LAPIN AMK
Lapland University of Applied Sciences

ETÄTYÖN TIETOTURVAHAASTEET

Latvala Annika

Opinnäytetyö

Tieto- ja viestintätekniikka
Insinööri (AMK)

2021

LAPIN AMK
Lapland University of Applied Sciences

Opinnäytetyön tiivistelmä

Tieto- ja viestintätekniikka
Insinööri (AMK)

Tekijä	Annika Latvala	Vuosi	2021
Ohjaaja	Kenneth Karlsson		
Toimeksiantaja	Arctic Connect Oy		
Työn nimi	Etätyön tietoturva		
Sivumäärä	57		

Tämä opinnäytetyö käsittelee kirjallisuuskatsauksen keinoin etätyön tietoturvahaasteita. Työssä esitellään aluksi tavallisimpia tietoturvaloukkauksia. Työn rakenne noudattaa tietoturvasuunnitelman runkoa. Jokaiseen tietoturvan osa-aluetta käsittelevään osioon on kerätty etätyöhön liittyviä käytännön ja hallinnon haasteita.

Työssä annetaan ohjeita tietoturvaongelmien ratkaisemiseksi ja kyberhyökkäyksiltä suojautumiseksi. Ohjeet on suunniteltu sekä organisaation että etätyöntekijän käytettäväksi. Tietoturvaloukkausten ilmoitusmenettelyjä, henkilötietojen käsittelyä ja nollaluottamuksen periaatetta on painotettu työssä toimeksiantajan toiveesta.

Lähteinä käytetään ensisijaisesti Kyberturvallisuuskeskuksen, Valtionhallinnon tietoturvallisuuden johtoryhmän, Tietosuojavaltuutetun toimiston ja amerikkalaisen tietoturvaviranomaisen, Cybersecurity & Infrastructure Security Agencyn virallisia ohjeita. Ohjelmistoesimerkeissä on käytetty Microsoftin tuotteita.

Toimeksiantaja, videoneuvottelupalveluja tarjoava yritys, on yhtenä palveluntarjoajana mukana asiakkaidensa etätyöjärjestelyissä. Toimeksiantaja halusi kartoittaa etätyöhön liittyviä tietoturvaongelmia ja käytännön ohjeita asiakasyritysten näkökulmasta.

Lapin ammattikorkeakouluun suunnitellaan useita etätyöaiheisia opinnäytetöitä syksylle 2021. Toivon oman työni tarjoavan aiheeseen tarttumapinta-alaa ja esittelevän käytännön tietoturvaohjeistuksia julkaisevia tahoja.

Avainsanat BYOD, etätyö, kovennus, pääsynvalvonta, tietoturva

LAPIN AMK
Lapland University of Applied Sciences

Abstract of Thesis

Study Programme in Information
and Communication Technology
Bachelor of Engineering

Author Annika Latvala Year 2021
Supervisor Kenneth Karlsson
Commissioned by Arctic Connect LLC
Subject of thesis Mitigation of Operational and Technical Cyber Threats Associated with Telework
Number of pages 57

The objective of this thesis was to provide a literary review of telework related cyber security guidelines and best practices published by national cyber security officials following the Corona virus pandemic. The aim was to comprise a practical set of cyber security guidelines for organizations and workers interested in deploying telework practices. The research was commissioned by Arctic Connect, a local video conferencing tool and service provider.

This thesis was structured in the manner of a general information security contingency plan. Therefore, the scope of security practices and challenges are wide, and technical instructions are not very detailed. Three sections of the topic were highlighted as per the commissioner's instructions. These sections were reporting procedures of information security breaches, management of personally identifiable information and deployment of Zero Trust principles. Differences between device manufacturers and operating systems were not included in the study. The software section of the guidelines consists of only two examples: e-mail and video conferencing platforms.

Statistics show that passwords have become an obsolete way of verification. The use of personal devices for work raises the need for centralized device management and new code of conduct principles. Telework requires device hardening and cyber hygiene training.

Key words BYOD, Cybersecurity, Cyber Hygiene, Hardening, Telework

SISÄLLYS

1 JOHDANTO

Vuonna 2020 etätyö yleistyi räjähdysmäisesti koronapandemian vuoksi. Etätyöhön siirryttiin maailmanlaajuisesti kaikilla toimialoilla. Nopea siirtyminen laajamittaisiin etätyöjärjestelyihin aiheutti uusia tietoturvaongelmia ja tarpeen käytännön ohjeille. Vuosi pandemian jälkeen vaikuttaisi siltä, että etätyö on koettu hyödylliseksi tavaksi organisoida työn tekemistä, eikä kaikkia etätyöjärjestelyjä aiota purkaa koronaa edeltäneelle tasolle. Nyt on siis hyvä hetki pysähtyä tutkimaan etätyöryntäyksen aiheuttamia tietoturvaongelmia ja oppimaan niistä. Vuoden aikana julkaistuja tietoturva- ja toimintaohjeita on kerätty tähän työhön tietoturvasuunnitelman rakennetta noudattaen.

Aihe on laaja, joten työssä esitellyt ohjeet ja periaatteet ovat yleisluontoisia. Eri laitevalmistajien eroihin ja sovellusten yksittäisiin asetuksiin työssä ei pureuduta. Tietoaineistoturvallisuudessa ei käsitellä eri turvallisuusluokitusten mukaisia aineistoja tai erityisiin henkilötietoryhmiin kuuluvia tietoja. Ohjelmistoturvallisuuteen on valittu tarkasteltavaksi vain sähköposti- ja neuvottelualustat yleisellä tasolla. Työn tavoitteena on tarjota tietoturvaohjeita sekä etätyöntekijälle että organisaatiolle. Nollaluottamuksen periaatetta, henkilötietojen käsittelyä ja tietoturvaloukkausten ilmoituskäytäntöjä on painotettu työssä toimeksiantajan toiveesta.

2 TIETOTURVALOUKKAUKSET

2.1 Vuosikatsaus

Vuonna 2020 koronapandemian aiheuttamat kokoontumisrajoitukset pakottivat yritykset kautta maailman siirtymään laajamittaisiin etätyöjärjestelyihin nopealla aikataululla. Pandemia heijastui myös kyberrikollisuuteen. Kyberturvallisuuskeskukselle raportoidut tietoturvaloukkaukset kaksinkertaistuivat edellisvuoteen nähden. VPN-yhteyksissä ja pilvipalveluissa havaittiin selkeitä kapasiteettiongelmia. Lisäksi verkossa havaittiin selvästi aiempaa enemmän avoimia laitteita ja suojattomia etätyöpöytäyhteyksiä. (Kyberturvallisuuskeskus 2020a, 5–6, 10, 18, 34; Kyberturvallisuuskeskus 2020b.)

Huijaukset ja tietojenkalastelu muodostavat valtaosan, noin kolme neljännestä, kaikista kyberturvallisuuskeskukselle raportoiduista tapahtumista. Loput tietoturvaloukkaukset koostuvat pääosin roskapostista, haittaohjelmista ja tietomurroista. (Kyberturvallisuuskeskus 2020a, 17.) Ponemon instituutin kansainvälisen kyselytutkimuksen mukaan koronapandemian aikana yleisimpiä tietoturvaloukkauksia olivat käyttäjätunnusten varkaus, tietojenkalastelu, käyttäjätilin haltuunotto, yleiset haittaohjelmat ja palvelunestohyökkäykset. Kyselytutkimuksessa tietoturvaloukkausten koettiin selvästi lisääntyneen pandemian aikana. Myös laitemurrot ja -varkaudet, sisäpiirin hyökkäykset, nollapäivähyökkäykset ja kiristyshaittaohjelmat yleistyivät etätyön myötä. Etätyön suurimmiksi riskeiksi arvioitiin etätyöympäristöjen fyysinen turvallisuus ja langattomien laitteiden tietoturvaongelmat. (Ponemon Institute 2020, 1–3.)

2.2 Tietojenkalastelu ja huijaukset

Tietojenkalastelulla pyritään keräämään yksityisiä tunnus- tai maksutapatietoja suoraan käyttäjältä. Tunnustietoja ovat esimerkiksi käyttäjätunnus, salasana ja tilille kirjautumiseen käytettävät vaihtoiset tiedot, kuten puhelinnumero ja turvakysymyksen vastaus. Maksutapatietoja ovat esimerkiksi pankki- ja luottokorttitiedot, PayPal-tilin tiedot, kryptovaluutta-avaimet ja verkkolompakon tilitiedot ja avaimet. Tietoja pyydetään käyttäjältä yleisimmin väärennetyn kirjautumissivun avulla, jonne käyttäjä ohjataan esimerkiksi sähköpostin liitetiedoston tai teksti-

viestin avulla. Tietoja voidaan myös kysyä käyttäjältä suoraan esimerkiksi soittamalla.

Kyberturvallisuuskeskus varoittaa erityisesti postin nimissä lähetetyistä tekstiviestihuijauksista, Microsoftin teknisen tuen nimissä soitetuista huijauspuheluista ja Microsoftin Office 365 -palvelua imitoivista tietojenkalasteluyrityksistä (Kyberturvallisuuskeskus 2020a, 38–39.) Tietosuojavaltuutetulle ilmoitetaan eniten juuri Microsoft-tiliin liittyviä tietojenkalasteluyrityksiä, mutta vastaavia keinoja käytetään kaikkien pilvipalveluiden tunnusten tietojen kalasteluun (Tietosuojavaltuutetun toimisto 2021e). Kriisitilanteissa syntyy aina laajoja huijauskampanjoita, joissa terveydenhoidon tai hätäaputoimien verukkeella käyttäjiltä kerätään tietoja tai maksuja olemattomista palveluista. Vuonna 2020 huijauksissa hyödynnettiin koronan herättämää pelkoa. (Kyberturvallisuuskeskus 2020a, 28; Check Point Research 2021a, 32.)

Etätyössä etäyhteyksien, pilvipalveluiden, tiedostonjako- ja viestintäsovellusten käyttö lisääntyy, joten myös tietojenkalastelun mahdollisuudet kasvavat. Tunnusten vaarantumiseen tulee reagoida heti, sillä yhdellä pilvipalvelun käyttäjätunnuksella hakkeri saattaa pystyä murtautumaan useaan eri järjestelmään. Pelkän sähköpostin avulla voidaan levittää tietojenkalasteluyrityksiä ja haittaohjelmia, lukea salassa pidettävää yritystoimintaan tai henkilötietoihin liittyvää tietoa ja räätälöidä väärennettyjä laskuja yrityksen nimissä. (Tietosuojavaltuutetun toimisto 2021a.) Tietojenkalastelulta suojautuminen on ensiarvoisen tärkeää, sillä tietojenkalastelu on ylivoimaisesti yleisin raportoitu tietoturvapoikkeama ja tavallisin ensiaskel laajemmissa kyberhyökkäyksissä.

Tietojenkalastelulta suojaudutaan parhaiten kouluttamalla työntekijöitä tunnistamaan huijausyrityksiä, ottamalla käyttöön kaksivaiheinen tunnistus kaikille tunnuksille ja suodattamalla roskapostia. Kalasteluyritysten aiheuttamia vahinkoja pienennetään käyttäjätunnus-, salasana- ja käyttöoikeusasetuksilla, ohjelmistojen ja laitteiden suoja-asetuksilla ja tietoaineistokäytännöillä.

2.3 Haittaohjelmat

Sanastokeskuksen termipankissa haittaohjelma määritellään ohjelmaksi, joka ”tarkoituksellisesti aiheuttaa koneen käyttäjän kannalta ei-toivottuja tapahtumia

tietojärjestelmässä tai sen osassa” (Sanastokeskus TSK 2021a). Hyviä esimerkkejä erilaisista haittaohjelmista ovat troijalainen, bottiverkko, vakoilu-, kiristys- ja mainosohjelma. Levinneimmät haittaohjelmat hyödyntävät useamman haittaohjelmatyypin ominaisuuksia. Monet haittaohjelmat asentavat ensi töikseen saastuneelle laitteelle muita haittaohjelmia. Haittaohjelmat leviävät yleensä sähköpostin liitetiedostojen ja epäilyttävien verkkosivujen kautta.

Troijalainen on asialliseksi ohjelmaksi tekeytynyt haittaohjelma. Tietoturvayhtiö Check Point Software Technologiesin tutkimustoiminnasta vastaava Check Point Research julkaisee kattavia globaaleja haittaohjelmatilastoja. Maaliskuun 2021 katsauksessa kaksi maailmanlaajuisesti yleisintä haittaohjelmaa olivat Dridex ja IcedID, kaksi maksutietoja keräävää troijalaista. Nämä haittaohjelmat keräävät maksutietoja muun muassa ohjaamalla käyttäjän kloonatuille valesivustoille ja syöttämällä ohjelmakoodia saastuneen laitteen prosesseihin ja selaimeen. IcedIDin raportoidaan yleistyneen nopeasti laajan korona-aiheisen, saastuneita doc-tiedostoja jakavan roskapostikampanjan avulla. (Check Point Research 2021b.)

Myös neljänneksi yleisin haittaohjelma Check Point Researchin maaliskuun listalla, Agent Tesla, on troijalainen. Agent Tesla mahdollistaa suoran etäyhteyden saastuneeseen laitteeseen. Ohjelma kerää myös näppäinpainalluksia, lukee järjestelmän leikepöytätietoja, ottaa ruudunkaappauskuvia ja hakee valtuustietoja asennetuista sovelluksista. Se edustaa siis myös vakoiluohjelmien aatelia. **Vakoiluohjelmaksi** kutsutaan haittaohjelmia, jotka keräävät ja välittävät eteenpäin käyttäjän yksityistietoja ja toiminnoista kerättyä dataa. (Check Point Research 2021b.)

Bottiverkko on saastuneiden koneiden kokoelma, jota hakkeri voi käyttää esimerkiksi keskitettyihin hyökkäyksiin, palvelunestohyökkäyksiin, vakoiluun, haittaohjelmien levitykseen tai kryptovaluutan louhintaan. Sekä Kyberturvallisuuskeskuksen että Check Point Researchin vuosikatsauksissa Emotet-bottiverkko nimettiin vuoden 2020 yleisimmäksi haittaohjelmaksi. Emotetin levinneisyyden salaisuus oli kyky ujuttaa haittaohjelman sisältävä tiedosto tai linkki vanhan sähköpostikeskustelun jatkoksi. Emotet, kuten muutkin bottiverkot, asentavat

myös muita haittaohjelmia saastuttamilleen koneille. (Kyberturvallisuuskeskus 2020a 11,17; Check Point Research 2021a 45–46.)

Emotetin serverit suljettiin kansainvälisessä poliisioperaatiossa tammikuun loppupuolella. Emotet onkin jo hävinnyt yleisimpien haittaohjelmien listauksista (Harjumaa 2021.) Check Point Researchin maaliskuun 2021 raportissa kymmenen yleisimmän haittaohjelman listassa sijalla 5 on Qbot-niminen bottiverkko ja sijalla 6 Emotetin levittämä Trickbot. Kumpikin bottiverkko keskittyy pääasiassa maksutietojen anastamiseen. Sijalla 7 on XMRig-haittaohjelma, joka valjastaa saastuneen koneen laskentatehoa Monero-nimisen kryptovaluutan louhintaan. (Check Point Research 2021b.)

Mainosohjelma levittää käyttäjälle lukuisia mainoksia ja myy käyttäjästä keräämiään tietoja kolmansille osapuolille. Aina ero haitallisen mainosohjelman ja mainoksilla kustannetun ilmaisohjelman välillä ei ole selvä. Käyttäjä voi lisenssiehdoissa hyväksyä mainonnan ja tietojen keräämisen ohjelman käyttöä vastaan. Näennäisesti asiallinen ilmaisohjelma voi kuitenkin mainosten näyttämisen lisäksi toimia jotenkin käyttäjän kannalta epäsuotuisasti. (Sanastokeskus TSK 2021b.) Kyberturvallisuuskeskuksen maaliskuun katsauksen mukaan Suomesta lähtöisin olevan haittaohjelmaliikenteen suurin yksittäinen aiheuttaja oli Android-alustan mainosohjelma nimeltä Hummer (Kyberturvallisuuskeskus 2021a, 24). Mainosten lisäksi Hummer kerää varoja asentamalla laitteeseen sovelluksia luvatta (Forrest 2016).

