Yritysten tietoturvallisuus henkilökunnan näkökulmasta: Tietoturvaopas henkilöstölle

Sanni Lavrenz

Haaga-Helia ammattikorkeakoulu

Tradenomi

Amk-opinnäytetyö

2024

Tiivistelmä

Tekijä
Sanni Lavrenz

Tutkinto
Tradenomi

Raportin/Opinnäytetyön nimi
Yritysten tietoturvallisuus henkilökunnan näkökulmasta: Tietoturvaopas henkilöstölle

Sivu- ja liitesivumäärä
27 + 7

Tämä toiminnallinen opinnäytetyö käsittelee operatiivisen toiminnan tietoturvallisuutta yrityksissä henkilökunnan näkökulmasta. Lähes jokaisessa yrityksessä käsitellään tietoa sähköisessä muodossa jollain tasolla ja sähköisen tiedon, eli datan, käsittely luo aina mahdollisuuden tietoturvauhkille. Monet uhat voitaisiin melko pienilläkin muutoksilla ennaltaehkäistä tarjoamalla henkilökunnalle säännöllistä tietoturvakoulutusta ja muuttamalla heidän toimintatapojaan päivittäisessä, operatiivisessa toiminnassaan. Tässä työssä paneudutaankin siihen, mitä on tietoturva, millaisia tietoturvauhkia datan käsittely voi aiheuttaa yrityksille ja millaisia keinoja sen ennaltaehkäisyyn henkilöstön näkökulmasta on.

Työn tietoperustassa käsitellään ensin tietoturvallisuutta terminä sekä tarkastellaan tiedon arvoa. Aihe rajautuu tämän jälkeen keskeisimpiin yritysten tietoturvauhkiin, uhkien toteutumisen seurauksiin yritystoiminnassa sekä lopulta siihen, millaisilla keinoilla voitaisiin ennaltaehkäistä tietoturvauhkia henkilökunnan operatiivisessa toiminnassa. Kaiken keskiössä ovat ihmiset ja tietoperusta onkin rajattu koskemaan tietoturvaa henkilökunnan näkökulmasta, jonka vuoksi työssä ei syvennytä tietoturvauhkien tai ennaltaehkäisevien toimien osalta teknisiin ratkaisuihin.

Opinnäytetyön toiminallisessa osuudessa laadittiin tietoturvaopas henkilökunnalle, jota ei ole sidottu mihinkään tiettyyn toimialaan, eikä oppaan lukijalta vaadita tietoteknistä osaamista tai -taustaa. Opas pyrkii toimimaan tietoturvaa lisäävänä ohjeistuksena toimialasta riippumatta työntekijän päivittäisten operatiivisten toimien kautta. Opasta voidaankin hyödyntää erinomaisesti esimerkiksi sellaisissa yrityksissä, joissa varsinaista tietoturvakoulutusta ei ole annettu henkilökunnalle tai tietoturvakoulutuksesta on kulunut useampi vuosi ja tietopohjaa tietoturvasta olisi hyvä päivittää. Opas neuvoo ja ohjeistaa operatiivisessa työssä, eikä syvenny tietoverkkoihin, it-infrastruktuuriin tai muihinkaan sellaisiin teknisiin ratkaisuihin, joilla voidaan suojautua kyberhyökkäyksiltä. Tämän opinnäytetyön, ja erityisesti oppaan, tavoite oli parantaa henkilökunnan tietoturvaosaamista sekä edesauttaa yrityksiä pienentämään riskiä kohdata mahdollisia tietoturvauhkia.

Asiasanat
Tietoturvallisuus, henkilöstön tietoturvakoulutus, tietoturvaopas

Sisällys

1 Johdanto

”Ihminen on usein tietoturvan heikoin lenkki” totesi Suomen Yrittäjien digi- ja koulutusasioiden päällikkö Joonas Mikkilä Kauppalehden tekemässä artikkelissa keväällä 2022, jossa käsiteltiin pk-yrityksille tehtyä yrittäjägallupia tietoturvaan liittyen. Samaisessa kyselyssä selvisi, että 61 prosenttia suomalaisista yrityksistä koki esteitä tietoturvassaan ja suurimpia haasteita aiheuttivat sekä osaamisen puute että tietoturvaan liittyvät kustannukset. Uutisessa todettiin, että paras ratkaisu tietoturvan ennaltaehkäisyyn olisi henkilöstön tietoturvaosaamisen lisääminen sekä koulutus ja paras ratkaisu haasteeseen olisi tarjota käytännönläheisiä tietoturvakoulutuksia sekä oppaita henkilöstölle. Jo olemassa olevien oppaiden tämänhetkisenä haasteena Mikkilä piti sitä, että oppaiden pitäisi pystyä vastaamaan paremmin yritysten tarpeisiin. (Tervola 2022.) Kyseinen uutinen tiivistää kokonaisuudessaan syyn ja motivaation tämän opinnäytetyön luomiseen.

Teknologiaa on lähes kaikkialla ja kun lähes jokaisessa yrityksessä käsitellään tietoa sähköisesti, tarkoittaa se myös sitä, että riski tiedon korruptoitumiselle, muuttumiselle, vuotamiselle tai menetykselle on olemassa (Traficom 2023b). Tietoturvallinen työkulttuuri saatetaan ajatella pitkälti teknilliseltä kannalta, jolla viitataan verkon turvallisuuteen, virustorjuntoihin tai palomuureihin, mutta suuri osa yrityksen tietoturvallisuutta ovat ihmiset. Tiedusteltuani laajasta lähipiiristäni sitä, kuinka moni työelämässä oleva henkilö oli saanut viimeisen kahden vuoden aikana työpaikallaan tietoturvakoulutusta, olivat vastaukset huolestuttavia. Vain muutama oli saanut tietoturvakoulutusta ja osalla siitä oli jo yli kaksi vuotta aikaa. On vastuutonta olettaa, että ihmiset, jotka käsittelevät töissään suurtakin määrää yritykselle erittäin tärkeää dataa ja ovat näin ollen vastuussa tietoturvallisuudesta, osaisivat toimia oikein tietoturvauhan kohdatessaan, mikäli eivät ole saaneet joko lainkaan, tai useaan vuoteen, tietoturvakoulutusta. Tämä toimi kimmokkeena tämän opinnäytetyön aiheeseen, jonka tarkoituksena jakaa tietoisuutta tietoturvallisesta työkulttuurista, ohjeistaa henkilökuntaa ja auttaa yrityksiä toimimaan tietoturvallisemmin toimialasta riippumatta.

Tämä toiminallinen opinnäytetyö käsittelee yritysten operatiivisen toiminnan tietoturvaa henkilökunnan näkökulmasta katsottuna. Työ sisältää tietoperustan tietoturvaan liittyen, jossa pohditaan sitä, mitä tietoturvallisuus tarkoittaa ja miksi tieto on arvokasta. On vaikeaa motivoida ketään toimimaan tietoturvallisemmin, mikäli ei ymmärretä sitä, mitä suojellaan. Lisäksi opinnäytetyössä käsitellään yritysten yleisimpiä tietoturvauhkia ja kerrotaan mahdollisten uhkien seurauksista yritystoiminnassa. Työssä pohditaan myös tulevaisuuden näkymiä tietoturvauhkien osalta ja tietoperustan lopussa käydään läpi ennaltaehkäiseviä toimia ja kerrotaan keinoja siihen, millä tavoin henkilökunta voi parantaa työympäristönsä tietoturvallisuutta. Koko opinnäytetyö on rajattu aiheeltaan käsittelemään tietoturvaa yleisellä tasolla yritystoiminnan kautta, toimialasta riippumatta ja henkilökunnan

näkökulmasta katsottuna. Tässä työssä ei siis syvennytä teknisiin ratkaisuihin tietoliikenteen, it-infrastruktuurin tai muiden vastaavien teknisten osa-alueiden osalta.

