/the-osi-model-explained-and-how-to-easily-remember-its-7-layers.html. Luettu 2.10.2021.

Siltainsuu, J. 2020. Salasanan hallintamenetelmien käyttöönoton mahdollistajat ja esteet. Pro gradu -tutkielma. Jyväskylän yliopisto, informaatioteknologian tiedekunta. Luettavissa: https://jyx.jyu.fi/bitstream/handle/123456789/70094/URN%3ANBN%3Afi%3Ajyu-202006224297.pdf?sequence=1&isAllowed=y. Luettu 9.9.2021.

Slattery, T., 2021, How and why automation can improve network-device security. Luettavissa: https://www.networkworld.com/article/3634432/how-and-why-automation-can-improve-network-device-security.html. Luettu 14.10.2021.

Soon, A. 2019. Why using a free VPN is a no good, very bad idea.
Luettavissa: https://www.hardwarezone.com.sg/blog-why-using-free-vpn-no-good-very-bad-idea. Luettu 2.10.2021.

Suomalainen, J., 2013. Älykäs tunnistautuminen ja käyttöoikeuksien hallinta monimuotoisessa verkotetussa maailmassa. Lisensiaattityö. Aalto-yliopisto, Perustieteiden korkeakoulu, Tietotekniikan laitos. Luettavissa: https://aaltodoc.aalto.fi/bitstream/handle/123456789/7691/lic_suomalainen_jani_2013.pdf?sequence=1&isAllowed=y. Luettu 9.9.2021.

Teknologiateollisuus. Tieto- ja kyberturvallisuus. Luettavissa: https://teknologiateollisuus.fi/sites/default/files/inline-files/T-Tieto-ja-kyberturvallisuus.pdf.
Luettu 11.11.2021.

Traficom.2020a. Näin pidät huolta tietoturvasta kotona ja työpaikalla. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-pidat-huolta-tietoturvasta-kotona-ja-tyopaikalla. Luettu:10.2.2021.

Traficom 2020b. Näin suojaudut tietomurroilta. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-tietomurroilta. Luettu 10.2.2021.

Traficom, 2020c. Tietoturvan vuosi 2020. Kyberturvallisuuskeskuksen vuosikatsaus. Traficomin julkaisuja 13/2021.
Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Tietoturvan-vuosi-2020_210212_FIN.pdf. Luettu 11.11.2021.

Trend Micro, 2020. Kyberturvallisuus vuonna 2021 nojaa käyttäjien koulutukseen, pilviturvaan ja uhkien laajennettuun havainta- ja vastauskykyyn.
Luettavissa: https://www.mynewsdesk.com/fi/trend-micro-finland/pressreleases/kyberturvallisuus-vuonna-2021-nojaa-kaeyttaejien-koulutukseen-pilviturvaan-ja-uhkien-laajennettuun-havainta-ja-vastauskykyyn-3057153
Luettu 15.10.2021

Tulevaisuusvaliokunta 2020. Koronapandemian hyvät ja huonot seuraukset lyhyellä ja pitkällä aikavälillä. Eduskunnan tulevaisuusvaliokunnan julkaisu 1/2020.
Luettavissa: https://www.eduskunta.fi/FI/naineduskuntatoimii/julkaisut/Documents/tuvj_1+2020.pdf. Luettu 11.11.2021

Työsuojelu, 2020. Työsuojeluhallinnon verkkopalvelu. Etätyö. Luettavissa: https://www.tyosuojelu.fi/tyoolot/tyoymparisto/etatyo. Luettu 11.3.2021.

Tietosuojavaltuutetun toimisto. Tietosuoja turvaa oikeutesi henkilötietoja käsiteltäessä.
Luettavissa: https://tietosuoja.fi/tietosuoja. Luettu 11.3.2021

Uitti, J. 2021. Merkittävimmät tietoturvauhat ratkaistaan koulutuksella. Luettavissa: https://www.etevat.fi/blogi/merkittavimmat-tietoturvauhat-ratkaistaan-koulutuksella.
Luettu 17.10.2021

Valonen, T., 2020. Miten hallitset etätyön kyberriskejä?
Luettavissa: https://www.ey.com/fi_fi/cybersecurity/miten-hallitset-etaetyoen-kyberriskejae-. Luettu 13.9.2021.

Valtiovarainministeriön julkaisuja 2010a. Sosiaalisen median tietoturvaohje. 4/2010. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä. Luettavissa: https://www.suomidigi.fi/sites/default/files/2020-06/Ohje_4_2010_etusivu_ohjepdf.pdf. Luettu 21.3.2021.

Valtiovarainministeriön julkaisuja 2017b. Tietoturvapoikkeamatilanteiden hallinta. 8/2017. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä. Luettavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79258/VM_8_2017.pdf?sequence=6&isAllowed=y. Luettu 10.2.2021.

Valvira, 2020. Potilastietojen ja henkilötietojen käsittely.
Luettavissa: https://www.valvira.fi/terveydenhuolto/hyva-ammatinharjoittaminen/salassapito/potilastietojen_kasittely.
Luettu 11.11.2021.

Vesajoki, K., 2018. Kun tietoturvaresurssit ovat rajalliset, keskitä ne tähän. Tivi.
Luettavissa: https://www.tivi.fi/kumppaniblogit/optimesys/kun-tietoturvaresurssit-ovat-rajalliset-keskita-ne-tahan/793118c6-4e7e-3baa-80a2-a71e1165bdc6
Luettu 15.10.2021

Virkkunen, H., 2020. Kyberturvallisuuden merkitys aliarvioidaan edelleen.
Luettavissa: https://www.eppgroup.eu/fi/nain-me-sen-teemme/eu-maiden-kanssa/suomi/uutiset/virkkunen-kyberturvallisuuden-merkitysta-aliarvioidaan.
Luettu 11.11.2021

Wayne, C., Bosworth, E., 2004. Password Policy: The Good, The Bad, and The Ugly, Columbus State University. Luettavissa: https://www.researchgate.net/profile/Wayne-Summers-2/publication/234799064_Password_policy_The_good_the_bad_and_the_ugly/links/54f204310cf2f9e34eff3d50/Password-policy-The-good-the-bad-and-the-ugly.pdf. Luettu 11.9.2021.

Wesley, C., 2021. Confidentiality, integrity, and availability. Luettavissa: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA. Luettu 12.11.2021

Yle, 2017. Digitreenit: Mikä ihmeen vpn? Se suojaa nettiyhteyttäsi avoimessa verkossa. Luettavissa: https://yle.fi/aihe/artikkeli/2017/09/06/digitreenit-mika-ihmeen-vpn-se-suojaa-nettiyhteyttasi-avoimessa-verkossa. Luettu 2.10.2021.

Yli-Korhonen, J., 2020. Etätyöt ovat lisänneet datan käyttöä huomattavasti - verkkojen kapasiteetit kestäneet.
Luettavissa: https://fin.afterdawn.com/uutiset/artikkeli.cfm/2020/03/20/etatyo-koronavirus-lisannyt-datan-kayttoa.
Luettu 11.11.2021.