Kaikkia edellä mainittuja haittaohjelmatyyppejä kohdennetaan myös älypuhelimille. Älypuhelin on tärkeässä roolissa myös tietojenkalastelussa, sillä pienellä näytöllä sisäänkirjautumissivun osoiterivi ei välttämättä ole helposti näkyvissä. Etätyön yleistyessä lisääntyy myös sähköpostin ja tiedostojen käyttö älypuhelimella. Kyberturvallisuuskeskus varoittaa maaliskuun Kybersää -katsauksessa erityisesti omaPosti-teemaisista huijaustekstiviesteistä. Viestin mukaan käyttäjälle on saapunut odottamaton paketti, ja linkkiä seuraamalla käyttäjä pääsee tarkastelemaan lähetyksen tietoja ja maksamaan puuttuvia toimituskuluja. Tekstiviestin kautta pyritään asentamaan Android-puhelimeen FakeCop-troijalainen tai FakeSpy-vakoiluohjelma ja ottamaan toistuva mobiililasku käyttöön Apple-

tilillä. Haittaohjelma lähettää liittymästä myös tuhansittain tekstiviestejä. (Kyberturvallisuuskeskus 2021a. 3, 16, 21.)

Check Point Researchin mukaan maaliskuussa 2021 maailmanlaajuisella tasolla kolme yleisintä mobiilialustojen haittaohjelmaa ovat Hiddad, xHelper ja Furball. Hiddad on pääasiassa mainosohjelma, joka paketoi oikeita sovelluksia haittaohjelmien kanssa yhteen ja julkaisee paketin luotettavassa sovelluskaupassa. xHelper asentaa muita haittaohjelmia ja näyttää mainoksia. Furball antaa etäyhteyden saastuneeseen laitteeseen ja muun muassa nauhoittaa ääntä ja kerää sijaintitietoja. (Check Point Research 2021b.)

Haittaohjelmilta suojautuminen vaatii käyttäjiltä tietoturvaosaamista haitallisten tekstiviestien, linkkien, liitetiedostojen ja epäilyttävien sovellusten tunnistamiseksi. Lisäksi kaikkien laitteiden virusturvaohjelmistojen päivitykset tulee pitää ajan tasalla. Sovelluksia ei saa ladata tuntemattomista lähteistä. Tärkeää on myös huomata, että viralliselta alustalta voi löytyä luotettavasta ohjelmasta saastunut asennusversio.

2.4 Ohjelmistohaavoittuvuudet

Kyberturvallisuuskeskuksen maaliskuun katsauksessa erilaiset laite- ja ohjelmistohaavoittuvuudet arvioitiin tärkeimmäksi pidemmän aikavälin kyberuhaksi. Haavoittuvuudella tarkoitetaan tässä yhteydessä luvattoman käytön mahdollistavaa tietoturva-aukkoa tietyssä kohdejärjestelmässä. (Kyberturvallisuuskeskus 2021a, 6–7.) Laite- ja ohjelmistohaavoittuvuuksilla pyritään yleensä kirjautumaan sisään haavoittuvaan tietojärjestelmään, ohjelmaan tai laitteeseen. Erityistä huomiota tulee kiinnittää nollapäivähaavoittuvuuksiin, joilla tarkoitetaan välittömästi käytettävissä olevia tietoturva-aukkoja. Luku 0 tarkoittaa, että ohjelman kehittäjällä ei ole yhtään päivää aikaa paikata tietoturva-aukkoa, ennen kuin se tulee julkisesti tietoon ja hyödynnettäväksi. (Sanastokeskus TSK 2021c.)

Check Point Researchin kuukausikoosteessa käytetyimpien haavoittuvuuksien listalla kahdeksan kymmenestä antaa hyökkääjälle mahdollisuuden suorittaa ohjelmakoodia uhrijärjestelmässä. Kolmanneksi käytetyin haavoittuvuus altistaa Dasan GPON-reitittimen alttiiksi autentikoinnin ohitukselle. Neljänneksi yleisin,

versionhallintatyökalu Gitistä löydetty haavoittuvuus tarjoaa hyökkääjälle mahdollisuuden kerätä palvelimelta tunnustietoja. (Check Point Research 2021a.)

Etätyön kannalta merkittävimmät tekniset haavoittuvuudet löytyvät etäyhteyksistä kuten VPN (Virtual Private Network) ja RDP (Remote Desktop Protocol). Haavoittuvuuksia on todettu useimpien valmistajien laitteissa. Etäyhteyslaitteiden ja -ohjelmien haavoittuvuuksien käyttö kasvoi räjähdysmäisesti vuoden 2020 aikana. Check Point Researchin vuosikatsauksen mukaan Citrix-tuoteperheen haavoittuvuuksien käyttö yleistyi edellisvuoteen nähden yli kaksikymmenkertaisesti ja VPN-haavoittuvuudet seitsenkertaistuivat. Myös etäyhteysohjelmistojen ja Ciscon tuoteperheen haavoittuvuuksien käyttö yleistyi merkittävästi. (Check Point Research 2021a 23–25)

Laite- ja ohjelmistohaavoittuvuuksien minimoimiseksi erityisesti virus- ja etäkäyttöohjelmat on pidettävä päivitettyinä. Virusohjelmat skannaavat tunnettuja haavoittuvuuksia automaattisesti, ja oman organisaation sisällä haavoittuvuuksia voi skannata manuaalisesti erilaisilla apuohjelmilla. Organisaatiolle olennaisia haavoittuvuuksia on mahdoton tunnistaa ilman kattavaa listaa käytössä olevista laitteista ja ohjelmistoista. Ohjelmakohtaiset suoja-asetukset tulee ottaa käyttöön, ja työntekijöitä tulee ohjeistaa sovellusten oikeaoppiseen käyttöön.

2.5 Kyberhyökkäykset ja tietomurrot

Kyberhyökkäys tarkoittaa sähköisissä tietojärjestelmissä tapahtuvaa yritystä häiritä, hallita tai varastaa kohteen tietojärjestelmää, sen fyysisiä ilmenemismuotoja tai tietoaineistoa (Computer Security Resource Centre 2021; Sanastokeskus TSK 2021d; Sanastokeskus TSK 2021e). Kohdennettu hyökkäys ei aina edellytä hyökkääjältä suoraa kiinnostusta kohdeyritykseen. Opportunistisen hakkerin uhriksi voi päätyä kuka vain, jos hyökkäys saa alkunsa laajasta ja kohdentamattomasta teknisten haavoittuvuuksien skannauksesta. Kohdennetuissa kyberhyökkäyksissä hyödynnetään lopulta tarpeen mukaan kaikkia edellä mainittuja tietoturvaloukkausten mekanismeja.

Kyberhyökkäyksen tekninen toteutus voidaan ostaa palveluna ja siinä voidaan hyödyntää kolmannen osapuolen tietojärjestelmään kohdistettua tietomurtoa tai laajaa tietojenkalastelukampanjaa. Kyberhyökkäyksiin liittyy usein pitkä tiedus-

telujakso, jonka aikana kerätään lisätietoja järjestelmästä ja sen käyttäjistä. Tietojärjestelmän sisällä liikutaan lateraalisesti huomiota herättämättä ja käyttäjiä manipuloidaan paljastamaan tietoja. (Kyberturvallisuuskeskus 2020a, 10; Brewer, 2017.)

2.6 Kiristyshyökkäykset

Kyberturvallisuuskeskus pitää kiristämiseen tähtääviä kyberhyökkäyksiä toiseksi tärkeimpänä pitkän aikavälin kyberuhista. (Kyberturvallisuuskeskus 2021b, 6). Kiristäjä voi uhata lamauttaa tiettyjä palveluja palvelunestohyökkäyksellä, jos lunnaita ei makseta. Toinen kiristystapa vaatii päätelaitteeseen asennetun haittaohjelman: kiristysohjelma kaappaa ja salaa kryptografisesti käyttäjän tietoaineiston ja vaatii maksua vastineeksi salausavaimesta. (Check Point Research 2021b.) Kolmas tapa on kerätä sosiaalisen vaikuttamisen keinoin tietoja käyttäjästä ja kohdejärjestelmästä. Viestissä voidaan väittää, että käyttäjää on kuvattu murretuilla päätelaitteilla, tai että hänestä on kerätty arkaluonteisia tietoja kuten selaimen selaushistoria. Yksilöity lunnasvaatimus lähetetään, vaikka todellista uhkaa ei olisikaan. (Kyberturvallisuuskeskus 2019a.)

Kiristysohjelmien hyväksikäyttö kyberrikoksissa yleistyi koronapandemian aikana. Valitettavan usein kohteena olivat terveydenhoitoalan yritykset ja varastettuna aineistona tavallisten ihmisten terveystiedot. Vuoden 2021 alkupuoliskolla sama suuntaus jatkuu (Check Point Research 2021a 19–21; Check Point Research 2021b.)

Suomessa mieleenpainuvin esimerkki kiristyshyökkäyksestä oli vuonna 2020 psykoterapiakeskus Vastaamoon kohdistunut tietomurto, jossa tietojen julkaisemisella kiristettiin rahaa paitsi yritykseltä, myös sen yksittäisiltä asiakkailta (Kyberturvallisuuskeskus 2020a, 13). Tietojen julkaisemisella ja palvelunestohyökkäyksillä kiristäminen yleistyivät hyökkäysmenetelminä vuoden 2020 aikana (Check Point Research 2021a 17–19). Koska Vastaamon kaltaisissa tietomurroissa tietojärjestelmää tutkitaan pitkään ennen lopullista kontaktia, tulisi epäilyyn tunnustietojen vaarantumisesta reagoida heti. Kyberturvallisuuskeskus kehottaa suojautumaan kyberhyökkäyksiltä vähentämällä hyökkääjälle tarjolla olevia keinoja tunkeutua järjestelmiin. Turhat palvelut tulee poistaa verkosta ja

välttämättömät suojata ja piilottaa näkyvistä. (Kyberturvallisuuskeskus 2020a 10–11.) Kiristyshyökkäyksen vahinkoja voi pienentää pitämällä yhden varmuuskopion verkkoyhteyksien ulottumattomissa.

Vuonna 2020 yli kymmenen tuhannen kyberturvallisuuskeskukselle raportoidun tietoturvaloukkauksen joukosta vain 153:ssa hyödynnettiin teknistä haavoittuvuutta ja 124:ssä palvelunestohyökkäystä (Kyberturvallisuuskeskus 2020a, 17). Tilasto tukee vanhaa näkemystä, jonka mukaan valtaosa tietoturvaongelmista liittyy käyttäjän toimiin ja vain murto-osa teknisiin tietoturva-aukkoihin.

3 HALLINNOLLINEN TURVALLISUUS

3.1 Tietoturvan kehittäminen ja johtaminen etätyössä

Kyberturvallisuuskeskus ennakoi raportoitujen tietoturvaloukkausten perusteella riskikartoituksen ja vastuunjaon haasteet neljänneksi merkittävämmäksi pidemmän välin kyberuhaksi. Kyberriskien vaikutusta on vaikeaa ennakoida ja vastuukysymykset hämärtyvät, kun palveluun liittyy useampi toimittaja. (Kyberturvallisuuskeskus 2021a 6.)

Tietoturva kokonaisuutena ja etätyöhön liittyvien tietoturvariskien hallitseminen on yrityksen vastuulla. Tietoturvan hallintaa ei voi palveluna kokonaan ulkoistaa, sillä vastuu tietoturvan tavoitteiden toteutumisesta on yrityksellä. Palveluntarjoajilta, yhteistyötahoilta ja kolmansilta osapuolilta täytyy vaatia samaa tietoturvan tasoa, jota yrityksen omissa järjestelmissä noudatetaan. Tietoturvavaatimukset kannattaakin kirjata ylös ja varautua jo ennalta tilanteeseen, jossa kumppanin tietoturvaratkaisut pettävät. (Kyberturvallisuuskeskus 2020c 8, 28–29, 33.)

Etätyö tulisi huomioida erikseen tietoturvasuunnitelmassa, sillä tietoturvan eri osa-alueet muuttuvat etätyössä huomattavasti. Varsinkin fyysinen turvallisuus laskee merkittävästi, kun työn tekeminen siirtyy työpaikan ulkopuolelle. Tietoturvan heikkeneminen yhdellä osa-alueella korvataan tehostamalla toimia muilla osa-alueilla. Etätyöhön liittyy erityisiä tietoturvariskejä, joten myös erillinen riskianalyysi on tarpeen. (Vahti 2002, 9–11.)

Koronapandemian aiheuttaman etätyöryntäyksen kaltaisessa tilanteessa tietoturvapolitiikan ja yrityskulttuurin merkitys korostuu, sillä yksityiskohtaisia tietoturvaohjeita ei välttämättä ehditä laatia ennen etätyön aloittamista. Yrityksen hallituksen vastuuta käsittelevässä kyberturvallisuusohjeessa listataan yleisluontoisesti toimia, joilla mahdollistetaan tietoturvan hallitseminen kokonaisuutena myös muuttuvissa tilanteissa. (Kyberturvallisuuskeskus 2020c, 10.)

Vastuu kyberturvallisuudesta tulee ohjata nimetylle henkilölle. Tietoturvapoikkeamien raportointiketjun tulee olla virtaviivainen ja yleisesti tunnettu. Työntekijöiden sitouttaminen tietoturvan tavoitteisiin ja johdon esimerkillinen toiminta ohjaavat etätyöntekijää toimimaan kentällä itsenäisesti tietoturvallisia periaattei-

ta noudattaen. Jotta tietoturvaohjeistus vastaisi käytännön tarpeita, täytyy työntekijöitä kannustaa antamaan rakentavaa palautetta. Työntekijöiden kokemukset otetaan myös aidosti huomioon toimintamalleja ja turvallisuuskäytäntöjä muokatessa, sillä työntekoa merkittävästi häiritseviä tietoturvaohjeita opitaan nopeasti kiertämään. (Kyberturvallisuuskeskus 2020c, 23–25, 29.)

3.2 Tietoturvaloukkausten ilmoittaminen

3.2.1 Tietoturvaloukkauksen tunnistaminen

Etätyöohjeissa varmistetaan, että työntekijä tuntee organisaation sisäisen ilmoitusketjun kaikissa tietoturvan poikkeamatilanteissa. Poikkeaman havainnoinnin jälkeen tapahtuva ongelman laadun määritteleminen voi viedä aikaa. Etätyössä työntekijällä on vähemmän mahdollisuuksia sisällöltään vapaamuotoisiin pikapalavereihin tietoturvavastaavan tai esimiehen kanssa, jolloin kynnys epäselvien tapauksien puheeksi ottamiselle kasvaa. Tietoturvapolitiikkaan hyvin sitoutettu työntekijä tuntee ilmoituskäytäntöjen taustalla vaikuttavat lait ja velvoitteet, ja osaa soveltaa niitä. (Vahti 2002, 11, 21.)

Raportointia vaativan tietoturvaloukkauksen tunnistaminen voi vaatia ohjeistusta. Ilmoituskäytäntö hämärtyy helposti varsinkin laajoissa häiriötilanteissa. On myös hyvä määritellä etukäteen, millainen tietoturvaloukkaus ylittää ilmoituskynnyksen tietoturvavastaavalle ja omalle yritysjohdolle. Samalla voi pohtia, missä vaiheessa tietoturvaloukkauksesta tiedotetaan eri tahoja, kuten sidosryhmiä ja palvelun alihankkijoita. (Kyberturvallisuuskeskus 2020c, 18–19, 36–37.)

Yleisesti raportoituja tietoturvaloukkauksia ovat esimerkiksi järjestelmän luvaton käyttö, laitteen katoaminen tai varkaus, palvelunestohyökkäys ja haittaohjelmahavainto. Yrityksen kannattaa pyytää työntekijöitä raportoimaan sisäisesti myös huijaus- ja tietojenkalasteluviesteistä. (Vahti 2017 42–47.)

3.2.2 Ilmoitukset Kyberturvallisuuskeskukselle

Yrityksen sisäisen ketjun jälkeen ensimmäinen raportointitaho on yleensä Kyberturvallisuuskeskus. Kybertuvallisuuskeskus auttaa tietoturvaloukkausten sel-

vittämisessä ja arvioinnissa sekä viestinnässä muiden ilmoitustahojen kanssa. Kyberturvallisuuskeskus tekee yhteistyötä ulkomaisten tietoturvatahojen kanssa ja voi tätä kautta välittää yritykselle toimintaohjeita tietoturvaongelmissa, jotka ovat jo muualla maailmalla tunnettuja. Vapaaehtoiset ilmoitukset auttavat virastoa muodostamaan kyberuhkista ajantasaisen kokonaiskuvan. Virasto myös ohjeistaa kuluttajia ja organisaatioita ehkäisemään ja toipumaan tunnetuista tietoturvaongelmista. (Vahti 2017,17.)