Opinnäytetyön toiminnallisessa osuudessa on luotu tietoturvaopas yritysten henkilökunnalle. Tietoturvaopas on tarkoitettu henkilökunnalle koulutusmateriaaliksi ja oppaan tavoitteena onkin parantaa ja päivittää henkilökunnan tietoturvaosaamista ja toimia näin ollen myös apuna yrityksille pienentäen tietoturvariskien mahdollisuuksia. Oppaaseen on koottu konkreettisia toimia ja neuvoja, joita noudattamalla päivittäiset, operatiiviset toimet muuttuvat tietoturvallisimmaksi tehdä. Opasta ei ole sidottu mihinkään tiettyyn toimialaan, eikä sitä lukiessa tarvitse olla tietoteknistä osaamista tai -taustaa.

Opinnäytetyön tavoitteena on lisätä tietoisuutta tietoturvallisuudesta myös suuressa kokonaiskuvassa alati muuttuvassa tilanteessa ja etenkin tämänhetkisessä maailman poliittisessa tilanteessa. Vuonna 2022 alkanut Ukrainan sota on lisännyt tietoturvauhkien määrää Suomessa ja uhat ovat monimutkaistuneet. Valtionneuvoston tuottaman raportin mukaan kyberhyökkäyksiä kohdistetaan valtion- ja kuntatason toimijoille samoin kuin myös muualle elinkeinoelämään, jolloin yritysten rooli julkisen- ja yksityisen sektorien yhteistoiminnassa on muuttunut tärkeämmäksi ja nostanut merkitystään. Raportissa korostetaan, että on entistä tärkeämpää ymmärtää uhkien aiheuttamat riskit koko arvoketjulle sekä saumakohdille, jotka on myös tunnistettava entistä paremmin. (Valtioneuvosto 2022, 32). Tekoälyn ja muun teknologian kehittyessä tietoturvahyökkäyksiä pyritäänkin jatkuvasti viemään hienostuneempaan suuntaan. (Aksela, Marchal, Patel, Rosenstedt & WithSecure 2022.) Kuten it-alalla yleisestikin, tieto vanhenee jatkuvasti ja on välttämätöntä seurata ja kouluttautua säännöllisesti, jotta pysyy kehityksessä mukana. Tämän vuoksi on myös tärkeää tarjota henkilökunnalle säännöllistä tietoturvakoulutusta, jotta toimintamallit pysyvät kehityksen perässä ja tietoturvauhkien ennaltaehkäisy olisi helpompaa.

2 Yritysten tietoturvallisuus

Tämä opinnäytetyö käsittelee tietoturvallisuutta yritysten operatiivisessa toiminnassa henkilökunnan näkökulmasta tarkasteltuna. Kun määritellään operatiivista toimintaa, Bäckström (2017) määrittelee operatiivisen puolen yritysmaailmassa keskittymään varsinaiseen toimintaan ja operatiivinen johtaminen keskittyy johtamaan arkista työtä sovitun strategian mukaisesti. Tällä viitataan siis siihen, kuinka suoritamme päivittäistä työtämme. Tietoturvallisuus voidaan arkikielessä puolestaan sekoittaa herkästi kyberturvallisuuteen, vaikka todellisuudessa tietoturvallisuudella tarkoitetaan tiedon turvaamista laajemmin. Tietoturvallisuus kattaa verkkoympäristöjen lisäksi myös fyysistä turvallisuutta esimerkiksi rakennusten suojaamisen osalta. Tietoturvallisuus pyrkii siis sekä suojaamaan dataa, että pitämään sen fyysisesti turvassa. Kyberturvallisuus puolestaan koskee vain verkkoympäristöjä, joilla suojataan dataa, järjestelmiä tai laitteita. Kyberturvallisuutta voidaankin jopa ajatella osana tietoturvallisuutta, vaikka eriytettyinä niiden uhat ovatkin hieman erilaisia. Tietoturvallisuutta tai kyberturvallisuutta ei kuitenkaan pidä sekoittaa tietosuojaan, joka puolestaan viittaa henkilötietojen lakeja noudattavaan käsittelyyn ja keräämiseen. (F-Secure 2023c.)

Kun operatiivinen toiminta yhdistetään tietoturvallisuuteen, voidaan ajatella esimerkiksi yksittäistä työpäiväesimerkkiä, jossa saavutaan työpaikalle, käynnistetään päätelaitteet, järjestelmät ja sovellukset, vastaillaan sähköposteihin, päivitetään esim. LinkedIn-profiilia, ollaan palaverissa, käydään lounaalla välissä ja päivän päätteeksi suljetaan koneet ja lopetetaan työt. Työpäiväesimerkki kuulostaa varsin automaattiselta ja yksiselitteiseltä toiminnalta, mutta moni ei kuitenkaan välttämättä tule ajatelleeksi, että jokaiseen edellä mainittuun prosessiin liittyy toimintoja, jotka vaikuttavat merkittävästi yrityksen tietoturvallisuuteen. Tietoturvallisuus ei aina vaadi henkilöstöltä suuria tekoja, mutta kun jokaisessa toiminnon prosessissa tai -saumakohdassa otetaan huomioon tiettyjä seikkoja, voi koko yrityksen tietoturvallisuus parantua huimasti.

2.1 Tietoturvallisuus terminä

Tietoturvallisuudella tarkoitetaan tiedon turvaamista hallinnollisilla ja teknisillä toimilla normaali- ja poikkeusoloissa (Opetushallitus 2023). Tietoturvan tarkoitus on suojata tietoa, eli taata, että tieto on, ja pysyy, eheänä, luottamuksellisena ja käytettävänä. Eheällä tiedolla viitataan siihen, ettei tietoa pysty muokkaamaan kukaan sellainen taho tai henkilö, jolla ei siihen oikeuksia ole. Tällä varmistetaan se, ettei esimerkiksi pankeissa asiakkaiden tilien saldot muutu kontrolloimattomasti. Tiedon luottamuksellisuudella viitataan siihen, että tieto on nimensä mukaisesti luottamuksellista. Pankki-esimerkkiin viitaten tämä turvaa sen, ettei tileille pääse kukaan sellainen ulkopuolinen taho, kenellä ei sinne pääsyoikeuksia ole. Eheyden ja luottamuksellisuuden lisäksi tiedon tulee olla käytettävissä. Käytettävyys tarkoittaa, että palvelu ja sen sisältämät tiedot ovat käytettävissä, hyödynnettävissä ja asiakkaan saatavilla palvelulupausten mukaisesti. Pankkiesimerkillä käytettävyydellä

tarkoitetaan sitä, että pankkien asiakkailla tulee olla pääsy tileilleen siten, kuten yrityksen palvelulupaus on luvannut. Mikäli pankki lupaa asiakkailleen ympärivuorokautisen pääsyn tileilleen, tulee tämän myös toteutua. (Traficom 2023a.)

Eheyden, luotettavuuden ja käytettävyyden lisäksi on myös muita tietoturvan osa-alueita, joilla määritellään tietoturvallisuutta. Opetushallitus (2023) mainitsee listassaan pääsynvalvonnan, kiistämättömyyden, osapuolten todentamisen sekä tunnistamisen. Ensimmäisellä, eli pääsynvalvonnalla, tarkoitetaan sitä, että käyttäjien pääsyä palveluun, jossa tieto on, rajoitetaan sekä valvotaan. Kiistämättömyydellä viitataan siihen, ettei henkilö voi kiistää osallistumistaan tapahtuneeseen, mihin hänet voidaan liittää esimerkiksi jonkin käyttäjätunnuksen nojalla. Kiistämättömyys on siis todisteiden luomista sen suhteen, ettei yksikään osapuoli voi kiistää osuuttaan liittyen johonkin tietoon tai esimerkiksi sen muokkaamiseen. Muun muassa lokitietojen seuraaminen auttaa tunnistamaan tahon, joka on nähnyt, käsitellyt tai muokannut dataa. Vaihtoehtoisesti myös pelkkä sähköpostin lähettäminen toiselle henkilölle voidaan tulkita siten, että sekä lähettäjällä että vastaanottajalla on ollut pääsy nähdä viestin sisältö. Tätä ajatellaan juridisena sitovuutena eikä tapahtunutta voida kiistää. (Opetushallitus 2023.)

Osapuolten todentamisesta puhuttaessa tulee ottaa huomioon kaksi asiaa; tunnistaminen sekä todentaminen. Tunnistanen tarkoittaa henkilön tai järjestelmän luotettavaa tunnistusta ja todentaminen viittaa kohteen ominaisuuteen, eli joko siihen, mitä kohteella on hallussaan tai mitä kohde tietää, esimerkkejä tällaisista ovat muun muassa pin-koodi sekä sormenjälki. Vahva todentaminen onkin näiden kahden menetelmän, eli tunnistamisen ja todentamisen, yhdistämistä. Vahva todentaminen perustuu prosessiin, jossa henkilö tai asiakasjärjestelmä on tuotu osaksi tunnistus- ja todennusjärjestelmää ja vahva todentaminen painottuukin enemmän identiteettijärjestelmään, eikä niinkään teknisiin prosesseihin. Esimerkkinä kulkukorttiin liitetty järjestelmä, joka pitää sisällään tiedon käyttäjästä, eli tunnistaa käyttäjän. Kun kulkukorttia näytetään oikealle järjestelmälle ja syötetään pin-koodi, tapahtuu kohdentaminen ja ovi avautuu. Vaikka tunnistaminen on mainittu osana osapuolten todentamista, on tärkeää myös määritellä tunnistaminen itsenäisesti. Tällä tarkoitetaan menettelyä, jolla yksilöidään tai tunnistetaan jokin kohde. Kohde voi tarkoittaa järjestelmää tai käyttäjää, esimerkiksi työkaveria. Ideana on, että kun jokin tietty henkilö tunnistetaan työkaveriksi ja tiedetään hänen kuuluvan osaksi työyhteisöä, on tunnistaminen tällöin toteutunut onnistuneesti. (Opetushallitus 2023.) Tällä pyritään siis ennaltaehkäisemään vieraiden ihmisten tai väärien ohjelmien pääsyä ja murtautumista yrityksen ympäristöön.

Kategorisesti Opetushallitus (2023) jakaa tietoturvallisuuden kahdeksaan eri osaan; hallinnollinen ja organisatorinen tietoturvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus sekä käyttöturvallisuus.

Tässä opinnäytetyössä käsitellään pääasiallisesti vain hallinnollista ja organisatorista tietoturvaa ja siinäkin keskitytään tarkemmin vain henkilöstölle tehtävään viestintään. Tästä syystä seuraavissa kappaleissa ei ole avattu tarkemmin muita kategorioita. On kuitenkin tärkeää ymmärtää tietoturvallisuuden laajuus ja se, että henkilöstön vastuu kaikissa kategorioissa on merkittävä, mutta muut osa-alueet vaativat henkilöstöltä enemmän ict-alan tuntemusta voidakseen turvata yrityksen tietoturvallisuutta.

Hallinnollisella ja organisatorisella tietoturvallisuudella tarkoitetaan tietoturvallisuuden johtamista, eli sitä, että yritys laatii ja sitoutuu laatimaansa tietoturvasuunnitelmaan. Hallinnollisessa tietoturvallisuudessa kartoitetaan nykyisen tietoturvallisuuden taso, laaditaan riskiarviointeja sekä laaditaan mahdolliset korjaus- ja kehitysehdotukset tietoturvallisuuden parantamiseksi sekä tehdään suunnitelmat riskien varalle. Suunnitelman ja strategian tekeminen on yrityksen johdon vastuulla ja tärkein ja kriittisin osuus on strategian jalkauttaminen henkilökunnalle, jotta henkilökunta osaa toimia laaditun tietoturvasuunnitelman mukaisesti. (Opetushallitus 2023.) Tämän opinnäytetyön tarkoitus onkin avata keskeisimpiä toimintatapoja, joita yritys voi ottaa huomioon laatiessaan suunnitelmaa.

On erittäin tärkeää, että tietoturvaohjeistus on selkeää ja käytännönläheistä, jotta jokainen osaa toimia laaditun suunnitelman mukaan operatiivisessa toiminnassaan tai mahdollisen tietoturvapoikkeaman kohdatessaan. Lisäksi viestinnän tulee olla kaksisuuntaista, jotta mahdolliset poikkeamat osataan korjata. Onkin siis tärkeää, että henkilöstö ilmoittaa poikkeamista myös toiseen suuntaan. (Ryhänen 12.7.2020.)

2.2 Tiedon arvo yrityksille

On hyvä ymmärtää tiedon arvo, sillä muutoin on hankalaa motivoida ketään toimimaan tietoturvallisemmin, mikäli ei ymmärretä kausaliteettia yritysten tietomurroille. Tieto on arvokasta ja internetin pimeille markkinoille päätyvät, varastetut tietokannat voivat olla hinnaltaan erittäin arvokkaita. Yritykset ovat tässä suhteessa erityisen hyviä kohteita, sillä niiden tietokannat ovat isoja ja suuresta massasta esimerkiksi käyttäjätietoja, salasanoja tai muita luottamuksellisia tietoja maksetaan paljon rahaa. (Nielsen 1.7.2023.) Yksittäisille ihmisille, eli yrityksen asiakkaille, tällaiset murrot ovat haitallisia, sillä uhkana tietoturvaloukkauksesta on identiteettivarkauksia, petoksia, henkilötietojen valvomiskyvyn menettämistä, maineen vahingoittumista tai muutoin salassa pidettävän tiedon paljastumista (Tietosuojavaltuutetun toimisto 2023a). Onkin varsin ymmärrettävää, että asiakas, joka on luottanut tietoja yrityksen haltuun ja luottanut siihen, että luovutetut tiedot ovat turvassa, menettää luottamuksensa yrityksen toimintaan tietoturvaloukkauksen kohdatessaan.

Arvokasta tietoa on kaikkialla ja dataa kerätäänkin valtavasti. Asiakkaan näkökulmasta katsottuna monille yrityksille joutuu luovuttamaan henkilötietoja, pankki- tai luottokorttitietoja. Esimerkiksi S-

Ryhmä, jossa monella henkilöllä on pankkitili, seuraa ostokäyttäytymistä ja onkin mukana mahdollistamassa Helsingin ja Tampereen yliopistojen teettämää tutkimusta, jossa tutkitaan suomalaisten ostokäyttäytymistä ruokaostosten, ruokavalioiden ja ruoan valintojen osalta (Tampereen yliopisto 2023). Harva tulee ajatelleeksi, kuinka paljon tietoa yksittäisestä henkilöstä kerätään hänen asioidessaan ruokakaupassa, hotellissa tai bensa-asemalla ja kerätessään bonuksia näyttämällä asiakaskorttiaan. Pelkästään S-Ryhmä omaa valtavan massadatan suomalaisista talouksista, henkilötiedoista sekä ostoskäyttäytymisistä ja nämä tiedot ovat myös valtavan arvokkaita. Ei pelkästään se, että tätä tietoa voidaan hyödyntää mm. mainonnassa laillisella puolella, mutta sen arvo on myös valtava pimeillä markkinoilla, laittomalla puolella. Tällaisen tiedon vuotaminen, murtaminen, korruptoituminen tai muuttuminen on valtava mainehaitta yrityksille ja voi johtaa asiakassuhteiden päättymisiin ja aiheuttaa jopa pahimmassa tapauksessa konkurssin, kuten kävi vuonna 2021 psykoterapiakeskus Vastaamolle valtavan tietomurtoskandaalin takia (Yle 2021).

Tietoturvallinen työilmapiiri on yrityksille äärimmäisen tavoiteltava tila, sillä tällä varmistetaan organisaation arkaluonteisen ja tärkeän tiedon suojaaminen. Se luo yritykselle luottamusta ja antaa lisäarvoa asiakkaiden näkökulmasta. Integroimalla tietoturvallisuuden osaksi jokapäiväistä operatiivista toimintaa varmistetaan se, ettei henkilöstön puolelta tule tehtyä turhia, vältettävissä olevia virheitä esimerkiksi puutteellisen koulutuksen vuoksi. (Ryhänen 12.7.2020.)