Yhteiskunnan toiminnan kannalta kriittisillä aloilla toimiville yrityksille tietoturvahäiriöistä raportoiminen on pakollista Euroopan Unionin verkko- ja tietoturvadirektiivin mukaan. Digitaalisen infrastruktuurin toimitsijoiden, esimerkiksi teleyritysten, ja digitaalisten palveluiden, esimerkiksi pilvipalveluiden, toimittajat raportoivat tietoturvaloukkauksensa Kyberturvallisuuskeskukselle. (Kyberturvallisuuskeskus 2021b.)

3.2.3 Rikosilmoitukset

Tietoturvaloukkausten ilmoittaminen viranomaisille on usein vapaaehtoista. Henkilötietojen käsittelyä koskevat lait ja Euroopan Unionin verkko- ja tietoturvadirektiivi velvoittavat raportoimaan tietoturvaloukkauksista, mutta muut kyberrikokset ovat usein asianomistajarikoksia, joiden tutkinta edellyttää uhrin rangaistusvaatimusta. Näin ollen läheskään kaikkia kyberrikoksia ei ilmoiteta poliisille. Poliisi voi tutkia epäilyjä kyberrikoksista ilman uhrin suostumusta myös yleisen edun niin vaatiessa, tai kun tutkimus on osa virallisen syytteen alaista rikosta. Rikosilmoitusta harkitessa tulee huomata, että rikoksella voi olla muitakin uhreja kuin organisaatio itse. Päätös tietoturvaloukkauksen raportoimisesta syntyy usein vasta pitkän ajan kuluttua alkuperäisen poikkeaman havaitsemisesta. Poikkeamat tulisi aina dokumentoida mahdollista myöhempää rikosilmoitusta tukevalla tavalla. (Opetus- ja kulttuuriministeriö, Poliisiammattikorkeakoulu & JYVSECTEC 2021, 8–9,16, 29.)

Siinä missä kyberhyökkäys on lähinnä kätevä kattotermi tahalliselle tietoturvaloukkaukselle, on tietomurrolla tarkempi määritelmä. Rikoslaissa se määritellään rangaistavaksi teoksi myös epäonnistuessaan ja silloin, kun tietoja ei hyödynnetä mihinkään. (Kyberturvallisuuskeskus 2020d.) Työntekijän tulisi tunnis-

taa kirjautumistietojen vaarantumisen vakavuus ja ymmärtää, että yrityksen resursseja käsitellään aina vain asiallisten, henkilökohtaisten tunnusten avulla.

Rikoslain luvussa 38 tieto- ja viestintärikokset jaotellaan tietomurron ohella tietosuojarikokseen, luvattomaan käyttöön, datavahingontekoon, vaaran aiheuttamiseen tietojenkäsittelylle, tietoliikenteen häirintään ja tietoliikenteen häirinnässä aiheutettuun haittaan tai vahinkoon, viestintäsalaisuuden loukkaukseen ja identiteettivarkauteen (Rikoslaki 39/1889 38: 3 – 9a §). Poliisi nimittää näitä suoraan tietojärjestelmiin kohdistuvia rikoksia tietoverkkosidonnaisiksi rikoksiksi. Tietoverkkoavusteisissa rikoksissa kyberhyökkäys on tekninen osa toista rikosta, esimerkiksi petosta, kiristystä tai yritysvakoilua. (Poliisi 2021.) Kyberrikoksen ilmoittaminen poliisille auttaa laajempien rikosten selvittelyä varsinkin tilanteissa, joissa rikosta on valmisteltu kuukausia tai jopa vuosia ja rikos koskee useita uhreja. (Poliisi 2021.)

Rikosilmoituksen tekemisen yhteydessä poliisi ohjeistaa jatkotoimista ja todistusaineiston keräämisestä tapauskohtaisesti. Vaarana on, että kyberrikoksen jäljet ehtivät kadota, mikäli rikosilmoitusta ei tehdä ja oikeaa todistusaineistoa kerätä jo hyvissä ajoin. Rikosilmoitusta varten kerätään kaikki tapahtumaan liittyvä saatavissa oleva tieto. Tärkeitä tietoja ovat ainakin hyökkäyksen senhetkinen tila sekä vahinkojen laajuus ja ulottuminen yrityksen ulkopuolelle. Poliisi on kiinnostunut lokitiedoista, tapahtuman selvittämiseksi tehdyistä toimenpiteistä, tietojärjestelmien omistajista ja sisäisistä riippuvuuksista. Yrityksen sisäisen epäillyn osuus rikokseen ja mahdollisuus vaikuttaa todistusaineistoon määritellään ensi tilassa. Tärkeää onkin, että todistusaineisto säilytetään muuttamattomassa tilassa ensihavainnosta asti, ja että rikokseen liittyvien tietojen eheys ja luottamuksellisuus voidaan todentaa lokitiedoin. (Opetus- ja kulttuuriministeriö 2021, 8, 32–34.)

3.2.4 Tietosuojaloukkaukset

Henkilötietojen kanssa työskentelevien tahojen on erityisen tärkeää tuntea tietosuojaloukkauksen määritelmä ja ilmoituskäytäntö. Henkilötietoja koskevan tietoturvaloukkauksen eli tietosuojaloukkauksen käsittely on määritelty lakitekstien avulla tarkemmin kuin muut kyberrikokset. Rikoslaissa tietosuojaloukkaus

tarkoittaa henkilötietojen luvatonta hankkimista, luovutusta tai siirtämistä. Tietosuojaloukkausta käsitellään tarkemmin Euroopan parlamentin ja neuvoston yleisessä tietosuoja-asetuksessa, tietosuojalaissa ja laissa henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä. (Rikoslaki 39/1889 38: 9 §).

Muista kyberrikoksista poiketen tietosuojaloukkausten dokumentointi ja tietyin ehdoin ilmoittaminen on pakollista. Tietoturvaloukkauksen aiheuttama haitta määrittelee, täytyykö tilanteesta ilmoittaa viranomaistaholle ja tietojen kohteelle. Mikäli tietoturvaloukkauksesta voi aiheutua riski rekisteröidyn yksityisyydelle tai muille oikeuksille ja vapauksille, tulee tapahtumasta tehdä ilmoitus viralliselle valvontaviranomaiselle, Suomessa tietosuojavaltuutetun toimistolle, 72 tunnin kuluessa loukkauksen havaitsemisesta. Ilmoituskäytännön ja yrityksen sisäisen toimintaketjun tulee olla työntekijöiden tiedossa ja hyvin dokumentoitu, sillä tietosuojaloukkauksen tapahtuessa ei ole aikaa selvitellä toimintakäytäntöjä. (Tietosuojavaltuutetun toimisto 2021a; Tietosuojavaltuutetun toimisto 2021.)

Rekisteröidylle henkilölle ilmoitus tietosuojaloukkauksesta tehdään korkean riskin tapauksissa. Tietoturvaloukkauksen riskin suuruus arvioidaan kuuden tekijän avulla. Ensimmäinen on loukkauksen tyyppi, jonka avulla arvioidaan todennäköisyyttä, että tietoturvaloukkaus johtaa tietojen hyväksikäyttöön. Toisena tekijänä arvioidaan henkilötietojen arkaluonteisuutta ja määrää. Rekisteröidyn tunnistamisen helppous, rekisteröidyn haavoittuvuus, rekisterinpitäjän ominaisuudet ja tietovuodon seurauksien vakavuus vaikuttavat myös riskiarvioon. Mikäli rekisteröidylle ilmoitetaan tietosuojaloukkauksesta, tulee ilmoituksesta käydä ilmi mitä on tapahtunut, tietosuojavastaavan tai muun lisätietoja tarjoavan tahon yhteystiedot, tapahtuman todennäköiset seuraukset, toimenpiteet, joihin rekisterinpitäjä on ryhtynyt ja mahdolliset toimintaohjeet rekisteröidylle. (Tietosuojavaltuutetun toimisto 2021a.)

4 KÄYTTÖTURVALLISUUS

4.1 Nollaluottamuksen periaate

Perinteiset tietoturva-arkkitehtuurit luottavat fyysiseen turvallisuuteen. Yrityksen palomuurin sisällä tietojärjestelmät ovat turvassa, joten riittää, että pääsyä sisäverkkoon valvotaan ja käyttäjiä vaaditaan kirjautumaan palveluihin käyttäjätunnuksella ja salasanalla. Palveluiden siirtyminen pilvipalvelimille, työntekijöiden siirtyminen etätyöhön ja laitteiden henkilökohtaisen käytön lisääntyminen vaatii tietoturvan tehostusta, jota ohjaa hyvin nollaluottamuksen periaate. Nollaluottamuksen periaatteita hyödyntävä yritys ei luota enää automaattisesti käyttäjän

- tunnukseen, joka voi olla murrettu tietojenkalastelulla,
- laitteeseen, joka voi olla myös kotikäytössä, tai
- verkkoon, joka voi olla esimerkiksi kahvilan avoin Wi-Fi täynnä väliintulohyökkääjiä.

Nollaluottamuksen periaatteena on varmentaa tietojärjestelmän käyttö olettamuksella, että jokaisessa prosessin osassa voi piillä luvaton tunkeutuja. Luottamusta ei periytetä järjestelmästä toiseen. (Borchert, Connelly, Mitchell & Rose 2020, 8.)

Tietoturvahaavoittuvuuksien kirjoa selatessa huomaa äkkiä, että luvaton tunkeilija voi todella piillä prosessin joka osassa. Pelkkiä etäkoodin suorittamisen sallivia haavoittuvuuksia löytyy niin verkoista, etäyhteyksistä, salausmenetelmistä, pilvipalveluista ohjelmista kuin laitteistakin. Laitteiden omistus – ja käyttötarkoitusten muuttuminen kasvattaa entisestään yrityksen toimintaan mahdollisesti vaikuttavien teknisten haavoittuvuuksien kirjoa. Työntekijän työtarkoitukseen käyttämällä koneella ja puhelimella voi olla yrityksen käyttöön listattujen ohjelmien lisäksi lukematon määrä haavoittuvia ohjelmia. Pelkkiä haavoittuvuuksia paikkaamalla ei tietoturvaa pidetä hyökkääjän toimien tasalla.

Nollaluottamukseen pohjautuvat, käyttöturvallisuutta parantavat yleishyödylliset keinot voidaan jakaa karkeasti vahvaan käyttäjien ja laitteiden tunnistamiseen, käyttöoikeuksien vähentämiseen, vahinkojen rajaamiseen ja valvontaan (Borchert ym. 2020 6–7). Luvut 4.2–4.5 esittelevät hyödyllisiä tietoturvallisia käytän-

töjä löyhästi nollaluottamukseen perustuen. Nollaluottamukseen perustuva tietojärjestelmäarkkitehtuuri, jonka noudattaminen vaatii rakennesuunnittelua, on esitelty lyhyesti luvussa 8.1.3.

4.2 Vahva laitteiden ja käyttäjien tunnistaminen

Nollaluottamuksen periaatteisiin kuuluu kaikkien tietolähteiden, palvelujen ja laitteiden mieltäminen resursseiksi, joihin myönnetään käyttötarpeen rajoittama pääsy vain istunnon ajaksi. Kaikki viestintä salataan ja yhteydenmuodostuspyynnöt autentikoidaan huolimatta siitä, onko laite sisäverkossa vai palomuurin takana. Valtuutuksessa otetaan erikseen huomioon käyttäjän ja laitteen oikeudet ja suositaan monivaiheista tunnistautumista. (Borchert ym. 2020, 6–7.) Monivaiheisessa tunnistautumisessa käyttäjältä pyydetään vähintään kaksi erityyppistä tunnistustietoa. Eri tyypit edustavat jotain,

- minkä vain käyttäjä *tietää*, kuten salasana
- jotain, jonka vain käyttäjä *omistaa*, kuten puhelinliittymään lähetetty muuttuva koodi tai kannettava USB-laite
- ja jotain käyttäjän *ominaisuutta*, kuten kasvot, iiris tai sormenjälki. (Kyberturvallisuuskeskus 2020e.)

Monivaiheista tunnistautumista suositellaan vahvasti erityisesti pilvipalveluihin, joissa samalla tunnuksella pääsee käsiksi esimerkiksi sähköpostitiliin ja pilvitallennuspalveluun. Mikäli tunnus on suojattu vain salasanalla, voi salasanan murtanut hakkeri rekisteröidä oman puhelinnumeronsa tai muun tiedon tunnukselle, jolloin tilin palauttaminen vaikeutuu entisestään. Pilvipalveluiden toimittajat tarjoavat usein muitakin kirjautumisen hallintamenetelmiä. (Kyberturvallisuuskeskus 2020f, 10.)

Microsoftin moderneihin tunnustamismenetelmiin kuuluu monimenetelmäisen tunnistautumisen lisäksi avoimien, kolmannen osapuolen tarjoamien sähköisten varmenteiden integrointi sekä ehdolliset käyttöoikeudet. Ehdollisten käyttöoikeuksien avulla resurssien käyttö voidaan rajata tunnuksen, laitteen, sijainnin tai autentikointimenetelmän mukaan. (Kyberturvallisuuskeskus 2020f, 10.)

Resurssikohtainen autentikointi voi muodostaa työntekoa häiritseviä katkoksia, ja palvelukohtaisista salasanoista kertyy helposti hallitsematon kirjasto. Käyttäjätunnusten ja -oikeuksien hallintaan tarvitaan siksi yritysmaailmassa usein identiteettien hallintaohjelmisto, kuten Microsoftin Azure Active Directory. Identiteettien hallintaohjelmistot ohjaavat tunnistusmenetelmien kehitystä pois salasanoista ja kohti dynaamista, taustalla tapahtuvaa jatkuvaa käyttäjän todentamista. (Microsoft 2016, 1.)

Microsoftin tuoteperheessä salasanattomia tunnistustapoja ovat biometrisiä tunnisteita käyttävä Windows Hello, mobiililaitteen tunnistautumisohjelma ja FIDO2 salausavain. Identiteetinhallintaohjelmistot tarjoavat muitakin työkaluja tunnistamiseen ja käytön valtuuttamiseen. Käyttöoikeuksia voidaan muokata hallintapaneelin avulla oikea-aikaisesti. Käyttöoikeuspyyntöjen analysointi ja tallentaminen mahdollistavat vaarantuneiden tunnusten nopean tunnistamisen ja turvallisuuskäytäntöjen kehittämisen koneoppimisen avulla. (Microsoft 2016, 2; Microsoft Docs 2021a.)

4.3 Käyttöoikeuksien rajaaminen

Minimikäyttöoikeuksien periaate (Principle of Least Privileges) on hyvä lähtökohta käyttöoikeuksien hallintaan. Jokaiselle käyttäjälle ja ohjelmalle annetaan vain niin paljon käyttöoikeuksia, kuin on välttämätöntä työn tekemiseksi. Tavoitteena on vähentää inhimillisten virheiden ja haittaohjelmien aiheuttamia vahinkoja. Käyttöoikeuksien rajoitus vähentää myös palveluiden näkyvyyttä verkossa ja sitä kautta kyberrikollisen hyödynnettävissä olevaa hyökkäyspinta-alaa. (Katakri 2020, 69; Beyondtrust 2020b, 5.)

On järkevämpää pyytää sovelluksen asennusoikeutta tapauskohtaisesti kuin antaa haittaohjelmien pyöriä pääoikeuksilla ja asentua taustalla huomaamatta. Käyttöoikeus tulisi myöntää resurssikohtaisesti käyttötarpeen mukaan istunto kerrallaan. (Borchert ym. 2020, 7.) BeyondTrust, käyttöoikeuksien hallintatyökaluja kehittävä markkinajohtaja arvioi vuoden 2020 vuosiraportissaan, että yli puolet vuoden 2020 kriittisistä haavoittuvuuksista Microsoftin kaikissa tuoteperheissä olisi voitu hallita pääkäyttäjän oikeuksia rajoittamalla (BeyondTrust 2020a, 6).

Luotettujen sovellusten kerääminen valkoiselle listalle tehostaa työskentelyä minimikäyttöoikeuksilla. Hyödyllisille sovelluksille myönnetään tarvittavat käyttöoikeudet automaattisesti. Mahdollisen nollapäivähaavoittuvuuden löydyttyä haavoittuva ohjelman versio voidaan poistaa luotettujen sovellusten listalta. Valkoisen listan ulkopuolisille ohjelmille käyttäjä voi anoa käyttöoikeutta. Pyynnöt jäävät muistiin, ja mikäli tiettyyn sovellukseen tulee pyyntöjä toistuvasti, voidaan se lisätä valkoiselle listalle. Valkoisen listan rinnalla voidaan käyttää myös kiellettyjen sovellusten listaa. (BeyondTrust 2020a, 17, 22; BeyondTrust 2020b, 6,12.)