2.3 Yritysten yleisimmät tietoturvauhat ja niiden seuraukset

Lähes jokainen yritys käsittelee nykypäivänä jotain tietoa sähköisesti. Tähän sisältyy aina riski tietoturvauhkasta ja riskin toteutuessa voi uhkana olla tärkeän, salaisen tiedon menettämistä, tiedon muokkaamista epätodeksi ja sen siirtämistä tai levittämistä, mainehaittoja tai häiriöitä palveluissa. (Traficom 2023b.) Kaikkea tätä vaikeuttaa se, että hienovaraisesti tehdyn tietoturvahyökkäyksen havaitsemiseen saattaa kulua pahimmassa tapauksessa useita viikkoja - jopa kuukausia. On tärkeää tietää ja tiedostaa mahdolliset tietoturvauhat sekä niiden tavoitteet, jotta uhkia on helpompi ennaltaehkäistä omassa operatiivisessa työssä. (If 2023.) Seuraavissa kappaleissa käsitellään muutamia yleisimpiä tietoturvauhkia työnantajien näkökulmasta. Tässä työssä ei paneuduta kuitenkaan uhkien tekniseen puoleen, vaan keskitytään painottamaan haittaa, joka yritykselle syntyy mahdollisten uhkien toteutuessa.

Puhuttaessa kyberhyökkäyksestä tarkoitetaan tällä tietomurtoa, haittaohjelman levittämistä, palvelunestohyökkäystä tai luvatonta murtautumista it-ympäristöön. Tunkeutumista luvattomasti johonkin järjestelmään kutsutaan myös termillä hakkerointi. Hakkerointi on kuitenkin hyvä erottaa termistä krakkerointi, sillä vaikka näillä kahdella on samat periaatteet, niillä on eri tavoite. Hakkerit toimivat usein jonkun yrityksen hyväksi ja koittavat tehdä tietoturvahyökkäyksiä parantaakseen yrityksen tietoturvaa, kun krakkerit pyrkivät hyökkäyksillään varastamaan tai vaurioittamaan tietoa. Krakkerin

toiminta voi onnistuessaan aiheuttaa yritykselle monenlaista haittaa; tietoa tai järjestelmää voidaan vahingoittaa, dataa voidaan poistaa tai sitä voidaan yrittää myydä eteenpäin. (If 2023.) Puhekielessä hakkeroinnin ja krakkeroinnin rinnalle ovat yleistyneet myös termit ”mustahattu- ja valkohattuhakkerit”, joissa valkohattuhakkereilla viitataan hakkereihin ja mustahattuhakkereilla krakkereihin (Kaspersky 2023).

Hakkeroinnin lisäksi puhutaan myös tietojenkalastelusta (eng. phising). Tietojenkalastelua on ollut jo pitkään ja sen yleisyyttä selittää sen monipuolisuus. Tietojenkalastelua voidaan suorittaa monessa eri ympäristössä joko puhelimitse, sähköpostitse tai esimerkiksi sosiaalisen median kautta ja sen idea on tekeytyä tunnetuksi tahoksi, jonka varjolla koitetaan saada kohde luovuttamaan luottamuksellista tietoa. (If 2023.)

Haittaohjelma (eng. Malware) on nimensä mukaisesti ohjelma, joka aiheuttaa haittaa järjestelmään tai it-ympäristöön. Haittaohjelmiin lukeutuvat mm. botit, madot, troijalaiset ja virukset. Madot ja virukset muistuttavat toisiaan. Molempien tarkoitus on levitä koneesta toiseen tekemällä itsestään kopioita, erona kuitenkin se, ettei mato tarvitse tähän isäntäohjelmaa. Troijalainen tunkeutuu koneeseen naamioitumalla joksikin muuksi, viattomaksi ohjelmaksi tai sen osaksi ja päästessään sisälle käynnistää viruksen tai muun haittaohjelman. Botteja (eng. bot) puolestaan hyödynnetään usein palvelunestohyökkäyksissä. (If 2023.) Palvelunestohyökkäyksissä hyökkääjä ottaa valtaansa suuren määrän laitteita, eli botteja, jotka ohjataan kohdistamaan liikennettä haluttuun palveluun aiheuttaen tietoliikennetulvan. Kun kohde kohtaa odottamattoman suuren määrän liikennettä, sen palvelimet kaatuvat ja yrityksen palvelu lopettaa toiminnan tai sen käyttö hidastuu (Poliisi 2023). Haittaohjelmien häiriöt yrityksen näkökulmasta ovat siis sellaisia, jotka lamaannuttavat yrityksen toimintaa; verkkosivuilla voi olla hitautta, jokin palvelu tai laite ei toimi, tietoa voi puuttua, verkkosivujen sisältö on muuttunut tai verkkosivut voivat kaatua kokonaan. Henkilökunnan näkökulmasta tarkasteltuna haittaohjelmien torjuntaan paras ennaltaehkäisy on lisätä tietoutta tietojenkalastelusta, sillä se on yksi yleisimmistä tavoista levittää edellä mainittuja haittaohjelmia. (F-Secure 2023d.)

Tietojenkalastelu tarkoittaa nimensä mukaisesti tietojenkalastelua. Yleisemmin hyökkääjä luo identtisen, tai lähes identtisen, verkkosivun haluamastaan sivustosta, jossa kerätään kohteilta tietoa; joko tunnuksia ja salasanoja, pankkitunnuksia tai muuta arkaluontoista tietoa. Hyökkääjä lähettää linkin esimerkiksi yrityksen sähköpostiin siten, että se näyttää tulevan luotettavalta taholta ja houkuttelee saatekirjeessä uhria klikkaamaan linkkiä tai avaamaan liitteen ja syöttämään tietonsa huijaussivustoonsa. Mikäli asiakas toimii halutulla tavalla, saa hyökkääjä käyttöönsä sivulle syötetyt tiedot ja pääsee hyödyntämään niitä. Tällaisissa tapauksissa hyökkääjä voi saada haltuunsa

erittäin paljon dataa, jota voidaan hyödyntää petoksiin, kiristyksiin, väärinkäyttöön tai datan myymiseen. Yritykselle tällainen on äärimmäisen ongelmallista, sillä yrityksen tulee vahingon sattuessa pystyä osoittamaan, mitä dataa hyökkääjä on saanut sekä mihin kaikkialle saadulla datalla voidaan päästä. (Tietosuojavaltuutetun toimisto 2023b.) Lisäksi tällaisesta saattaa aiheutua yritykselle suurta mainehaittaa sekä asiakassuhteiden päättymistä.

Tärkein ennaltaehkäisy haittaohjelmien torjunnassa tai tietojen kalastelussa on ymmärtää, ettei mihinkään päätelaitteeseen tulleita epäilyttäviä viestejä tai sähköposteja, jotka sisältävät linkkejä tai liitteitä, kannata avata. Työnantajan antamat päätelaitteet ovat tarkoitettu työnteolle, eikä ylimääräisillä verkkosivuilla tulisi vierailla. Työtä tulisi lisäksi tehdä vain niille tarkoitetuilla laitteilla. Kalasteluviesteille tyypillistä voivat lisäksi olla huono kieliasu, kirjoitusvirheet tai asian kiireellisyys, mutta näissäkin asioissa tietojenkalastelun suhteen on tultu valtavasti eteenpäin ja viestit voivatkin olla erittäin uskottavia. Tärkeintä on luottaa omaan vaistoon ja kyseenalaistaa erikoisia lähestymistapoja tahoilta, jotka eivät normaalisti lähettäisi tekstiviestiä tai sähköpostia, joka sisältäisi linkin tai liitteen. (F-Secure 2023e)

2.3.1 Tietoturvauhkien kehittyminen ja tulevaisuus

Teknologioita käsittelevien opinnäytetöiden haasteena on niiden nopea tiedon vanhentuminen. Tämän vuoksi onkin tärkeää pohtia myös mahdollisia tulevaisuuden näkymiä tai trendejä tietoturvauhkien osalta, jotta yritysten olisi helpompi varautua tietoturvauhkiin myös tulevaisuudessa. Tulevaisuuden riskeistä puhuttaessa esiin nousee erityisesti tekoäly ja sen mahdollistamat, uudet keinot hyödyntää ja tehostaa tietoturvahyökkäyksiä.