Päätelaitteiden käytön valvontaan on tarjolla BeyondTrustin kaltaisia pilvipalveluja, joiden avulla käyttöoikeuksia hallitaan dynaamisesti. Palveluja kutsutaan liikkuvuuden hallinnaksi (Enterprise Mobility Management, EMM). Liikkuvuuden hallinnassa otetaan huomioon käyttäjän ja laitteen ominaisuuksien lisäksi sijainti verkossa, maantieteellinen sijainti, pyynnön ajankohta, asennetut valtuustiedot ja poikkeamat tavallisesta käytöstä. Tietylle resurssille voidaan antaa ajallisesti rajattu käyttöoikeus esimerkiksi projektin keston vuoksi. Valtuuksia pyritään myöntämään oikea-aikaisesti juuri tarvitun tehtävän suorittamisen ajalle. Vaikka käyttäjällä olisikin valtuudet tiettyyn ohjelmaan, täytyy hänen aktivoida käyttöoikeus työtehtävän ajaksi. Oikeuksien aikarajoituksilla rajataan hyökkääjälle otollinen aikaikkuna mahdollisimman pieneksi. Samalla voidaan seurata, tarvitsevatko kaikki käyttäjätilit kaikkia niille määriteltyjä käyttöoikeuksia. Turhat oikeudet voidaan poistaa, jolloin hyökkäyspinta-ala pienenee lisää. (BeyondTrust 2020, 6–8.)

4.4 Vahinkojen rajaaminen osastoihin

Resurssien ja verkkojen jakaminen osioihin käyttötarpeiden ja yrityksen fyysisten osastojen mukaisesti vähentää olennaisesti tietomurron vaikutuksia. Hyökkääjä pyrkii yleensä keräämään tietoja kaikista nähtävillä olevista resursseista liikkumalla lateraalisesti järjestelmän sisällä. Tarkasti segmentoidussa verkossa vahingot rajoittuvat murrettuun osastoon. Dynaamiset pääsynvalvontapäätökset tehdään loogisesti erillisessä yksikössä, johon portinvartijana toimiva laite ottaa yhteyttä. Laite voi olla esimerkiksi yksittäistä resurssia vartioiva reititin.

Valtuutuspyyntö voi tulla myös suoraan yrityskoneelta asiakasohjelmaan upotetun agentin avulla. (Borchert ym. 2020, 9–11.)

Tietojärjestelmien rakenteet vaihtelevat yrityksestä toiseen, joten verkon segmentointitapakin on yksilöllinen. Ohjelmatason agentit soveltuvat hyvin käyttöön yrityksissä, joissa pääsy resursseihin halutaan rajata vain yrityksen omille laitteille. Resurssien ryhmittely yksityisiin pilviryppäisiin, joita verkkolaite vartioi, sopii perinteisesti suunnitelluille palvelinkeskuksille, joissa ei joko voida reitittää liikennettä palvelun eri osien välillä, tai käytetään vanhoja ohjelmia, jotka eivät taivu ulkoiseen valtuutukseen. On myös mahdollista valtuuttaa jokainen resurssi erikseen, mutta jättää verkkorakenne jakamatta. Kun jokaiselle käyttäjälle annetaan pääsy kokonaisverkkoon, riski hyökkääjän tiedusteluille ja palvelunestohyökkäyksille kasvaa. (Borchert ym. 2020, 12–15.)

4.5 Jatkuva valvonta, analytiikka ja lokitiedot

Ehdolliset käyttöoikeudet ja dynaaminen pääsynvalvonta vaativat aktiivista tietojen keräämistä koko järjestelmän toiminnasta. Erityisesti laitteiden ja ohjelmien tietoturvan tilaa tulee seurata. Päivityshistoria, julkiset haavoittuvuusraportit ja -verkon haavoittuvuusskannaukset antavat tietoa laitteiden tilasta. Kerätystä datasta tunnistetaan resurssien normaali käyttö. Kun käyttäjä ottaa yhteyttä uudella laitteella tai uudesta sijainnista, vaaditaan uusi tunnistussykli. Valtuutusanalyysin tulokset voivat olla erilaiset eri tilanteissa. Verkkoliikennettä ja valtuutuspyyntöjä seurataan ja analysoidaan. Tietomurrot pyritään tunnistamaan mahdollisimman aikaisessa vaiheessa. Analysoitujen tietojen pohjalta tehdään muutoksia valtuutusmenettelyihin. (Borchert ym. 2020, 20–21; Ping Identity 2021, 3–6.)

Lokitietojen puutteellisuus on merkittävä tietoturvaongelma. Tietomurtojen ja teknisten käyttöongelmien laajuus voidaan usein selvittää vain lokitietoja tarkkaan tutkimalla. Lokitietojen säilyttäminen riittävän pitkältä ajalta on tarpeen, jotta tapahtumia voidaan selvitellä jälkikäteen. Kyberturvallisuuskeskus kehottaa säilyttämään tietoturvaloukkaukseen liittyviä lokitietoja vähintään vuoden ajan. (Kyberturvallisuuskeskus 2020b, 11.) Käytännössä lokitietojen säilytysaika mietitään käsiteltävän aineiston mukaan.

Henkilötietorekistereihin liittyvät lokitiedot tulee säilyttää niin kauan, kun rekisteröity voi vielä nostaa tutkintapyyntöjä niiden käsittelyyn liittyen. Mikäli lokitiedot todistavat virallisen asiakirjallisen tiedon luottamuksellisuutta ja eheyttä, tulee ne säilyttää ja arkistoida kohteen mukana. Lokitiedot voivat sisältää henkilötietoja, esimerkiksi IP-osoitteen, jolloin lokitietojen käsittelyä koskevat samat säännöt kuin muitakin henkilötietorekistereitä. (Vahti 2009, 58–60.)

Koska lokitietoja käytetään tietojärjestelmän ja sen tietojen luottamuksellisuuden, eheyden ja käytettävyyden varmistamiseen, tulee niitä suojella käyttöoikeuksin ja murtohälytyksin. Keskitetty lokitietojen hallinta ja jatkuva-aikainen tallennus vaikeuttaa lokitietoihin kajoamista murron yhteydessä. Erityisesti yrityksen sisäisen hyökkääjän mahdollisuus kajota lokitietoihin tulee estää. Lokitietoja käsittelevällä taholla ei saa olla eturistiriitaa tai ylläpito-oikeuksia kohteena olevaan järjestelmään. Lokitiedot ovat tietoturvan aseena sitä arvokkaammat, mitä nopeampi on vaste järjestelmässä havaittavissa olevaan häiriöön. Häiriöön puuttumisen prosessit täytyy organisoida etukäteen ja päivittää tarvittaessa. (Vahti 2009, 38, 46–47.)

5 HENKILÖSTÖTURVALLISUUS

5.1 Vastuut

Työnantajan tehtävä on ottaa käyttöön tietoturvaa parantavat tekniset työkalut, ohjeistaa työntekijöitä käytännön tasolla ja valvoa tietoturvan toteutumista. Työntekijän ei voi odottaa itse suunnittelevan sopivia tietoturvakäytäntöjä etätyössä. (Helle 2004, 191–194.) Tiedotusketjujen ja keskustelukanavien tulee olla hyvin mietittynä ja tiedotettuna etätyöhön siirryttäessä. Etätyössä keskustelu kollegoiden kanssa nimittäin typistyy helposti kiireisiin tiimipalavereihin. (Vahti 2002, 11, 20.)

Työntekijän tulee etätyössä noudattaa annettuja ohjeita ja kehittää tietoturvaosaamistaan. Etätyössä raja työn ja vapaa-ajan tietoturvan välillä hämärtyy, jolloin tietoturvallisten toimintatapojen merkitys korostuu. Kyberhygienian voisi ajatella kuuluvan jo yleissivistykseen samalla tavalla kuin käsien pesun ja hengitysmaskien käytön. Nopean sovelluskehityksen ja laajan työkaluvalikoiman vuoksi etätyöntekijän tietoturvaohjeet eivät tule koskaan kattamaan kaikkia mahdollisia käyttötilanteita tai yksityiselämän tietoturvahaasteita. Etätyöntekijän tulee ymmärtää, että etätyössä vastuu tietoturvan toteutumisesta kasvaa ja ohjelmien käyttöoikeudet ja käyttäjien valvonta voi olla toisenlaista kuin työnantajan tiloissa toimiessa. (Vahti 2002, 11–12.)

5.2 Toimenpiteet etätyöhön siirryttäessä

Valtionhallinnon tietoturvallisuuden johtoryhmä on luonut valtion yksiköitä varten etätyön tietoturvallisuusohjeen. Työssä esitellyt yleisluontoiset toimenpideohjeet noudattavat pääasiassa tätä Vahdin alkuperäisohjetta vuodelta 2002. Ohje on jo 19 vuotta vanha eikä sido yksityisen sektorin toimijoita, mutta sen esittelemät periaatteet sopivat edelleen hyvin etätyön käyttöönottoon ja täydentävät vuoden 2005 etätyön puitesopimusta ja työmarkkinakeskusjärjestöjen lisäohjeita. (Vahti 2002, 3.)

Etätyön käyttöönottoa varten työtehtävien soveltuvuus etätyöhön tulee arvioida riskianalyysin mukaisesti. Henkilötietojen käsittelyyn liittyvät työtehtävät eivät

aina edes sovellu etätyöhön. Matkatyöhön voidaan liittää tiukemmat rajoitukset kuin kotona tapahtuvaan työskentelyyn. Etätyössä tarvittavat laitteet, ohjelmat ja käyttöoikeudet kartoitetaan tarkasti valvontaa varten. Kun etätyö loppuu, huolehditaan järjestelyjen purkamisesta asianmukaisesti. (Vahti 2002, 13–14.)

Etätyöstä täytyy tehdä sopimus työntekijän kanssa. Sopimuksessa määritellään tietoaineistojen, laitteiden ja ohjelmien luvallinen käyttö. Samalla käydään läpi työnantajan hallintaoikeus etätyölaitteisiin työntekijän yksityisyyden suojaa kunnioittaen. Etätyöhön varattu tekninen tuki ja ongelmatilanteiden raportointiketju esitellään. Tietoturvaohjeistus ja siihen sisältyvät seuraamukset käydään läpi työntekijän kanssa. (Vahti 2002, 11.)

Keskusmarkkinajärjestöt kehottavat kiinnittämään erityistä huomiota esimiehen valmiuteen johtaa etätyötä ja työnantajan laitteiden henkilökohtaisen käytön rajoituksiin (Työmarkkinakeskusjärjestöt 2005). Työntekijällä on oikeus kieltäytyä etätyöstä tai tottua niin halutessaan työtehtäviin ennen etätyöhön siirtymistä. Työntekijällä on oltava samat mahdollisuudet osallistua koulutuksiin kuin muilla työntekijöillä. (Vahti 2002, 14 & Helle, 99.) Etätyöstä sopimisen yhteydessä olisi järkevää varmistaa ja päivittää työntekijän tietoturvaosaamista. Etätyön tekniset tietoturvaohjeet on käsitelty työssä omien otsikoidensa alla. Seuraavassa kappaleessa esitellään puhtaasti työntekijän hallinnassa olevia tietoturvallisia toimintatapoja.

5.3 Etätyöntekijän tietoturvaosaamisen kulmakivet

5.3.1 Huijausten tunnistaminen

Huijaukset, kyberhyökkäykset ja haittaohjelmien mekanismit kehittyvät jatkuvasti. Ensimmäinen askel huijausten tunnistamisessa onkin seurata tietoturvauutisia ja raportteja toteutuneista kyberhyökkäyksistä. Erilaisista huijausyrityksistä keskusteleminen kahvitauolla on yksinkertainen tapa levittää tietoisuutta hyökkäysten mekanismeista. Yrityksen sisällä leviävistä huijausviesteistä kannattaa varoittaa käyttäjiä. On tehokkaampaa viestiä positiivisella otteella hyvin raportoiduista huijauksista, kuin levittää myötähäpeää huijauksiin lankeamisista. (Kyberturvallisuuskeskus 2020c, 14–15, 26.)

Katteettomat lupaukset, kiireen korostaminen ja todisteiden puute kielivät huijauksista yleisellä tasolla. Pankit, viranomaiset tai työnantajan tekninen tuki eivät pyydä henkilö- käyttäjätunnus- tai maksutietoja yllättävällä viestillä tai puhelimitse. Ensimmäinen varoittava tekijä epärehellisessä yhteydenotossa on lähettäjän nimi, osoite tai numero, joka ei millään tavalla liity väitettyyn organisaatioon. Lähettäjään ei kuitenkaan kannata sokeasti luottaa, sillä puhelinnumeron ja lähettäjän voi väärentää, tai lähettäjänä voi olla tilin murtanut hakkeri tai haittaohjelma. Massatuotantona lähetetyissä huijausviesteissä vastaanottajaa ei yleensä yksilöidä mitenkään, eikä viestissä anneta yhteystietoja lähettävälle taholle. (CISA 2009; Kyberturvallisuuskeskus 2021c.)

Käyttäjätunnuksia kalastellaan yleisimmin väärennetyn sisäänkirjautumissivun avulla. Väärennetyn sivuston voi tunnistaa vieraasta osoiterivistä, kirjoitus- ja kielioppivirheistä tai graafisen ulkoasun eroista alkuperäiseen nähden. Kaikki huijaussivustot eivät osaa väärentää varmenteita. Osoiterivin HTTPS-tunnisteen tai SSL-sertifikaatin (vihreän lukon kuvan) puuttuminen voi siis varoittaa väärennöksestä. (Kyberturvallisuuskeskus 2021c.)

Mikäli jokin yksityiskohta kirjautumissivustossa herättää epäilyksiä, kannattaa linkki jättää huomioimatta ja kirjautua palveluun suoraan tutulla tavalla. Jos linkki sisältyy epäilyttävään tai odottamattomaan viestiin kollegalta, kannattaa viestin sisältö varmistaa ensin lähettäjältä. Yrityksen nimissä lähetetyn huijausviestin alkuperän voi varmistaa yrityksen kotisivuilta, joilla usein tiedotetaan huijausviesteistä. Väärennösviesti voi saapua myös tutulta kontaktilta vanhan keskusteluketjun jatkoksi. (Kyberturvallisuuskeskus 2021c.)

Useissa tietoturvaohjeissa suositellaan tarkastelemaan linkkitekstin kohdesivustoa siirtämällä hiiri tekstin päälle, ja lukemalla yleensä sivun alareunaan ilmestyvä osoite. Näin linkkiä ei tarvitse klikata, jotta näkee, minne linkki todellisuudessa ohjaa. Ohjetta ei kuitenkaan kannata noudattaa Powerpoint tiedostoissa. Ohjelman voi asettaa aktivoitumaan juuri hiiren kelluessa linkin päällä. (Hashim, 2020.) Linkitettyjä osoitteita voidaan myös lyhentää erillisellä palvelulla, jolloin kohdeosoite ei kerro todellista määränpäätä.

Kyberrikostietoisuutta voidaan parantaa organisaation sisäisellä työpajatyyppisellä harjoittelulla, joka tukee omaan työhön liittyvän tietoturvaloukkauksen tun-

nistamista ja toimintaohjeiden soveltamista (Kyberturvallisuuskeskus 2020c, 36–37.) Digi- ja väestötietovirasto järjestää vastaavia koulutustilaisuuksia. Taisto-harjoituksissa kehitetään organisaation tietoturvan toimintaprosesseja. Harjoituksissa simuloidaan tietoturvaloukkauksen käsittelyä, viranomaisviestintää ja mediayhteydenottojen käsittelyä. (Rousku 2020.)

5.3.2 Salasanat

Salasanojen valinta ja käyttö on työntekijän vastuulla. Salasanaa ei tulisi koskaan luovuttaa toiselle henkilölle, eikä tunnusten yhteiskäyttö ole tietoturvallista. Salasanaa tulisi kohdella kuten fyysistä avainta: yksi luonnollinen henkilö on siitä koko ajan vastuussa, eikä hän tee siitä kopioita tai jätä sitä lukkoon paikalleen. Tärkeitä salasanoja ei saa tallentaa selaimeen. Yhteiskäytössä olevan laitteen selaimen välimuisti on tyhjennettävä käytön jälkeen. Henkilökohtaisessa käytössä olevien tilien kirjautumisilmoitukset kannatta ottaa käyttöön. Niiden avulla käyttäjä näkee, miltä laitteilta ja miltä maantieteellisiltä sijainneilta tunnuksille on kirjauduttu sisään. (Kyberturvallisuuskeskus 2021d.)

Salasana on sitä vaikeampi murtaa, mitä pidempi se on, ja mitä suuremmasta kokoelmasta sen merkit on kerätty. Siksi moderneissa salasanoissa vaaditaan isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä. Lyhyt salasana murretaan helposti väsytystekniikalla (englanniksi brute force -hyökkäys), jossa salasanaa yksinkertaisesti arvataan järjestelmällisesti, kunnes oikea merkkijono löytyy. Laskentatehosta ja salasanan pituudesta riippuen salasanan murtaminen voi olla vain ajan kysymys. Laskentatehon lisäksi murtamisessa käytetään apuna listaa useimmin käytetyistä salasanoista, yleisimmistä fraaseista ja tavallisen sanakirjan koko sisällöstä. Kyberturvallisuuskeskus 2020f, 17; Kyberturvallisuuskeskus 2021d.)

Kohdistetussa tietomurrossa käytetään esimerkiksi sosiaalisesta mediasta kerättyjen tietojen perusteella muodostettuja valistuneita arvauksia salasanan murtamiseksi. Kyberturvallisuuskeskus suositteleekin käyttämään salasanana vähintään 15 merkin satunnaista merkkijonoa tai kokonaista lausetta. Lauseen pituus nostaa väsytystekniikalla murtamiseen vaadittujen yritysten määrää. Lisäksi lauserakenne on helpompi muistaa kuin satunnainen merkkijono ja se

sisältää luonnollisesti erikoismerkkejä ja suuria alkukirjaimia. Kyberturvallisuuskeskus 2020f, 15; Kyberturvallisuuskeskus 2021d.)

Samaa salasanaa ei tulisi käyttää eri palveluissa. Erityisesti työhön liittyviä salasanoja ei tulisi sekoittaa yksityiskäytössä oleviin palveluihin. Tavallisen verkkokaupan ei voi olettaa huolehtivan salasanojen suojauksesta samalla tasolla kuin yrityksen, jonka resursseihin salasana antaa käyttöoikeuden. Yhdessä käyttökohteessa murrettua salasanaa on helppo kokeilla muihinkin käyttäjän tileihin. Jos salasana murretaan yhdessä palvelussa, tulee se poistaa käytöstä kaikissa palveluissa. Kyberturvallisuuskeskus 2021d.)

Unohtuneen salasanan palauttamiseen käytetyn tilin salasanaan kannattaa panostaa. Monimenetelmäinen tunnistautuminen tulisi ottaa käyttöön vähintäänkin siinä tilissä, jota käytetään muiden tunnusten palauttamiseen. Salasanan palauttamisessa käytettyyn turvakysymykseen kannattaa valita kuvitteellinen vastaus, jota ei esimerkiksi sosiaalista mediaa tutkimalla voida kaivaa esille. Kyberturvallisuuskeskus 2021d.)

Yksilöllisen salasanan valitseminen jokaiseen palveluun erikseen johtaa usein valtavaan määrään muistettavia tunnuksia ja salasanoja. Harvoin käytettävien tunnusten salasanat voi hyvin uusia joka käyttökerralla palautustilin avulla, mutta mikäli säännöllisesti käytettäviä tilejä on useita, kannattaa salasanat tallentaa erilliseen salasanojen hallintaohjelmaan. Ohjelma generoi vahvoja satunnaismerkkijonoja ja tallentaa kaikkien tilien salasanat salatussa muodossa yhteen tietoturvalliseen kirjastoon. Salasanoja ei tulisi koskaan säilöä tai viestiä salaamattomassa muodossa. Salasanan sisältävää paperia tulisi kohdella samalla tavalla kuin muitakin arkaluonteisia tietoja sisältäviä tulosteita. (Kyberturvallisuuskeskus 2020g; Kyberturvallisuuskeskus 2021d.)

5.3.3 Yksityisyys ja näkyvyys sosiaalisessa mediassa

Sosiaaliseen mediaan eli verkostoitumista tukeville sivustoille ei kannata ladata mitään sellaista tietoa, joka hakkerin käsissä kääntyisi aseeksi. Esimerkiksi sijaintitietoja, edes valokuviin upotettuna, tai päivittäisiä rutiineja ei kannata paljastaa julkisesti. Kyberrikollinen voi saada eri palveluista kerätyistä julkisista tiedoista kerättyä yhteen kokonaisuuden, joka ei enää olekaan julkinen. Turval-

lisuusasetuksilla saadaan tietojen näkyvyyttä rajattua, mutta rajoitusten kiertäminen on rikollisten työtä. Henkilökohtaisten tietojen näkyvyys tulisi rajata vain omille kontakteille. Työpaikan paljastaminen profiilitiedoissa tarkoittaa, että tilillä käyttäjä toimii työnantajansa epävirallisena edustajana. Terveydenhuoltoalalla toimivien henkilöiden tulisi noudattaa erityistä varovaisuutta julkisen ja työprofiilin pitämisessä erillään. Työnantaja voi myös ottaa kantaa asioihin, joita työntekijöiden on sallittua työstään paljastaa julkisilla alustoilla. (Vahti 2010, 36–37.)

Salasanan palauttamisessa kysyttyjä tietoja ei pitäisi koskaan julkaista sosiaalisessa mediassa. Eri sivustojen käyttöehtoihin ja tietosuojaselosteisiin tulisi tutustua vähintäänkin aina sääntöjen muuttuessa. Sivustoa tulisi estää luovuttamasta sähköpostiosoitetta eteenpäin, markkinoimasta itseään tilin kontakteille ja jakamasta tietoja hakukoneille. Sosiaalisessa mediassa julkaistuja tai mainostettuja kolmannen osapuolen sovelluksia ja kyselyitä tulisi välttää. Pienoisohjelmiin on helppo upottaa haittaohjelmia ja ne saattavat luovuttaa tietoja eteenpäin käyttäjältä salaa. Roskapostia voi vähentää luomalla roskapostitilin vähemmän tärkeille sivustoille kirjautumiseen. Tällöin päätili ja sen kontaktit ovat paremmassa suojassa roskapostilta. (CISA 2011; NSA 2018, 2–4.)

6 FYYSINEN TURVALLISUUS

Etätyössä fyysinen turvallisuus heikkenee vääjäämättä. Yrityksen tilat on jaettu vyöhykkeisiin sen mukaan, kuinka arkaluonteista tietoa rakennuksen sisällä käsitellään. Kulku rakennuksessa ja vyöhykkeiden välillä on valvottua. Tilojen suunnittelussa on otettu murron, salakuuntelun, sähkövian, tulipalon ja tulvan mahdollisuudet huomioon. Yritystilat on kaikin puolin suunniteltu tietoturvan kannalta optimaalisiksi, koteja ei. Vastuu työympäristön fyysisen turvallisuuden järjestämisestä, etenkin perheenjäsenten pääsystä työresursseihin on työntekijällä. Työnantaja ei voi käytännössä auditoida etätyöntekijän työpistettä. (Vahti 2002, 15, 21; Katakri 2020, 22–23, 30.)

Fyysisiä tallennusvälineitä ja tietoaineistoja käsitellään työpaikan ulkopuolella mahdollisimman vähän, tietoaineiston etäkäytöstä annettujen ohjeiden mukaan. Käytön jälkeen aineistot palautetaan mahdollisimman pian työpaikalle tai tuhotaan samoin kuin työpaikalla. Työlaitteita tai tietoaineistoja ei jätetä valvomatta työpisteen ulkopuolelle, esimerkiksi autoon. Etätyöpisteessä laitteet ja aineistot säilytetään lukkojen takana. Matkatyössä fyysistä turvallisuutta voidaan parantaa lukitsemalla laitteet kaapelilla rakenteisiin, käyttämällä päätelaitteen näytössä katselukulmaa rajoittavaa suojakalvoa ja välttämällä työasioista puhumista. (Vahti 2002, 16, 22)

Puhtaan pöydän periaate parantaa fyysistä tietoturvaa etätyössä. Periaate tarkoittaa sitä, ettei työpisteelle jätetä näkyviin asiakirjoja tai muistilappuja. Toimistotyössä työpisteen puhdistuksella estetään arkaluonteisten tietojen paljastuminen ulkopuolisille kuten siivoojille ja huoltohenkilökunnalle. Etätyössä periaatteen tarve korostuu, koska useammalla ulkopuolisella henkilöllä voi olla pääsy työpisteelle. Kodinomaisissa työpisteissä raportin etsiminen epäjärjestyksessä olevalta työpisteeltä voi olla työläämpää kuin työpaikalla, jos joukossa on henkilökohtaisiakin papereita. (Alexander, Finch, Sutton & Taylor 2013, 160–161.)

Puhtaan pöydän periaatteeseen sisältyy myös päätelaitteen näytön lukitseminen laitteelta poistumisen ajaksi (Alexander ym. 2013, 161). Lukitusnäytön ilmoitustekstit kannattaa poistaa käytöstä niin tietokoneella kuin kannettavallakin laitteella. Ilmoitustekstit voivat paljastaa arkaluonteista tietoa, kuten sähköposti-

viestin otsakkeen tai liittymään tilatun kertaluonteisen koodin. (Franklin, Howell, Scarfone, Souppaya & Sritapan 2021, 9.) Puhtaan pöydän periaate kannattaa muistaa myös videoneuvotteluun liittyessä. Taustalta ei pitäisi pystyä erottamaan työhön liittyvää aineistoa. Samalla periaatteella tulisi kokouksessa sisältöä jakavan tahon rajoittaa ilmoituksia ja työpöydällä näkyviä tietoja. (CISA 2021b, 3–4)

7 LAITTEISTOTURVALLISUUS

7.1 Laitehallinnan tekniset haasteet

Etätyöhön siirryttäessä työlaitteiden käyttötavat muuttuvat merkittävästi. Kannettavien laitteiden käyttö lisääntyy. Kannettavat laitteet, erityisesti älypuhelimet ja tabletit, tuovat mukanaan monia teknisiä haavoittuvuuksia ja operationaalisia riskejä. Riskit ja haavoittuvuuksien runsaus johtuvat pääasiassa siitä, että älypuhelin välineenä taipuu paljon monipuolisempaan käyttöön kuin perinteisessä toimistotyössä käytetty pöytätietokone. Kannettavat laitteet muodostavat hyvin värikkään osion yrityksen laitekatalogiin: Kannettavia laitteita hankitaan useilta eri laitevalmistajilta ja laitteiden käyttöjärjestelmät kehittyvät ja päivittyvät tiheällä tahdilla. Tietoturvapäivitysten saatavuuden kannalta vilkas kehitys on hyödyllistä, mutta laitehallintaa eri versioiden määrä hankaloittaa entisestään.

Älypuhelimessa ja tabletissa on pöytäkoneeseen verrattuna monipuolisemmat langattomat yhteydet ja enemmän kolmannen osapuolen sovelluksia, esimerkiksi maksusovelluksia. Langattomat yhteydet ovat avoimia salakuuntelulle ja väliintulohyökkäyksille. Käyttöjärjestelmään voi kuulua esiasennettuja sovelluksia, joita ei voi poistaa, eikä yritys tietoturvan näkökulmasta voi luottaa ulkopuolisen tahon tarjoamaan sovellukseen. Älypuhelinten asetusvalikkoja ei ole keskitetty tietoturvan kannalta parhaalla mahdollisella tavalla. Osa tietoturvaan liittyvistä asetuksista, esimerkiksi sovellusten laiteoikeudet, on usein hajautettu sekä järjestelmäasetuksiin, että sovellusten sisälle. (NCSC 2020; Franklin, ym. 2021, 7–9.)

Älypuhelimen ja tabletin sisäänkirjautumisen suojaus on usein heikompi kuin tietokoneen. Työkoneelle on totuttu kirjautumaan sisään oikeaoppisesti, mutta älypuhelimen käyttöönoton oletetaan olevan salamannopeaa ja helppoa. Mahdollisuuksien mukaan myös kannettaviin laitteisiin tulisi asentaa eri tasoiset käyttäjätunnukset sovellusten asentamista ja tavallista käyttöä varten. Älypuhelimissa pääkäyttäjän oikeudet on onneksi oletusarvoisesti poistettu käytöstä. Järjestelmän muokkauksesta kiinnostunut käyttäjä tai haittaohjelma voi kuitenkin murtaa oikeudet käyttöön. Tietoturvariskien takia pääkäyttäjän tai juuren

oikeuksille murrettuja henkilökohtaisia laitteita ei tulisi käyttää etätyössä. (Brown ym. 2016, 8–9; Franklin ym. 2021, 8.)

7.2 Laitehallinnan operationaaliset haasteet

Teknisten haasteiden lisäksi kannettavat laitteet ovat äärimmäisen haavoittuvaisia varkauksille, katoamisille ja fyysisille vaurioille (Franklin ym. 2021, 7). Laitteiden omistusoikeudet ja eri käyttötarkoitukset muodostavat omat riskinsä tietoturvalle. Vaikka työlaitteet olisivat työnantajan omistuksessa ja hallinnassa, täytyy vahingollinen henkilökohtainen käyttö kieltää tietoturvan perusteella. Lisäohjeita tarvitaan erityisesti, kun työssä käytetään henkilökohtaisia laitteita, tai kun työnantajan hankkima laite on tarkoitettu myös henkilökohtaiseen käyttöön. Henkilökohtaisella laitteella tarkoitetaan tietoturvaohjeissa käyttäjän itse *hallinnoimaa* laitetta. Laitehallinnassa omistussuhteella ei ole suurtakaan merkitystä, mikäli laite on täysin oikeuksin työnantajan keskitetyssä laitehallinnassa. Harva älypuhelimen omistaja kuitenkaan haluaa antaa työnantajalle täysiä oikeuksia laitteeseensa. (NCSC 2020.)

Etätyössä työ- ja henkilökohtaisen käytön välinen raja hämärtyy helposti, ja työntekijän perheenjäsenillä voi olla pääsy laitteille. Kyselytutkimusten mukaan työlaitteita käytetään yllättävän paljon henkilökohtaisiin asioihin. Detwiler kiteyttää artikkelissaan näppärästi useamman kyselytutkimuksen tulokset aiheeseen liittyen: Malwarebytes-yhtiön vuoden 2020 kyselytutkimuksessa todettiin, että työkoneella tarkistetaan henkilökohtaisia sähköposteja, luetaan uutisia, tehdään ostoksia, käytetään sosiaalista mediaa ja jopa asennetaan kolmannen osapuolen sovelluksia. Erilaisiin kyselytutkimukseen vastanneista etätyöntekijöistä yli puolet tunnustaa myös käyttävänsä kotikonetta työskentelyyn tai henkilökohtaista älypuhelinta sähköpostin lukemiseen. (Detwiler 2021.)

Yksinkertaisia työasioita on helppo sortua hoitamaan tutulla älypuhelimella, jos valinta säästää aikaa ja vaivaa. Varjotekniikka (shadow-IT) on jo oma terminsä tietoturva-alalla: Jos työnantaja ei tarjoa tiettyä tarpeelliseksi koettua ohjelmaa tai laitetta, oppivat työntekijät nopeasti hyödyntämään henkilökohtaisia laitteita ja ohjelmia. Yritysketju ei välttämättä tule varjoresursseista tietoiseksi, ennen

kuin käytöstä aiheutuu tietoturvaloukkaus. (Hertvik & Raza 2020; Franklin ym. 22.)

7.3 Laitteiden käytöstä sopiminen

Etätyö vaatii monia laitehallintaan liittyviä pelisääntöjä työntekijän ja työnantajan välille. Etätyönä tehtävät työt tulisi luokitella tietoturvan tason vaativuuden mukaan, jotta ymmärretään, millaisia työtehtäviä varsinkin kannettavilla laitteilla on turvallista suorittaa. Työnantajalla on vastuu tietoturvasta kokonaisuutena, ja turvattomien laitteiden käyttö tulee perustella riskianalyysillä ja kompensoida riittävillä tietoturvatoimilla. Kokonaisriskiä voidaan pienentää teknisillä vaatimuksilla ja käytön rajoituksilla. (Vahti 2002, 11–12)

Työtehtävien tietoturvavaatimukset siis määrittelevät, mitä tehtäviä saa tehdä eri laitteilla. Työnantajan hallinnoimalle laitteelle voidaan sallia laajemmat etäkäyttöoikeudet kuin henkilökohtaiselle tietokoneelle, ja henkilökohtaiselle älypuhelimelle voidaan sallia vaikka pelkkä sähköpostin käsittely. Töitä voidaan rajata myös ajallisesti tai tietoaineistojen käyttöoikeuksilla. (Vahti 2013, 21–22; Greene, Scarfone & Souppaya 2020, 11–12.)