Tekoäly mahdollistaa tulevaisuudessa entistä paremman kohdentamisen tietojenkalastelun osalta. Yritysten ja henkilöstön näkökulmasta tekoälyn avustamaa tietojenkalastelua voidaan kohdistaa paremmin tietyillä perusteilla valittuihin henkilöihin esimerkiksi tietyn statuksen tai korkean profiilin osalta. Kun halutut, tietyn profiilin henkilöt on valittu, tekoäly laitetaan tekemään tiedonkeruuta muun muassa sosiaalisen median kanavien, kuten Facebookin, LinkedInin tai X:n, kautta ja dataa kerätään muun muassa iästä, julkaisujen määrästä, kiinnostuksen kohteista, reaktioista tai tykkäysten määrästä. Kun nämä osuudet ovat valmiita, tekoäly etsii helposti tietojenkalasteluun lankeavia henkilöitä ja pyrkii näyttämään heille sellaista materiaalia, joka osuu henkilöiden kiinnostusten kohteisiin. Mallia pystytään kouluttamaan ja tarkentamaan käyttäjän somekäytöksen avulla, jolloin kaikki tekijät edesauttavat tietojenkalastelun onnistumisen mahdollisuuksia tarkoin valittujen profiilien keskuudessa. (Aksela ym. 2022.) Tällainen toimintamalli mahdollistaa entistä nopeamman, tarkemman, valikoidumman ja hienostuneemman tietojenkalasteluprosessin, jolloin käyttäjän vastuu verkkokäyttäytymisessä ja medialukutaidossa kasvaa. On entistäkin tärkeämpää kouluttaa henkilökuntaa sen varalta, millaisia ohjelmia tai sivustoja on sallittua käyttää työkoneilla ja -päätelaitteilla

tai millaisten viestien, sähköpostien ja yhteydenottojen kuuluisi herättää epäilystä ja jättää klikkaamatta.

Koska tekoäly mahdollistaa entistä taitavampia tietojenkalasteluyrityksiä tulevaisuudessa, myös imitaatio on syytä ottaa huomioon. Imitaatio on tekniikka, joka hyödyntää äänen syväoppimista ja luo generointijärjestelmän avulla kohteesta imitaation äänen osalta. Tarkoituksena on siis luoda halutusta henkilöstä synteettinen, aidon kuuloinen puheääni. Tällä tekniikalla on mahdollista luoda esimerkiksi väärennettyjä puheita ja ääniviestejä, joita onkin jo hyödynnetty esimerkiksi rahansiirroissa, joissa muun muassa Hong-Kongilaista pankinjohtajaa imitoitiin vuonna 2020 ja tämä johti useiden miljoonien arvosta vääriin rahansiirtoihin. Äänen imitointia on myös enenevissä määrin alettu hyödyntää videoissa, joissa ääni liitetään kuvaan ja henkilön kasvon ilmeet ja huulet synkronoidaan synteettiseen puheeseen. Tämä on mahdollista toteuttaa myös reaaliajassa, jolloin on entistä vaikeampaa hahmottaa sitä, mitä on aitoa ja mikä ei. (Aksela ym. 2022.) Tällaisten, erittäin hienostuneiden huijausten varalta on mahdollista, että tulevaisuudessa myös puhelut tai videopuhelut työelämässä joudutaan aloittamaan jollain tietyllä tunnussanalla. Tai vaihtoehtoisesti video- ja ääniviesteihin lisätään jokin varmenne, jolla pystytään varmistumaan viestin aitoudesta. Varmaa on kuitenkin se, että teknologia ja tekoäly mahdollistavat jatkuvasti uusia, kekseliäitä tapoja toimia tietojenkalastelun osalta ja niihin olisi syytä yrittää varautua ennalta parhaansa mukaan lukemalla alan uutisointia ja kouluttautumalla säännöllisesti tietoturvan osalta.

2.4 Päätelaitteiden tietoturvallisuus

Yksi yleisin alusta levittää haittaohjelmia ovat päätelaitteet, koska haittaohjelmat leviävät herkästi erilaisten sivustojen, ohjelmien tai sähköpostien kautta. Tämän vuoksi on tärkeää selventää henkilökunnalle, mitkä sivustot, järjestelmät tai ohjelmat ovat sallittuja käyttää työnantajan päätelaitteilla (F-Secure 2023d.) On erittäin suotavaa tehdä selkeä rajanveto siitä, että työnantajan antamilla päätelaitteilla saa tehdä vain työhön liittyviä asioita ja omalla vapaa-ajalla käytetään omia, henkilökohtaisia laitteita.

Päätelaitteiden suhteen tulisi huomioida, että ne ovat työntekijän vastuulla ja niiden säilytyksessä tulisikin käyttää suurta huolellisuutta. On olemassa lukuisia uutisartikkeleita tapauksista, joissa työkone on varastettu esimerkiksi autosta tai ravintolasta, jossa päätelaite on jätetty hetkeksi huomioimatta. Työhön liittyviä päätelaitteita, jotka sisältävät yritykselle kuuluvaa dataa, ei missään olosuhteissa tulisi jättää vartioimatta autoon, junaan tai muuhunkaan julkiseen paikkaan. (Järvinen 2022, 89.)

On ensisijaisen tärkeää, ettei työnantajan päätelaitteisiin kiinnitetä mitään vierasta laitetta, esimerkiksi usb-tikkua tai latausjohtoa, sillä ne voivat sisältää haittaohjelman ja olla näin ollen tietoturvariski. Tämän hetken yksi suosituimmista trendeistä on Flipper Zero-laite, joka mahdollistaa muun muassa yksinkertaisen tavan toteuttaa BadUsb-hyökkäyksen, mikäli Flipper Zero liitetään laitteen usb-porttiin. BadUsb-hyökkäys vaatii usb-laitteen, sekä siihen liitetyn koodin, jolla päätelaite saadaan toimimaan halutulla tavalla. Flipper Zeron ominaisuuksiin kuuluu BadUsb, jolloin sen käyttäminen kyseisissä hyökkäyksissä on paljon helpompaa. Tällöin Flipper Zero-laitteeseen voidaan vain lisätä haluttu koodi ja sujauttaa Flipper Zero halutun päätelaitteen usb-porttiin. BadUsb-hyökkäysten avulla päätelaitteesta voidaan varastaa tietoa, kohdelaite voidaan kaataa tai määrätä suorittamaan haluttuja komentoja. Onkin siis erityisen tärkeää, ettei päätelaitteita jätetä vartioimatta eikä vieraita laitteita liitetä päätelaitteisiin. (Leppälä 14.10.2023.)

2.4.1 Salasanat

Kun listataan asioita tietoturvasta henkilökunnan näkökulmasta, puhutaan usein salasanoista, joka onkin yksi keskeisimpiä pointteja, sillä salasanoja on kaikkialla. Salasana on käyttäjän ja palvelun välinen, yksilöllinen tunnus, jonka avulla käyttäjä saa pääsyn haluttuun ohjelmaan tai järjestelmään. (Järvinen 2022, 94.) Salasanat ovat edelleen erittäin yleinen tapa käyttää yksilöitäviä tunnuksia, mutta teknologioiden mennessä eteenpäin on salasanojen luonnekin muuttunut. Salasanoja ei välttämättä tarvitse vaihtaa enää niin usein, sillä salasanojen on nykyisin oltava paljon monimutkaisempia ja pidempiä. Koska salasanoja kohtaa edelleen useissa palvelussa, on se johtanut siihen, että niiden ulkoa oppiminen on entistä työläämpää. Tämän vuoksi mukaan on tullut monia uusia teknologioita, joilla pyritään helpottamaan salasanojen käyttöä ja turvallisuutta käyttäjän näkökulmasta katsottuna. Seuraavissa kappaleissa käydäänkin läpi tarkemmin edellä mainittuja asioita, vaikkakin on hyvä ottaa huomioon, ettei salasanoja voi jättää täysin huoletta minkään teknologian varaan.

Nykyisin tulisi ottaa huomioon, että hyvä salasana on oikeastaan salalause. Yleinen ohjeistus on, että vahvan salasanan sopiva pituus tulisi olla vähintään 12 merkkiä (Järvinen 2022, 94). Tämä ohjeistus on kuitenkin jäämässä vanhaksi, ja esimerkiksi F-Securen tietoturva-asiantuntija Jussi Koskinen vastasi Elisa Oyj:n tekemässä artikkelissa kysymykseen hyvästä salasanasta ja painotti, että vahvan salasanan pituus on 16 merkkiä (Elisa Oyj, 2023). Hive Systems julkaisi puolestaan X:ssä vuonna 2022 taulukon salasanojen merkkipituudesta, jossa salasanojen vahvuutta verrattiin siihen aikaan, mikä salasanojen murtamiseen menee ja 18 merkkiä pitkä salasana, joka sisälsi numeroita, isoja- ja pieniä kirjaimia sekä symboleita, oli taulukon vahvin salasana (Hive Systems, 18.4.2023). Edellä mainitut seikat huomioon ottaen onkin perusteltavaa suositella, että vahva salasana sisältää mielellään – ja vähintään – 18 merkkiä.

Salasanojen murtamiseen on muutamia, harmillisen toimivia vaihtoehtoja, joilla lyhyet salasanat, jotka sisältävät esimerkiksi minkään maailmassa puhutun kielen sanakirjasanoja, ovat yllättävän nopeita ja helppoja murtaa. Tästä syystä nykyisin puhutaankin enemmän salalauseista, jotka ovat pitkiä ja sisältävät mahdollisesti murresanoja, sanontoja tai mahdollisesti tarkoituksellisia kirjoitusvirheitä. Monet ohjelmat jopa vaativat nykyisin erilaisia merkkejä, numeroita, isoja- ja pieniä kirjaimia salasanoihinsa, jotta salasana on tarpeeksi vahva. (Järvinen 2022, 94.)

Salasanan tulisi aina olla henkilökohtainen, riittävän vaikea ja jokaisessa palvelussa erilainen, jotta sitä olisi vaikea murtaa tai varastaa. Kun salasana on jokaisessa palvelussa uniikki, ennaltaehkäistään myös riskiä sille, että varkaan saadessa salasanan käsiinsä varas ei pääse kaikkiin käyttäjän käyttämiin palveluihin. (Järvinen 2022, 94.) Kun otetaan huomioon, että erilaisia palveluita, joihin salasanoja vaaditaan, on lukuisia, tekevät nämä seikat salasanojen muistamisesta erittäin haastavaa, jolloin voi olla suositeltavaa käyttää luotettavia salasanojen tallennusohjelmia.

KeePass on avoimen lähdekoodin salasanojen hallinnointiohjelma, joka mahdollistaa salasanojen tallentamisen turvallisesti yhteen tietokantaan. Tietokanta on lukittu yhdellä master-salasanalla, jolloin ei tarvitse muistaa kuin yksi salasana, jolla pääsee kiinni tietokantaan. Tietokannan tiedostot ovat kryptattuja ja KeePassilla voi lisäksi generoida salasanoja halutuilla kriteereillä. KeePass on ilmainen ja ladattavissa muun muassa Windowsille, Linuxille, OS X:lle. (KeePass 2023.) Työkalu on erittäin hyvä vaihtoehto lukuisien salasanojen säilömiseen ja lisää tietoturvallisuutta mahdollistaessaan monimutkaisten, erilaisten salasanojen käytön vaihtelevasti erilaisissa ympäristöissä ilman pelkoa siitä, ettei salasanoja muista ulkoa. On myös paljon turvallisempaa tallentaa salasanat muistiin kryptattuun tietokantaan, kun kirjoittaa salasanoja lapuille tai paperille. Salasanojen ei koskaan tulisi olla esillä päätelaitteiden lähettyvillä, eikä niitä ole turvallista myöskään tallentaa selaimeen. Selaimiin tallennetut tiedot ovat paljon heikommin suojattuja, kun salasanojen hallinnointiohjelmien suojaukset ja selaimessa olevat tiedot ovat näin ollen paljon helpommin varastettavissa (Kullas, 13.3.2023).

Koska salasanojen luonne on muuttunut yhä monimutkaisemmaksi, on oletettavaa, että tulevaisuudessa SpearID FIDO2 -suojausavaimen tyyliset ratkaisut tulevat lisääntymään. FIDO, eli Fast Identity Online, on FIDO alliancen luoma standardi, jonka takana ovat muun muassa Apple, Microsoft, Google sekä useita muita pienempiä yrityksiä. FIDO-suojausavain on fyysinen usb-tikku, eli tunnisteavain, joka perustuu avainpariin. Tunnisteavaimen voi liittää kaikkiin FIDO- tai muihin kaksiosaiseen tunnistautumisen palveluihin, jolloin suojausavain toimii ikään kuin kotiavaimena. Kun suojausavain on otettu käyttöön, riittää, että käyttää vain yhtä tikkua salasanojen suojaamiseen. Koska kyseessä on fyysinen laite, ei sen salasanoja voi murtaa tai hakkeroida verkosta, jolloin suojaus-

avaimen käyttäminen lisää merkittävästi tietoturvallisuutta. Tällaiset fyysiset suojausavaimet mahdollistavat sen, että salasanat ovat itsessään täysin merkityksettömiä, eikä niitä tarvitse lainkaan muistaa, sillä samaa ”kotiavainta” voi käyttää kaikkiin palveluihin. (Spear Innovation Oy LTd, 2023.)

SpearID FIDO2-suojausavain toimii kaikissa käyttöjärjestelmissä ja sille on olemassa myös hallinta, jolloin tällaisen käyttäminen yritysympäristössä lisää merkittävästi yrityksen tietoturvaa. Kun työnantaja antaa työntekijälle avaimen, kasvaa tällöin sekä työntekijän yksityisten tilien suoja, että työnantajan tilien suoja. Työnantaja voi hallita avaimen käyttöä, mutta ei voi kontrolloida yksityisiä tilejä, jolloin työntekijän työsuhteen päättyessä - tai suojausavaimen kadotessa -, voi työnantaja sulkea työhön liittyvät osiot tikulta ja jättää avaimen työntekijän yksityiseen käyttöön, eikä kenelläkään olisi tällöin enää pääsyä yrityksen palveluihin. Suojausavaimelle on myös olemassa palautusmenetelmä, jolloin vahingon sattuessa tiedot voidaan palauttaa ongelmitta. (Spear Innovation Oy LTd, 2023.)

2.4.2 Päivitykset ja asennukset

Elämme arkea, jossa erilaisia päivityksiä on paljon ja usein. Päivityksiä ilmestyy lähes jokaiseen käyttöjärjestelmään eri päätelaitteissa. Näiden lisäksi selaimet ja ohjelmat vaativat päivityksiä, jolloin niiden yleisyys voi aiheuttaa käytösmallin, missä päivitykset sivuutetaan, eikä niitä priorisoida päivittäisessä toiminnassa. Päivitykset paikkaavat kuitenkin tietoturva-aukkoja, haavoittuvuuksia, korjaavat virheitä, eli bugeja, sekä saattavat lisätä ominaisuuksia, jonka vuoksi niiden asentaminen olisi ensisijaisen tärkeää (Järvinen 2022, 36). Päivityksen asentamatta jättäminen voi altistaa käyttöjärjestelmän, ohjelman tai laitteen tietoturvariskille, jonka vuoksi päivitykset tulisi priorisoida. Päivitykset voivat viedä aikaa ja aiheuttaa katkoja operatiiviseen toimintaan, jonka vuoksi niitä ei tarvitse tehdä välittömästi, mutta niille olisi hyvä varata aikaa työpäivän päätteeksi. Päivityksiä voidaan tarvittaessa myös automatisoida, jolloin niistä ei tarvitse huolehtia manuaalisesti, tällöin – kuten muutoinkin – on kuitenkin tärkeä huolehtia muistin määrästä ja tarkistaa, että päätelaitteessa tilaa on tarpeeksi, jotta päivitys onnistuu. (Järvinen 2022, 40.) Päivitysten lisäksi on suositeltavaa sammuttaa päätelaitteet säännöllisesti, sillä päätelaitteen sammuttaminen nollaa järjestelmän ja ennaltaehkäisee tällä tapaa esimerkiksi joidenkin ohjelmien tilttaamista. Lisäksi jotkin päivitykset vaativat sammutuksen. (El Kamel 27.7.2018.)