Luvallisesta käytöstä sopimalla vältetään räikeät mutta tahattomat tietoturvarikkomukset. Työntekijälle tulee tarjota käyttöohjeiden ohella selkeä kuvaus sääntöjen rikkomisesta aiheutuvista seurauksista. Käytöstä sopimalla huolehditaan myös työntekijän yksityisyyden suojasta. Työnantajalla on oikeus valvoa hankkimiensa työlaitteiden käyttöä ja määritellä, mihin laitteita ja esimerkiksi sähköpostitiliä saa käyttää. (Vahti 2013, 25–26.) Vuonna 2020 etätöihin siirryttiin sankoin joukoin ja nopealla varoitusajalla. Detwilerin kartoituksen mukaan myös työntekijöiden etävalvonta yleistyi poikkeustilanteen aikana. Ilman asiallisia sopimuksia improvisoidut järjestelyt ovat hyvinkin voineet loukata työntekijöiden yksityisyyden suojaa. (Detwiler 2021).

7.4 Käyttöprofiilit

Luvallista käyttöä määritellessä lähdetään liikkeelle siitä, että työ-, edustus- ja henkilökohtainen käyttö eriytetään toisistaan, toisin sanoen työntekijä käyttää

laitetta yhdessä roolissa kerrallaan. Eri roolien tietolähteitä ja järjestelmiä ei pidetä käynnissä rinnakkain. Pelkkään työtarkoitukseen tarkoitetun työkoneen kohdalla tämä tarkoittaa, että laitteen ohjelmia ei käytetä henkilökohtaisen tietoaineiston käsittelemiseen. Vaikka tiedot olisivat koneella turvallisesti salatussa muodossa, voi työnantajan edustaja olla valtuutettu tarkastelemaan tietoja työntekijän seurannan tai järjestelmän ylläpitotehtävien ohella. Sopimalla laitteiden käytöstä voidaan vahvistaa lisensoitujen ohjelmien käyttötarkoitus ja varmistaa, että työntekijä ei kehitä etätyössä alkuperäisiä lisenssisopimuksia rikkovia tapoja. Käyttötavoista sopiessa voi olla tarpeen muistuttaa, että työsähköpostiin tai puhelinliittymään saapuvia viestejä ja puheluita ei saa uudelleenohjata henkilökohtaisiin tileihin. (NSA Cybersecurity 2020, 1–2.)

Laitteilla, joissa sekä henkilökohtainen että työkäyttö on sallittua, tulisi eri rooleihin liittyvät tehtävät eriyttää toisistaan muilla keinoin. Laitteeseen kirjaudutaan sisään joko työ- tai henkilökohtaisilla tunnuksilla, ja eri tileillä käsitellään vain käyttörooliin kuuluvia tietoaineistoja. Uuteen rooliin siirtyessä vanhat välilehdet, ohjelmaikkunat ja taustatoiminnot suljetaan, ja selaimen välimuisti tyhjennetään. Sisään kirjautumista vaaditaan ohjelmatasolla, eikä kirjautumistietoja tallenneta sovelluksiin tai selaimiin (NSA Cybersecurity 2020, 1–2.)

Virtualisointi on tehokas tapa eristää eri profiilien resurssit toisistaan. Tietokoneelle voidaan asentaa useampia erillisiä virtuaalikoneita, jotka jakavat koneen laiteresurssit, mutta eivät pääse saastuttamaan toisiaan. Virtualisointi alkaa yleistyä myös älypuhelinalustoilla. Android ja Apple tarjoavat käyttöjärjestelmän tasolla keinoja profiilien eriyttämiseen ja osittaiseen laitehallintaan. Ideana on estää henkilökohtaisten sovellusten käyttöoikeus resursseihin, jotka työprofiililla on käytössä. Erityisesti laitekohtainen VPN-yhteys yrityksen tietojärjestelmiin tulisi eristää henkilökohtaisilta sovelluksilta. (Vahti 2013, 49; Greene ym. 2020 2–3.)

Eristetyn työprofiilin voi asentaa henkilökohtaiseen puhelimeen myös kolmannen osapuolen sovelluksen, esimerkiksi ManageEngine:n tai SureMDM:n avulla. Pilvipalveluiden toimittajat tarjoavat laitteiden ja mobiilisovellusten hallintaan omia ratkaisujaan. Microsoftilla mobiilisovellusten hallinta (Mobile Application Management) ja mobiililaitehallinta (Mobile Device Management) kuuluu Intune

– tuoteperheeseen, joka on osa päätelaitteiden hallintapaneelia (Endpoint Manager). (Microsoft Docs 2021b.)

7.5 Keskitetty laitehallinta ja yleiset tietoturvavaatimukset

Osa nollaluottamuksen periaatetta ja ehdollisia käyttöoikeuksia on laitteen huomiointi valtuutusprosessissa. Yleisesti suositellaan, että työkäytössä olevat ja resursseja käsittelevät laitteet listataan laiterekisteriin. Laiterekisteristä löytyvät laitteen käyttöjärjestelmän versio, asennetut ohjelmat, palomuuri ja virustorjuntaohjelma listattuna. Luettelotietojen avulla määritellään asetukset, joilla saavutetaan laitteelta vaadittava tietoturvan taso. Rekisteri auttaa löytämään laitteisiin liittyvät tekniset haavoittuvuudet. Vain rekisterin perusteella luotetuille laitteille tulisi sallia yhteys tietojärjestelmiin. (Franklin ym. 2021. 15–16.) Laiterekisterin tietojen huomioiminen valtuutusprosessissa voi vaatia erillisen päätelaitteiden tai liikkuvuuden hallintasovelluksen.

Laitehallinnan tavoitteena on yleisesti huolehtia, että etätyössä käytetyt laitteet noudattavat niille määriteltyjä tietoturvavaatimuksia. Tietoturvavaatimukset lähtevät siitä, että työskentelyssä käytetään työnantajan määrittelemiä tietoturvatyökaluja ja virallisia ohjelmia. Käyttöjärjestelmä ja työssä tarvittavat sovellukset päivitetään mahdollisimman nopeasti. Etätyölaitteeseen ei tulisi asentaa tuntemattomia sovelluksia kolmannen osapuolen lähteistä. Parhaiten ohjelmaasennuksia hallitaan minimikäyttöoikeuksien ja valkoisen listan avulla. (Franklin ym. 2021, 8.)

Tietoturvavaatimuksissa määritellään laitekohtaisesti varmuuskopiointi ja lokikirjanpitoasetukset sekä viestinnän ja levyasemien salausmenetelmät. Käytännössä mikä vain etätyölaite voidaan varastaa, joten autentikointi ja muistin kryptografinen salaus ovat pakollisia turvamenetelmiä. (Scarfone, Sexton & Souppaya 2007 15–17.) Päätelaitteiden hallintaohjelman avulla tietoturva-asetukset voidaan pakottaa käyttöön hallittaville laitteille. Vähintäänkin kadonneen laitteen paikantava ja tarvittaessa tyhjentävä hallintasovellus on tarpeen. Laitehallintaan kuuluu myös huoltojärjestelyjen sovittaminen etätyön vaatimuksia vastaavaksi ja käytöstä poistettujen tai käyttötarkoitusta vaihtavien laitteiden asiallinen tyhjentäminen. (Franklin ym. 2021, 19–21.)

7.6 Päätelaitteiden kovennus

Yleisten tietoturvavaatimusten lisäksi yrityksen on mahdollisimman yksityiskohtaisesti linjattava halutut tietoturva-asetukset ja laitteiden kovennusohjeet. Kovennusohjeiden määrittely vaatii valmistajan ohjeisiin ja laitteiden ominaisuuksiin tutustumista. (Franklin ym. 2021, 21, 29.) Laitearsenaalia kannattaa yhtenäistää, ja kiinnittää hankinnoissa huomiota alustan yleisiin teknisiin haavoittuvuuksiin ja tietoturva-asetusten helppokäyttöisyyteen.

Nollaluottamuksen periaatteita noudattaen älypuhelimen ylimääräiset langattomat yhteydet, palvelut ja toiminnot rajataan välttämättömiin. Langattomat yhteydet mahdollistavat salakuuntelun ja väliintulohyökkäyksen. Esimerkiksi aina päällä olevat sijaintitiedot tarjoavat hyökkääjälle kohdennetuissa hyökkäyksissä hyödyllistä tietoa käyttäjän rutiineista ja kanssakäymisistä. Hyökkääjä skannaa paikkatiedot esiin myös tiedostojen, erityisesti valokuvien metatiedoista. Laitteen paikannus- ja aikatiedot voidaan sekoittaa syöttämällä väärennettyä GPS-signaalia laitteen lähellä. (Franklin ym. 2021, 9; Scarfone ym. 10)

Kannettavan laitteen näyttö tulisi asettaa lukittumaan automaattisesti muutaman minuutin jälkeen. Lukituksessa tulee käyttää tarpeeksi pitkää ja vaikeasti arvattavaa koodia, jota ei saada murrettua muutamalla yrityksellä. Kuvio on tietoturvan kannalta huono valinta lukituskoodiksi, sillä sen piirtämisestä voi jäädä näytön lasiin helposti tunnistettavat jäljet. Väärän avauskoodin syöttäminen loputtomasti täytyy estää, muuten pitkänkin koodin saa murrettua väsytyshyökkäyksellä. Laitteen muistin voi asentaa pyyhkiytymään tyhjäksi, kun avausta yritetään tarpeeksi monta kertaa. Lukituksen voi avata myös biometrisellä tunnisteella. (Franklin ym. 2021, 16.)

Älypuhelimet ladataan useimmin USB-johdolla, jossa on myös tiedonsiirron mahdollistavat pinnit. Laitteen asetuksista tulisi poistaa mahdollisuus virheenkorjaukseen ja tiedonsiirtoon USB kaapelin kautta. Tiedonsiirto-ominaisuuksien salliminen mahdollistaa haittaohjelmien latautumisen ja murtautumisen laitteelle näyttölukituksen ohi. Työlaitteita ei tulisi koskaan ladata tuntemattomissa latauspisteissä, eikä kannettavaa laitetta ole aihetta yhdistää työkoneeseen kaapelilla tai langattomasti. Matkatyöhön voidaan hankkia pelkät virtapinnit sisältä-

vä latausjohto. Laitteet tulisi ladata pääsääntöisesti virtapistokkeesta, ei dataportista. (Summerson 2017; Brown ym. 2016, 15.)

Takaportin asentaminen älypuhelimeen on kyberrikollisen näkökulmasta hyödyllistä ainakin kolmesta eri syystä: Älypuhelinta pidetään aina päällä ja verkossa, se on käyttäjän kaikissa toimissa mukana ja se sisältää vakiovarusteina hyödyllisiä vakoiluvälineitä kuten ääninauhuri, kamera ja GPS-paikannin. Kameran ja ääninauhurin luvaton käyttö voidaan estää käyttämällä tarkoitukseen suunniteltua suojakuorta. Älypuhelin voidaan paikantaa monella eri tavalla, joten sijainniltaan arkaluonteisissa työtehtävissä ei valvomatonta älypuhelinta kannata kantaa mukana ollenkaan. (NSA Cybersecurity 2020, 1–2.) Vakoilunäkökulman tiedostaminen voi auttaa työntekijöitä sitoutumaan kannettavien laitteiden hallintatoimenpiteisiin.

8 TIETOLIIKENNETURVALLISUUS

8.1 Etäyhteydet

8.1.1 Tunnelointi

Tunnelointi tarkoittaa yksityisen, salatun käytävän muodostamista käyttäjältä resurssiin julkisen verkon sisällä. VPN, eli virtuaalinen erillisverkko, muodostaa yksityisen tunnelin käyttäjän laitteelle asennetun asiakasohjelman ja VPN-yhdyskäytävän välille. Yhdyskäytävä kommunikoi palvelinohjelmiston kanssa. Yhdyskäytävän avulla käyttäjä pääsee sisään yrityksen palvelimilla sijaitseviin resursseihin. VPN tarjoaa kryptografisen salauksen, käyttäjän tunnistamisen ja pääsynvalvonnan työkaluja. (Scarfone & Souppaya 2016, 4–6.)

VPN-yhteyttä käyttäessä VPN-asiakasohjelmisto ja servereiltä haettu data täytyy tallentaa käyttäjän koneelle. VPN vaatii rinnalleen muita tietoturvaratkaisuja, sillä se ei suojaa tallennettuja tietoja tai havaitse asiakaslaitteen muiden ohjelmien toimintaa. Yhteyttä ei tulisi ottaa käyttöön turvattomilla laitteilla. (Scarfone & Souppaya 2016, 5–7.) VPN-laitteisiin ja yhteyskäytäntöihin liittyviä haavoittuvuuksia hyödynnetään ahkerasti. Korjauspäivitysten käyttöönotto on kuitenkin usein hidasta. VPN palvelu on jatkuvasti ylhäällä ja laitteet harvoin tukevat käytönaikaista päivitystä. Laitevalmistajat julkaisevat kovennusohjeita ja korjauspäivityksiä tiheästi. (Sarvepalle 2019.)

VPN tunnelointi voidaan pakottaa kaikelle liikenteelle, vain organisaation sisäiselle liikenteelle, tai valikoiden. Tyypillinen tapa valikoida tunneloitavaa liikennettä on jättää päivitysten lataaminen VPN-tunnelin ulkopuolelle. Valinta keventää VPN-liikenteen kuormitusta ja varmistaa päivitysten latautumisen myös niille etätyölaitteille, joilla VPN-yhteyttä ei välttämättä tarvita säännöllisesti. Jos laitteelle sallitaan tavallista internetkäyttöä VPN-yhteyden lisäksi, täytyy tietoturvaohjelmiston ja muiden tietoturvavaatimusten olla tarvittavalla tasolla. (Kyberturvallisuuskeskus 2020h.)

8.1.2 Virtualisointi

Virtualisoinnilla toteutetaan ohjelmaversiona kopio palvelimesta, päätelaitteesta, käyttöjärjestelmästä tai yksittäisestä sovelluksesta. Tarkoituksena on luoda turvallinen käyttöympäristö, jonka sisällä yrityksen resursseja voi hyödyntää tietoturvallisesti myös etänä. Microsoft suositteleekin keskitetyn laitehallinnan ulkopuolisille laitteille virtuaalityöpöytäyhteyttä resursseihin. Mobiililaitteissa virtualisoinnilla on selkeitä etuja: sama käyttökokemus saadaan aikaiseksi eri laitteilla, työ- ja henkilökohtainen profiili saadaan eristettyä toisistaan ja päätelaitteelle ei tarvitse asentaa asiakasohjelmia tai tallentaa käsiteltävää dataa pysyvässä muodossa. (Microsoft 2021.)

Mobiililaitteilla virtuaalityöpöytäympäristöön päästään käsiksi joko sovelluksen tai selaimen lisäosan avulla. Virtualisointiratkaisuja on aina testattava ennen käyttöönottoa, sillä kannettavien laitteiden näytön koko ja näppäimistön ja hiiren puuttuminen voivat vaikeuttaa esimerkiksi valikoiden käyttöä kohtuuttomasti. (Perakovic, Husnjak & Cvitic 2014, 3–4, 6)

8.1.3 Zero Trust -arkkitehtuuri

Puhtaasti nollaluottamukseen pohjautuva tietojärjestelmä suunnitellaan alusta alkaen rakenteeltaan tiedon kulun tarpeiden mukaan. Jokaiseen palveluun kirjaudutaan salatusti ja suoraan, jolloin tietoliikennetason kiertoratkaisut kuten VPN-yhteydet jäävät tarpeettomiksi. Valmiita tietojärjestelmiä ei pystytä jälkikäteen organisoimaan uudelleen täysin nollaluottamuksen arkkitehtuurin mukaisiksi, sillä kaikki vanhat järjestelmät eivät tue keskitettyä autentikointia. (Borchert ym. 2020, 36.)

Nollaluottamukseen pohjautuva arkkitehtuuri voidaan rakentaa tietoturvatyökaluja tarjoavan pilvipalvelun, esimerkiksi Zerotierin, avulla. Zerotier virtualisoi tietojärjestelmän verkkolaitteita ja tarjoaa yhden sovelluksen sisällä kaikki perinteisen tietojärjestelmäarkkitehtuurin verkkoliikenteen hallintatyökalut. (Zerotier 2021.)

8.2 Kotiverkkojen tietoturva

8.2.1 Toimintaohjeita

Etätyössä kaikki kotiverkkoon yhdistetyt laitteet muodostavat tietoturvariskin. Oheislaitteiden haavoittuvuuksien avulla voidaan murtautua lähiverkkoon ja edelleen työnantajan resursseihin. Erityisen hyödyllisiä tietomurrossa ovat kuvaus ja äänitysominaisuuksilla varustetut pelikonsolit, turvakamerat ja esineiden internet -älylaitteet (Internet Of Things). Laitteiden ja niiden hallintaohjelmien tietoturvapäivitykset tulisi asentaa välittömästi, ja kamerat ja mikrofonit sijoittaa siten, ettei niiden kautta pysty monitoroimaan työskentelypistettä. (Haney 2020 & NSA 2018, 3–4.)