Päivityksiä ajatellen on parempi, että esimerkiksi tietokoneessa on pienin mahdollinen määrä sovelluksia asennettuna, jotta turhat sovellukset eivät syö levytilaa. Tämä on myös tietoturvallinen tapa toimia, sillä ylimääräiset sovellukset suurentavat haavoittuvuuksien riskiä. Kun päätelaitteisiin asennetaan sovelluksia, olisi syytä lukea käyttöehdot erityisesti työympäristöä ajatellen. Ohjelmat, nettipalvelut tai selaimet saattavat pyytää kuittauksia tai näyttää sivuillaan ilmoituksia, joissa pyydetään hyväksymään joitain tiettyjä, tarkoin määriteltyjä ehtoja. Mikäli ei kuitenkaan ole täysin

varma siitä, mitä on hyväksymässä, on suositeltavaa ottaa esimerkiksi kuva kysymyksestä ja tiedustella asiaa oman organisaation tieturvasta vastaavalta henkilöltä. Sokkohyväksymisten riski on, että voi vahingossa hyväksyä itseään tai yritystään koskevia ehtoja tai antaa luvan mahdolliselle haittaohjelmalle. (Järvinen 2022, 50.)

2.5 Toimitilojen tietoturvallisuus

Moni ei välttämättä tule ajatelleeksi toimistolleen tai työpaikalleen astuessaan, että tietoturvahaasteet kattavat myös fyysiset tilat, kuten työhuoneet tai neuvotteluhuoneet. Haasteet koskevat myös muita ympärillämme olevia oheislaitteita tai tavaroita, joita ei saateta pitää kovin suurena tietoturvariskinä niiden ei teknisten ominaisuuksien vuoksi. Kuitenkin jokainen asia, joka sisältää tietoa yrityksestä, on mahdollinen tietoturvariski, mikäli jokin ulkopuolinen taho pääsee sisälle yrityksen tiloihin. Onkin erityisen tärkeää kouluttaa henkilökuntaa myös havainnoimaan asioita ympärillään ja kiinnittämään huomiota siihen, millaisia tietoja yrityksestä on näkyvillä ja ovatko kaikki henkilöt rakennuksessa tunnistettavissa tai kulkevatko he valvotusti yrityksen tiloissa jonkin yrityksessä työskentelevän henkilön kanssa (Ulkoministeriö 2020, 36).

Vierailijoiden suhteen yrityksen olisi suotavaa luoda omat pelisäännöt ja ohjeistaa henkilöstöä siitä, kuinka vierailijoiden kanssa toimitaan vierailun aikana. On tärkeää ottaa huomioon koko prosessi alusta loppuun ja tehtävä toimintasuunnitelma sen suhteen, kuinka henkilökuntalle informoidaan tulevista vierailijoista, jotta jokainen olisi tietoinen siitä, ketä ulkopuolisia henkilöitä yrityksen tiloissa liikkuu. Tietoturvallinen tapa toimia on saattaa vierailija ulko-ovelta neuvotteluhuoneeseen ja takaisin. Jokaisen henkilökunnan jäsenen tulisi tietää, missä tiloissa vierailijat saavat olla tai mistä ovista he saavat kulkea. Tällä ennaltaehkäistään sitä, ettei kukaan ulkopuolinen näe vahingossa mitään sellaista tietoa, jota hänen ei kuuluisi nähdä. Lisäksi on tärkeää sopia, kuinka toimitaan, mikäli ulkopuolinen henkilö liikkuu yrityksen tiloissa itsenäisesti, eikä häntä ole tunnistettu. (Ulkoministeriö 2020, 36). Järvinen (87, 2020) muistuttaa teoksessaan siitä, kuinka helppoa toimittajan oli murtautua tunnettujen, suomalaisten yritysten tiloihin käyttämällä huoltomiehen haalaria sekä kantamalla tikkaita mukanaan. Henkilökunta avasi oletetulle huoltomiehelle lukittuja ovia ja päästi jopa hissiin sisälle, jolloin toimittaja pääsi yrityksen tiloihin täysin ongelmitta. Tällainen tilanne olisi ollut helposti ennaltaehkäistävissä oikeanlaisella ohjeistuksella.

2.5.1 Kulkuluvat ja vierailijat

Tietoturvallisuudesta puhuttaessa ei voida välttyä termiltä ”vähemmän oikeuden periaate”. Tähän viitataan yleisemmin, kun käsitellään käyttöoikeuksia johonkin järjestelmään tai ohjelmaan, mutta kyseinen periaate soveltuu erinomaisesti myös toimistotiloihin. Vähemmän oikeuden periaate tar-

koittaa sitä, että mahdollisimman pienelle määrälle ihmisiä annetaan mahdollisimman pienet oikeudet mahdollisimman vähäksi aikaa (Traficom 2020). Etenkin suuremmissa toimistotiloissa olisi järkevää miettiä, kuinka laajat pääsyoikeudet työntekijöillä voi olla liikkumisen suhteen ja voisiko niitä rajoittaa vaikkapa työtehtävien mukaan. Esimerkiksi suuressa tavaratalossa, jossa sijaitsee myös yrityksen pääkonttori, ei välttämättä ole tarpeellista, että edes tavaratalossa työskentelevillä myyjillä on pääsyä yrityksen toimistoon tai toimiston työntekijöillä on pääsyä esimerkiksi myymälän varastoon. Rajoitetuilla pääsyoikeuksilla pienennetään riskiä, jossa varkaalla on avaimet tai tunnukset saadessaan pienempi mahdollisuus päästä käsiksi kaikkeen mahdolliseen tietoon, kuten tietoverkkoihin, sovelluksiin tai muihin yrityssalaisuuksiin (Traficom 2020).

Kuvalliset henkilökortit sekä kulkuoikeuksilla varustettujen kulkukorttien käyttö on yrityksissä yleinen toimintamalli. Mikäli yrityksessä on käytössä esimerkiksi kuvallinen henkilökortti, on erittäin tärkeää muistuttaa henkilökuntaa niiden oikeanlaisesta käytöstä. Erityisesti suurissa yrityksissä, joissa on paljon henkilökuntaa ja kaikki eivät tunnista toisiaan, olisi ensisijaisen tärkeää, että henkilökortti olisi jatkuvasti esillä tai se pitäisi pyydettäessä pystyä näyttämään. On tärkeää, ettei yrityksen tiloissa liikkuessa päästä tiloihin ketään, ketä ei voida tunnistaa. Ulkopuolinen henkilö yrityksen tiloissa on aina sekä tietoturvallisuusriski että henkilöturvallisuusriski ja ulkopuolinen, tunnistamaton henkilö pitäisi aina saattaa sellaiseen tilaan, jossa ulkopuoliset saavat oleskella. (Järvinen & Rousku 2017, luku 2.)

Työpaikan kulunvalvontaa ajatellen rfid-tunnisteet, eli käytännössä kulkukortit tai -lätkät, ovat erittäin suosittu tapa rajoittaa ja valvoa henkilökunnan liikkumista yrityksen tiloissa. Rfid on teknologia, joka tulee sanoista Radio Frequency IDentification ja sen avulla kaksi kohdetta, esim. maksukortti ja maksupäätelaite, voivat välittää toistensa kanssa tietoa radioaaltoja hyödyntäen. Tunnistus tapahtuu automaattisesti ja niitä hyödynnetään paljon muun muassa pääsynvalvonnassa ja maksukorteissa. (mySafety 2023.) Tietoturvallisuusperiaatteita noudattaen kulkukortteja ei tulisi koskaan säilyttää samassa, yrityksen logolla varustetussa kaulanauhassa tai samassa avainnipussa henkilökortin tai muiden työpaikkaan liittyvien avainten kanssa. Kadonnut kulkukortti ei saisi paljastaa, millaiseen tilaan sillä pääsee, eikä mahdollistaa pääsyä muihin tiloihin muilla avaimilla. (Järvinen 2020, 87).