Kotiverkkoon kuuluvien tietokoneiden käyttöjärjestelmät voivat aiheuttaa tarpeettomia tietoturvariskejä. Päivittämätön käyttöjärjestelmä sisältää aina hyödynnettäviä haavoittuvuuksia. Vanhimmille tuotteille ei päivityksiä enää julkaista. Esimerkiksi Windows XP-käyttöjärjestelmälle ja vanhoille Explorer-selaimille ei julkaista korjaustiedostoja. Päivitystuen ulkopuolisia tuotteita ei etätyöläisen kotiverkon laitteissa kannata käyttää. Kaikkien kotiverkon koneiden käyttöjärjestelmät tulee pitää päivitettyinä. (NSA 2018, 1–2; BeyondTrust 2021a, 6.)

Työntekijä voi parantaa kotiverkon tietoturvaa noudattamalla minimikäyttöoikeuksien periaatetta myös kotona: laitteet ja verkkoyhteydet pidetään päällä ja yhteydessä verkkoon vain tarvittaessa. Viimeistään yöksi tietokoneet ja tulostimet kannattaa sammuttaa kokonaan. Hyökkääjä ei siten pääse etäkäyttämään laitteita täysin huomaamatta yön pimeinä tunteina. Kotiverkossa ei kannata pitää jatkuvasti yhdistettynä laitteita, jotka toimivat ilman verkkoyhteyttäkin, tai joita käytetään vain harvoin. Paikalliset varmuuskopiot kannattaa säilyttää kokonaan kotiverkon ulottumattomissa. (NSA Cybersecurity 2020,1; Haney 2020.)

8.2.2 Verkkolaitteiden kovennus

Verkkolaitteen oletusasetukset tulisi tarkistaa ja tarvittaessa koventaa. Ainakin tehdasasetusten mukainen pääkäyttäjän tunnus pitää yksilöidä. Verkon reitittimen tulisi tukea verkko-osoitteen muunnoksia (Network Address Translation, NAT). Amerikkalainen tietoturvaviranomainen CISA (Cybersecurity & Infrastruc-

ture Security Agency) suosittelee WPA3- (Wi-Fi Protected Access 3), AES- (Personal Advanced Encryption Standard) ja TKIP-menetelmiä (Temporary Key Integrity Protocol). WPS (Wi-Fi Protected Setup) kannattaa ottaa pois käytöstä. Asetus mahdollistaa langattomien laitteiden liittymisen verkkoon PIN-koodin avulla. Asetuksen haavoittuvuutta hyödynnetään reitittimen väsytyshyökkäyksissä. (NSA 2018, 1–2; CISA 2015.)

Kotiverkon SSID-tunniste kannattaa muuttaa niin anonyymiksi kuin mahdollista. Hyökkääjä voi oletusnimen perusteella päätellä reitittimen mallin tai käyttäjän sijainnin. Reitittimen salasanan valinnassa tulee olla erityisen huolellinen. NSA:n ohjeissa suositellaan vähintään 20 merkin pituista satunnaismerkkijonoa. Reitittimen etähallinta ja verkon laitteiden universaali Plug-n-Play toiminto tulisi ottaa pois käytöstä. Reitittimen verkon palomuuri kannattaa ottaa käyttöön. Mikäli reititin ei sisällä omaa palomuuria, kannattaa sellainen hankkia ulkopuoliselta palveluntarjoajalta. Omaa palomuuria kannattaa harkita myös jokaiselle verkon tietokoneelle. Tietoturvaa voi parantaa eristämällä työlaitteet muista verkon laitteista omaan verkkosegmenttiinsä. Etähallittavien laitteiden autentikointi- ja salasanavalinnat täytyy koventaa samoilla periaatteilla kuin työhön käytetyissä laitteissa. (NSA 2018 1-2; CISA 2015.)

9 TIETOAINEISTOTURVALLISUUS

9.1 Pilvipalvelut

Vain etätyösopimuksessa määriteltyjä aineistoja saa käsitellä työpaikan ulkopuolella. Tietoaineistojen turvallisuusluokitus vaikuttaa tiedon käsittelyohjeisiin. Tiedot varmuuskopioidaan automaattisesti. Päätelaitteiden muistit salataan kryptografisesti. Poikkeustapauksessa, esimerkiksi työntekijän kuoltua, täytyy yrityksen varautua avaamaan käyttäjän salaamat tiedot. (Vahti 2002, 16–17.)

Pilvipalveluihin tallennettavan tiedon käsittely- ja omistusoikeus säilyy tiedon verkkoon vieneellä taholla. Liikesalaisuuksiin, ydintoimintaan ja henkilötietoihin liittyvien tietojen tallennuksesta ja käsittelystä voi olla aiheen tehdä kirjallinen salassapitosopimus pilvipalvelun tarjoajan kanssa. (Kyberturvallisuuskeskus 2021e, 7.) Pilvipalveluihin tallennettujen tietojen, erityisesti henkilötietojen, kohdalla tulee selvittää etukäteen, minne tiedot ja varmuuskopiot maantieteellisesti tallennetaan. Suomea sitova GDPR-asetus ei velvoita EU:n talousalueen ulkopuolisia valtioita. Tietojen sijoitusmaan omat lait voivat vaikuttaa siihen, mitä tietoa palvelimilla saa säilöä. Kannattaa selvittää etukäteen, minkä maan lainsäädäntöä seurataan mahdollisissa poikkeustilanteissa, ja millaiset oikeudet paikallisilla viranomaisilla on puuttua palvelinkeskusten tietosisältöön. (Kyberturvallisuuskeskus 2021e 8–9.)

Pilvipalvelua valitessa tulee myös varmistua siitä, että pilvipalvelun muistit tyhjennetään ja poistetaan elinkaarensa lopuksi käytöstä yhtä tiukoilla tietoturvamenetelmillä kuin yrityksen omassa käytössä olevat muistiasemat. Pilvipalvelun tarjoajan tiloihin voi pyytää auditointimahdollisuutta. Suuret palveluntarjoajat saattavat tarjota asiakkailleen pyynnöstä kolmannen osapuolen teettämän auditointiraportin. (Kyberturvallisuuskeskus 2021e, 9.)

9.2 Henkilötietojen käsittely

Henkilötietoja ovat kaikki luonnolliseen henkilöön liittyvät tiedot ja tiedot, joiden avulla henkilö voidaan tunnistaa. Henkilötietoja ovat esimerkiksi nimi, puhelinnumero, sijaintitiedot ja terveystiedot. Etätyölle ominaisia henkilötietoja ovat IP-osoite, ääni- ja videokuvavirrat ja -tiedostot, sekä etäpalavereiden mukana tallennetut keskusteluketjut. Henkilötietojen käsittelyä koskevat lait määrittelevät velvollisuuksia henkilörekisterin ylläpitäjälle ja henkilötietojen käsittelijöille. Rekisteröidyille henkilöille lait takaavat tiettyjä oikeuksia. (Tietosuojavaltuutetun toimisto 2021c.)

Henkilötietorekisterin ylläpitäjä ja henkilötietojen käsittelijät velvoitetaan noudattamaan tietosuojaperiaatteita tietojen käsittelyssä. Rekisterinpitäjä määrittelee henkilötietojen käsittelyn tarkoitukset, kerää vain tarpeellisen määrän tietoja tarkoitusta varten ja huolehtii tietojen päivityksestä ja korjauksesta. Tietoja ei saa säilyttää käyttötarkoitusta pidempään sellaisessa muodossa, josta luonnollinen henkilö on vielä tunnistettavissa. Tietoja on käsiteltävä luottamuksellisesti, turvallisesti, vain toimeksiannosta, keräystarkoituksen mukaisesti ja rekisteröidyn henkilön kannalta läpinäkyvällä tavalla. (Henkilötietojen käsittely 2021b.)

Rekisterinpitäjällä on velvollisuus informoida rekisteröityä tiiviissä ja ymmärrettävässä muodossa rekisterin ominaisuuksista ja käyttötarkoituksesta. Rekisteröidyllä on muun muassa oikeus tietää, miten hänen tietojaan käsitellään, tarkistaa itseään koskevat tiedot ja pyytää tietoja korjattavan tai poistettavan tietosuojaperiaatteiden mukaisesti. Rekisteröity voi myös siirtää tietonsa toiseen järjestelmään. (Tietosuojavaltuutetun toimisto 2021c.)

Yrityksen tulee aina tietää, missä roolissa se missäkin henkilötietorekisterissä on mukana, ja milloin tallennettu tieto luokitellaan henkilötiedoiksi. Rekisterinpitäjänä toimiessaan yrityksen tulee ohjeistaa työntekijät henkilötietojen käyttöön, harjoittaa ennakoivaa riskinhallintaa ja varmistaa tietosuojan toteutuminen läpi koko palveluprosessin. Henkilökunta tulee perehdyttää tunnistamaan henkilötiedot ja tietosuojaloukkaukset. (Tietosuojavaltuutetun toimisto 2021b.)

Henkilötietojen käsittelijät ovat tietoturvaloukkauksista ensisijaisesti yhteydessä rekisterinpitäjään. Tietoturvaloukkausten ilmoittaminen on rekisterinpitäjän vas-

tuulla. Kun henkilötietoja siirretään rekisteristä toiseen, on rekisterinpitäjän vastuulla varmistua siitä, että kolmas osapuoli on oikeutettu käsittelemään tietoja. Tietojen siirtämiseksi Euroopan Unionin talousalueen ulkopuolelle, missä tietosuoja-asetus ei ole voimassa, tulee siirrolle löytyä lisäksi tietosuoja-asetuksessa määritelty peruste. (Tietosuojavaltuutetun toimisto 2021d.)

10 OHJELMISTOTURVALLISUUS

Kaikki työssä tarvittavat ohjelmat, erityisesti virustorjuntaohjelmistot, selaimet ja verkkolaitteiden hallintaohjelmat päivitetään säännöllisesti. Tuntemattomien tahojen lähettämiä sähköposteja tai niiden liitetiedostoja ei tule koskaan avata haittaohjelmien vuoksi. Sähköpostitse lähetettyjä linkkejä ei kannata avata suoraan sähköpostista. Linkitetylle sivulle voi siirtyä manuaalisesti selaimen kautta. Poissaoloviestiä tulisi käyttää vain välttämättömissä tilanteissa. Poissaolostatuksen mainostaminen voi innostaa rikollisia murto- ja huijausyrityksiin. (NSA 2018, 1–4.) Tärkeitä tietoja ei saa lähettää sähköpostin kautta salaamattomassa muodossa. Kaikenlainen kiertokirjeiden ja massapostin lähettäminen työsähköpostista tulee kieltää. (Vahti 2002, 16–17.)

Huijausviestejä voidaan hillitä sähköpostiasetuksilla. TLS-asetus (Transport Layer Security) salaa sähköpostipalvelinten välisen liikenteen ja varmentaa osapuolet. SPF- (Sender Policy Framework) ja DKIM-asetuksilla (DomainKeys Identified Mail) voidaan vähentää oman yrityksen nimissä lähetettyjä huijausviestejä. Saapuvat viestit, jotka eivät täytä omalle toimialueelle määriteltyjä asetuksia, voidaan merkitä roskapostiksi tai hylätä DMARC-määritysten (Domain-based Message Authentication, Reporting & Conformance) mukaisesti. Saapuvista sähköposteista voidaan suodattaa pois huijausviestejä täsmällisten hakusanojen avulla. (CISA 2021a & Kyberturvallisuuskeskus 2019b, 14.)

Amerikkalainen kyberturvallisuusviranomainen CISA (Cybersecurity & Infrastructure Security Agency) ohjeistaa valitsemaan pääasiallisen videoneuvottelualustan etätyötä varten ja poistamaan ylimääräiset palvelut käytöstä. Palvelun valintaan vaikuttavat käyttötarkoitus, osallistuvat tahot ja laitteet, käsiteltävä tieto, salauksen tarve ja palvelun hinta. Ilmaisversioiden kokousten pituus ja osanottajamäärä voi olla rajattu. Valitun palvelun tietoturva-asetuksiin tulisi perehtyä huolella ja tiedottaa niistä käyttäjiä helposti ymmärrettävässä muodossa. Jos videoneuvottelualustaan kuuluu etähallintaohjelma, tulisi se poistaa käytöstä. Valitun palvelun päivitykset asennetaan ajallaan ja vanhat versiot poistetaan käytöstä. Jos palavereja joudutaan pitämään tuntemattomalla alustalla, tulisi käyttäjiä ohjeistaa osallistumaan kokoukseen selaimen, ei sovelluksen kautta. (Kyberturvallisuuskeskus 2020i; CISA 2021b, 2–4.)

Videoneuvottelutyökalujen räjähdysmäinen yleistyminen koronapandemian aikana toi esiin ohjelmistoissa piileviä haavoittuvuuksia ja herätti keskustelua työkalujen tietoturvasta. Videoneuvottelu kovennetaan suojaamalla kokouskutsu salasanalla, joka jaetaan käyttäjille erillään kutsulinkistä. Tunnistamattomia käyttäjiä ei päästetä suoraan kokoukseen, vaan erilliseen odotustilaan. Osallistujien oikeudet tulee rajoittaa minimiin kokouskohtaisesti. Kokouksen tallentamista harkitessa tulee ottaa huomioon käyttäjien yksityisyyden suoja ja henkilötietoja koskevat säännöt. (Kyberturvallisuuskeskus 2020i; CISA 2021b, 2–4.)

.

11 POHDINTA

Vaikka tietojenkalastelu ja tietomurrot johtavat vielä määrällisesti poikkeamatilastoja, nostaisin itse ehkä etäyön suurimmaksi haasteeksi kannettavien laitteiden ja niiden käytön kirjon. On vaikea kuvitella, miten kaikkia etätyössä käytettäviä laitteita pystyttäisiin kattavasti hallitsemaan ilman jonkinlaista liikkuvuuden hallinnan tai päätelaitehallinnan palvelua.

Valitettava tosiasia on, että edelleen valtaosa tietoturvapoikkeamista aiheutuu käyttäjän toimista. Salasana luovutetaan väärään paikkaan tai koneelle ladataan vahingollinen ohjelma. Työkoneella selataan sosiaalista mediaa ja kotikoneella käsitellään työresursseja. Inhimillisiin virheisiin vetoaminen ja käyttäjien kouluttaminen ei kuitenkaan vie tietoturvaa alana eteenpäin. Teknisiä ja operationaalisia suojakäytäntöjä täytyy kehittää hyökkäysmekanismien ohjaamaan suuntaan. Salasanasta ja VPN-yhteydestä on tullut vanhanaikainen tapa suojata järjestelmä tunkeutumiselta.

Pilvipalveluntarjoajat vaikuttaisivat vastaavan haasteeseen monilla erilaisilla hallintatyökaluilla. Identiteettien, liikkuvuuden ja päätelaitteiden hallintaan on suunniteltu monia hallintasovelluksia ja palveluita. Tarvittaessa myös infrastruktuurin verkkolaitteineen voi ostaa pilvipalveluna. Pilvipalveluiden kehittyminen ohjaa myös tietoturvan kehitystä. Samalla kuitenkin yritysten riippuvaisuus ohjelmistojäteistä kasvaa huolestuttavasti. Microsoftin työkalut ja tuoteperheeseen kohdistetut kyberhyökkäykset on dokumentoitu hyvin kenties juuri käytön yleisyyden vuoksi. Microsoftin tuotteita oli siksi helppo käyttää esimerkkeinä tässä työssä. Työn aikana heräsi kiinnostus tutkia, kuinka pitkälle nollaluottamuksen periaatteita pystytään hyödyntämään valmiissa tietojärjestelmissä ilman, että elektronisen kulunvalvonnan ja sitä kautta tietoturvan hallintapaneelia annetaan kokonaan ulkoisen palveluntarjoajan käsiin.

Kirjallisuuskatsauksen laatu on tiukasti sidoksissa käytettyihin lähteisiin. Jos tekisin työn nyt uudestaan, sitoisin teorian tiukemmin ISO-27001- ja ISO-27002-standardeihin. Painotin käytännön tietoturvaohjeita, mutta ne jäivät hyvin yleisluontoisiksi. Eri valmistajien laiteasetuksiin olisi ollut mielenkiintoista tutustua, mutta valikoimasta ei pysty nostamaan esille esimerkkejä, jotka varmasti palve-

lisivat tiettyä asiakasyritystä. Käyttöjärjestelmä- ja ohjelmakohtaiset asetukset myös vanhenevat nopeammin kuin muu työssä käytetty materiaali. Toivon osanneeni valita työhön tarpeeksi tuoreita ja luotettavia lähteitä, jotta teoriasisällöstä ja lähdeluettelosta on tuleville opinnäytetöille hyötyä. Luin itsekin työn alkuvaiheissa tiedon perusteita mieluummin vanhoista opinnäytetöistä kuin Wikipediasta. Uskon, että etätyöstä ja sen tietoturvahaasteista löytyy aihetta vielä moneen opinnäytetyöhön.

LÄHTEET

Alexander, D., Finch, A., Sutton, D. & Taylor, A. 2013. Information security management principles. 2nd ed. Swindon, U.K.: BCS Learning & Development Ltd.

BeyondTrust 2020a. Microsoft Vulnerabilities Report 2021. Viitattu 23.5.2021 https://www.beyondtrust.com/assets/documents/BeyondTrust-Microsoft-Vulnerabilities-Report-2021.pdf.

BeyondTrust 2020b. A Guide to Endpoint Privilege Management. White paper. Viitattu 23.5.2021 https://www.beyondtrust.com/assets/documents/BT_WhitePaper_2020_Guide_to_Endpoint_Privilege_Management_v1.pdf.

Borchert, O., Connelly, S., Mitchell, S. & Rose S. 2020. Zero Trust Architecture. Viitattu 20.5.2021 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

Brewer, R. 2016. The six stages of a cyber-attack lifecycle. Viitattu 9.5.2021 https://www.helpnetsecurity.com/2017/03/06/cyber-attack-lifecycle/.

Brown, C., Dog, S., Franklin, J., McNab, N., Voss-Northrop, S., Peck, M., Stidham, B. 2016. Assessing Threats to Mobile Devices & Infrastructure. The Mobile Threat Catalogue. NIST julkaisu NISTIR 8144, luonnos. Viitattu 26.5.2021 https://csrc.nist.gov/CSRC/media/Publications/nistir/8144/draft/documents/nistir8144_draft.pdf.

Check Point Research 2021a. Cyber Security Report 2021. Viitattu 9.5.2021 https://resources.checkpoint.com/cyber-security-resources/cyber-security-report-2021?utm_source=drift-chat&utm_medium=cp-website&utm_campaign=pm_wr_21q1_ww_security_report.

Check Point Research 2021b. March 2021's Most Wanted Malware: IcedID Banking Trojan Enters Top 10 Following Covid-Related Campaign. Viitattu 9.5.2021 https://blog.checkpoint.com/2021/04/13/march-2021s-most-wanted-malware-icedid-banking-trojan-enters-top-10-following-covid-related-campaign/.

CISA=Cybersecurity & Infrastructure Security Agency 2009. Security Tip (ST04-014) Avoiding Social Engineering and Phishing Attacks. Cybersecurity & Infrastructure Security Agency. Viitattu 29.5.2021 https://us-cert.cisa.gov/ncas/tips/ST04-014.

CISA 2011. Security Tip (ST06-003) Staying Safe on Social Networking Sites. Viitattu 30.5.2021 https://us-cert.cisa.gov/ncas/tips/ST06-003.

CISA 2015. Security Tip (ST15-002) Home Network Security. Viitattu 28.5.2021 https://us-cert.cisa.gov/ncas/tips/ST15-002.

CISA 2021a. Enhance web and email security. Viitattu 29.5.2021 https://www.cisa.gov/publication/enhance-email-and-web-security.

CISA 2021b. Cybersecurity Recommendations for Critical Infrastructure Using Video Conferencing. Viitattu 29.5.2021 https://www.cisa.gov/sites/default/files/publications/CISA_Cybersecurity_Recommendations_for_Critical_Infrastructure_Using_Video_Conferencing_S508C.pdf.

Computer Security Resource Centre 2021. Cyber Attack. Viitattu 15.5.2021 https://csrc.nist.gov/glossary/term/Cyber_Attack.

Detwiler, B. 2021. Stop using your work laptop or phone for personal stuff because I know you are. Viitattu 26.5.2021 https://www.zdnet.com/article/stop-using-your-work-laptop-or-phone-for-personal-stuff-because-i-know-you-are/.

Forrest, C. 2016. 1.2 million infected: Android malware 'Hummer' could be biggest trojan ever. Viitattu 9.5.2021 https://www.techrepublic.com/article/1-2-million-infected-android-malware-hummer-could-be-biggest-trojan-ever/.

Franklin, J., Howell, G., Scarfone, K., Souppaya, M. & Sritapan, V. 2021. Guidelines for Managing the Security of Mobile Devices in the Enterprise. NIST julkaisu 800–124 Revision 2, luonnos. Viitattu 26.5.2021 https://doi.org/10.6028/NIST.SP.800-124r2-draft.

Greene, J., Scarfone, K. & Souppaya, M. 2020. ITL BULLETIN MARCH 2020 Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions. Viitattu 26.5.2021 https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf.

Haney, J. 2020. Cybersecurity Awareness Month: Securing Devices at Home and Work. Viitattu 28.5.2021 https://www.nist.gov/blogs/cybersecurity-insights/cybersecurity-awareness-month-securing-devices-home-and-work.

Harjumaa, M. 2021. Maailman vaarallisin haittaohjelma Emotet on saatu kaadettua. Viitattu 9.5.2021 https://yle.fi/uutiset/3-11759178.

Hashim, A. 2020. PowerPoint Vulnerability Allows Mouse-Over Attacks by Installing Malware. Viitattu 30.5.2021 https://latesthackingnews.com/2020/04/15/powerpoint-vulnerability-allows-mouse-over-attacks-by-installing-malware/.

Helle, M. 2004. Etätyö. Helsinki: Edita Publishing Oy.

Hertvik, J. & Raza, M. 2020. Shadow IT Explained: Risks & Opportunities. Viitattu 26.5.2021 https://www.bmc.com/blogs/shadow-it.

Katakri 2020. Tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 29.5.2021 https://um.fi/documents/35732/0/Katakri-2020_201218.pdf.

Kyberturvallisuuskeskus 2019a. Pornokiristyksiä runsaasti liikkeellä – älä usko huijarien väitteitä. Viitattu 30.5.2021 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/pornokiristyksia-runsaasti-liikkeella-ala-usko-huijarien-vaitteita.

Kyberturvallisuuskeskus 2019b. Suojautuminen Microsoft Office 365 –tunnusten kalastelulta ja tietomurroilta. Viitattu 29.5.2021. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Suojautuminen%20Microsoft%20Office%20365%20-tunnusten%20kalastelulta%20ja%20tietomurroilta%20web.pdf

Kyberturvallisuuskeskus 2020a. Tietoturvan vuosi 2020: Kyberturvallisuuskeskuksen vuosikatsaus. Viitattu 2.5.2021 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Tietoturvan-vuosi-2020_210212_FIN.pdf.

Kyberturvallisuuskeskus 2020b. Suojattomien etätyöpöytä- ja verkkoyhteyspalveluiden määrä kasvoi maaliskuussa selvästi. Viitattu 9.5.2020 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/suojattomien-etatyopoyta-ja-verkkoyhteyspalveluiden-maara-kasvoi-maaliskuussa.

Kyberturvallisuuskeskus 2020c. Kyberturvallisuus ja yrityksen hallituksen vastuu 2/2020. Viitattu 16.5.2021 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf.

Kyberturvallisuuskeskus 2020d. Näin suojaudut tietomurrolta. Viitattu 9.5.2021 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-tietomurroilta.

Kyberturvallisuuskeskus 2020e. Kyberturvallisuuden perussanasto. Viitattu 21.5.2021 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/kyberturvallisuuden-perussanasto?toggle=Monivaiheinen%20tunnistautuminen.

Kyberturvallisuuskeskus 2020f. Pienyritysten kyberturvallisuusopas. Viitattu 29.5.2021 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf.

Kyberturvallisuuskeskus 2020g. Neuvoja salasanan hallintasovelluksen käyttöönottoon. Viitattu 27.5.2021 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-salasanan-hallintasovelluksen-kayttoonottoon

Kyberturvallisuuskeskus 2020h VPN-yhteyksien kapasiteetin varmistaminen. Viitattu 27.5.2021 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vpn-yhteyksien-kapasiteetin-varmistaminen.

Kyberturvallisuuskeskus 2020i. Valitse videoneuvotteluratkaisu käyttötarpeen ja tiedon luottamuksellisuuden mukaan. Tietoturva nyt. Viitattu 29.5.2021. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/valitse-videoneuvotteluratkaisu-kayttotarpeen-ja-tiedon-luottamuksellisuuden-mukaan

Kyberturvallisuuskeskus 2021a. Kybersää maaliskuu. Viitattu 9.5.2021 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4_maaliskuu_2021_TLP_WHITE_0.pdf.

Kyberturvallisuuskeskus 2021b. NIS-koordinointi ja viranomaisyhteistyö. Viitattu 18.5.2021 https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/nis-koordinointi-ja-viranomaisyhteistyo?toggle=Digi-infrastruktuuri&toggle=Digitaaliset%20palvelut.

Kyberturvallisuuskeskus 2021c. Näin suojaudut nettihuijaukselta. Viitattu 29.5.2021. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-nettihuijaukselta

Kyberturvallisuuskeskus 2021d. Salasanat haltuun - Kuka käyttää tiliäsi? Viitattu 29.5.2021. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/salasanat-haltuun

Kyberturvallisuuskeskus 2021e. Pilvipalveluiden turvallisuus: Mitä organisaatioiden tulisi huomioida pilvipalveluja hyödyntäessä. Viitattu 29.5.2021 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_tietoturva_organisaatioille.pdf.

Microsoft Docs 2021a. What authentication and verification methods are available in Azure Active Directory? Viitattu 21.5.2021 https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods.

Microsoft Docs 2021b. Microsoft Endpoint Manager documentation. Viitattu 26.5.2021. https://docs.microsoft.com/en-us/mem/

Microsoft 2016. Microsoft Advanced Threat Analytics Datasheet 2016. Viitattu 21.5.2021 https://download.microsoft.com/download/2/8/B/28BAF7CA-AF5F-4BF5-A466-2C52F8CF1134/Azure_Active_Directory_Datasheet_EN_US.pdf.

Microsoft 2021. Implementing a Zero Trust security model at Microsoft. Viitattu 26.5.2021 https://www.microsoft.com/en-us/itshowcase/implementing-a-zero-trust-security-model-at-microsoft.

NCSC 2020. Mobile Device Guidance: Bring Your Own Device (BYOD). National Cyber Security Centre Viitattu 26.5.2021. https://www.ncsc.gov.uk/collection/mobile-device-guidance/bring-your-own-device.

NSA Cybersecurity 2020. Mobile Device Best Practices Viitattu 26.5.2021 https://media.defense.gov/2020/Jul/28/2002465830/-1/-1/0/MOBILE_DEVICE_BEST_PRACTICES_FINAL_V3%20-%20COPY.PDF.

NSA 2018. Best Practices for Securing Your Home Network. Viitattu 28.5.2021 https://media.defense.gov/2019/Jul/16/2002158056/-1/-1/0/Best%20Practices%20for%20Securing%20Your%20Home%20Network%20-%20Copy.pdf.

Opetus- ja kulttuuriministeriö, Poliisiammattikorkeakoulu & JYVSECTEC 2021. Kyberrikos on poliisiasia. Viitattu 18.5.2021 https://polamk.fi/documents/25254699/34112600/Opas_Kyberrikos+on+poliisiasia.pdf/24ef8ce6-d86c-bf3f-ea66-d8f414dae212/Opas_Kyberrikos+on+poliisiasia.pdf?t=1616740405258.

Perakovic, D., Husnjak, S. & Cvitic, I. 2014. Comparative analysis of enterprise mobility management systems in BYOD environment. Viitattu 27.5.2021 https://www.fpz.unizg.hr/ikp/upload/perakovic_husnjak_cvitic.pdf.

Ping Identity 2021. Enable seamless, secure access with adaptive authentication and authorization. Viitattu 20.5.2021 https://www.pingidentity.com/content/dam/ping-6-2-assets/Assets/technical-briefs/en/3271-adaptive-authentication-and-authorization.pdf.

Poliisi 2021. Kyberrikokset. Viitattu 18.5.2021 https://poliisi.fi/kyberrikokset.

Ponemon Institute 2020. Cybersecurity in the Remote Work Era: A Global Risk Report 2020. Viitattu 2.5.2021 https://www.keeper.io/hubfs/PDF/Cybersecurity%20in%20the%20Remote%20Work%20Era%20-%20A%20Global%20Risk%20Report.pdf.

Rikoslaki 19.12.1889/39

Sanastokeskus TSK 2021a. Haittaohjelma. Viitattu 9.5.2021 https://termipankki.fi/tepa/fi/haku/haittaohjelma.

Sanastokeskus TSK 2021b. Mainosohjelma. Viitattu 9.5.2021 https://termipankki.fi/tepa/fi/haku/mainosohjelma.

Sanastokeskus TSK 2021c. Nollapäivähaavoittuvuus. Viitattu 9.5.2021 https://termipankki.fi/tepa/fi/haku/nollap%C3%A4iv%C3%A4haavoittuvuus.

Sanastokeskus TSK 2021d. Kyberhyökkäys. Viitattu 19.5.2021 https://termipankki.fi/tepa/fi/haku/kyberhy%C3%B6kk%C3%A4ys.

Sanastokeskus TSK 2021e. Kybertoimintaympäristö. Viitattu 19.5.2021 https://termipankki.fi/tepa/fi/haku/kybertoimintaymp%C3%A4rist%C3%B6.

Sarvepalle, V. 2019. VPN - A Gateway for Vulnerabilities Carnegie Mellon University. Viitattu 27.5.2021 https://insights.sei.cmu.edu/blog/vpn-a-gateway-for-vulnerabilities/

Scarfone, K., Sexton, M. & Souppaya, M. 2007. Guide to Storage Encryption Technologies for End User Devices. NIST:in julkaisu 800–111. Viitattu 26.5.2021 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf.

Scarfone, K. & Souppaya, M. 2016. Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. NIST:in julkaisu 800–46, uudistettu versio 2. Viitattu 26.5.2021 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf.

Summerson, C. 2017. What Is USB Debugging, and Is It Safe to Leave It Enabled on Android? Viitattu 26.5.2021 https://www.howtogeek.com/258788/what-is-usb-debugging-and-is-it-safe-to-leave-it-enabled-on-android/.

Tietosuojavaltuutetun toimisto 2021a. Tietoturvaloukkaukset. Viitattu 9.5.2021 https://tietosuoja.fi/tietoturvaloukkaukset.

Tietosuojavaltuutetun toimisto 2021b. Henkilötietojen käsittely. Viitattu 18.5.2021 https://tietosuoja.fi/henkilotietojen-kasittely.

Tietosuojavaltuutetun toimisto 2021c. Rekisteröidyn oikeudet. Viitattu 18.5.2021 https://tietosuoja.fi/rekisteroidyn-oikeudet.

Tietosuojavaltuutetun toimisto 2021d. Henkilötietojen siirrot Euroopan talous-alueen ulkopuolelle 2021. Viitattu 18.5.2021 https://tietosuoja.fi/henkilotietojen-siirrot-etan-ulkopuolelle.

Tietosuojavaltuutetun toimisto 2021e. Tietojen kalasteluun perustuvat tietoturva-loukkaukset. Viitattu 18.5.2021 https://tietosuoja.fi/tietojenkalastelu.

Työmarkkinakeskusjärjestöt 2005. Sopimus etätyötä koskevan puitesopimuksen täytäntöönpanosta. Viitattu 16.5.2021 https://www.kt.fi/sites/default/files/media/document/etatyosta-sovittaessa-huomioon-otettavaa.pdf.

Vahti = Valtionhallinnon tietoturvallisuuden johtoryhmä 2002. Valtionhallinnon etätyön tietoturvallisuusohje. Viitattu 16.5.2021 https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_3_2002.pdf.

Vahti 2009. Lokiohje. Viitattu 23.5.2021 https://www.suomidigi.fi/sites/default/files/2020-06/pdf_3_2009.pdf.

Vahti 2010. Sosiaalisen median tietoturvaohje. Viitattu 29.5.2021 https://www.suomidigi.fi/sites/default/files/2020-06/Ohje_4_2010_etusivu_ohjepdf.pdf.

Vahti 2013. Päätelaitteiden tietoturvaohje. Viitattu 26.5.2021 https://www.suomidigi.fi/sites/default/files/2020-06/VAHTI_5_2013_pdf.

Vahti 2017. Tietoturvapoikkeamatilanteiden hallinta. Viitattu 17.5.2021 https://www.suomidigi.fi/sites/default/files/2020-06/VM_8_2017.pdf.

Zerotier 2021. Manual. Viitattu 27.5.2021 https://www.zerotier.com/manual/.