Uuden haasteen rfid-tunnisteisiin kulkukortteihin liittyen on tuonut Flipper Zero-laite, jonka muuntuu erittäin kätevästi myös digitaaliseksi yleisavaimeksi. Flipper Zero sisältää radiovastaanottimen sekä lähettimen, jonka avulla se voi kopioida rfid-tunnisteita muutamassa sekunnissa. Rfid:n ongelma on hyvin heikko salaus, jonka vuoksi sen kopioiminen on helppoa. Haasteena on kuitenkin se, että haluttu rfid-tunniste on saatava fyysisesti Flipper Zero laitteen lähelle. (Leppälä 24.8.2023.)

Näin ollen mahdollisessa kopioimistilanteessa Flipper Zeron omistajalla tulee olla anastettuna kulkukortti. Tämänkin vuoksi on suositeltavaa, ettei kulkukortteja säilytetä yrityksen muiden avainten, kulkukorttien tai logollisten avainnauhojen kanssa samassa paikassa ja että mahdollisissa katoamistapauksissa asiasta informoidaan työnantajalle pikimmiten, jotta kulkukortin kulkuoikeudet saadaan nollattua.

2.5.2 Työpisteet

Erityisesti näyttöpäätetyö sijoittuu aina johonkin työpisteeseen, olipa kyseessä sitten toimisto, kotitoimisto tai julkinen paikka. Tässä osiossa ei keskitytä julkisella paikalla työskentelyyn, sillä sen käsittely painottuu kappaleeseen ”2.7 Tietoturva etätyössä”, mutta seuraavissa kappaleissa käydään läpi sitä, kuinka paljon työtilat sekä niiden pienetkin yksityiskohdat paljastavat yrityksestä ja millaisia asioita olisi hyvä ottaa huomioon tietoturvan kannalta. Työtä tehdessä ei tule välttämättä ajatelleeksi, että myös työtilat ovat osa yrityksen imagoa sekä paljastavat herkästi toimintatapoja, työkulttuuria sekä näin ollen mahdollisia liikesalaisuuksia, jotka voivat herkästi paljastua yrityksen ulkopuolisille henkilöille joko vierailijoiden tai muiden ulkopuolisten henkilöiden kautta.

Siisti työpiste on hyvä muistisääntö, kun ajatellaan tietoturvallista työpistettä. Kaikki esillä olevat postit-laput, paperit tai muut näkyvällä olevat asiat, jotka paljastavat yrityksestä tietoa ja jotka lojuvat työpisteillä avoimesti henkilön ollessa poissa työpisteeltään, voivat paljastaa liikesalaisuuksia ja olla tietoturvariski. Huonoin esimerkki tällaisesta toiminnasta ovat postit-lapulla olevat salasanat päätelaitteen lähellä. Tällainen toimintamalli on syytä muuttaa, mutta ajattelua voidaan viedä myös pidemmälle. Lähtökohtaisesti kaikki, mitä ei tarvitse pitää esillä, ei ole järkevää olla esillä. Järvinen (2022, 51) muistuttaa teoksessaan Yrityksen tietoturvaopas, että kaikki esillä olevat kirjoitustaulut, fläppitaulut tai valkotaulut tulisi repiä tai pyyhkiä pois palaverien jälkeen sekä ylimääräiset paperitulosteet tulisi säilyttää joko lukituissa kaapeissa tai kierrättää paperisilppurin tai muun vastaavan, turvallisen keräysastian kautta. Neuvotteluhuoneisiin on helppo jättää fläppitaululle muistiinpanoja ajatellen, että ne ovat irrelevantteja tietoja ulkopuolisille. Kaikki tiedot ovat kuitenkin yrityksen tietoa ja on parempi siivota kaikki tieto pois palaverien jälkeen. (Järvinen 2022, 51.) Lisäksi neuvotteluti-loissa olisi syytä ottaa huomioon mahdollisen asian kriittisyys. Mikäli käsiteltävä asia on laadultaan erittäin salaista, on syytä ottaa huomioon mahdolliset ikkunat ja peittää näkyvyys esimerkiksi verhoilla tai kaihtimilla. Sama pätee myös omaan työpisteeseen. Mikäli esimerkiksi rakennuksen ulkopuolelta on hyvä näkyvyys päätelaitteen näytölle, olisi tällöin syytä käyttää tietokoneen tietoturvasuojaa (M3 2023).

Siisti työpiste pitää sisällään paperisten tietojen lisäksi myös digitaaliset tiedot. Työpöydille ei ole syytä jättää valvomatta mitään sellaista tietoa tai esinettä, joka sisältää yrityksen dataa. Tällaisilla

asioilla tarkoitetaan esimerkiksi muistitikkuja, ulkoisia kovalevyjä tai näytöllä avoinna olevia tiedostoja. Kun poistutaan työpisteeltä, kone olisi syytä lukita ja tietoa sisältävät esineet olisi syytä säilyttää lukituissa kaapeissa tai kassakaapeissa. Työpäivän päätteeksi olisi myös tärkeää sammuttaa tietokoneet sekä säilyttää niitä lukituissa tiloissa tai -kaapeissa. (Järvinen 2022, 52.)

2.6 Sosiaalinen media työpaikalla

Vuonna 2021 Tilastokeskuksen julkaiseman tutkimuksen mukaan vuonna 2020 lähes 70 % aikuisista suomalaisista käytti verkkoviestintäympäristöjen yhteisöpalveluita, eli tunnetummin sosiaalista mediaa (Kohvakka, Saarenmaa 2021). Muun muassa Jodel, LinkedIn, Meta, Tiktok tai X ovat palveluita, joissa on helppo olla aktiivinen viestijä, vastaanottaa tietoa sekä tuottaa itse sisältöä (Rauramo 2022). Sosiaalisessa mediassa törmääkin usein päivityksiin, jossa ihmiset jakavat tietoa työpäivistään, työpäivien operatiivisista toimistaan, toimistotiloista, työympäristöistä tai työyhteistöistään. Nämä voivat kaikki vaikuttaa täysin harmittomilta postauksilta, mutta voivat harkitsemattomasti jaettuna sisältää paljon sellaista tietoa yrityksestä, jota ei todellisuudessa suositella jaettavan. Tämän vuoksi onkin erittäin tärkeää sopia pelisäännöt sosiaalisen median käytöstä työpaikalla (Rauramo 2022). On selvää, että joidenkin yritysten imagoon saattaa jopa kuulua työympäristön näkyminen sosiaalisessa mediassa osana viestintä- ja markkinointistrategiaa, sillä tätä pidetään läpinäkyvänä. Läpinäkyvyys on vahva trendi ja Suomalaisen Työn Liiton teettämästä tutkimuksesta (2015) selviää, että läpinäkyvyys ja avoimuus luovat vahvan mielikuvan yrityksen vastuullisuudesta. Läpinäkyvyys voi siis olla tavoiteltava tila, mutta se on myös strategia, jonka säännöt olisi syytä jalkauttaa henkilökunnalle. Henkilökunnan tulisi tietää, millaisia asioita he saavat jakaa, näyttää tai kertoa työpaikastaan paljastamatta liikaa.

Työntekijää sitoo lain sekä mahdollisten erillisten sopimusten myötä salassapito- tai vaitiolovelvollisuus, jolloin työntekijällä ei ole oikeutta paljastaa työnantajan liikesalaisuuksia ulkopuolisille. Näin ollen onkin hyvä huomioida, että esimerkiksi täysin viaton sosiaaliseen mediaan postattu kuva tietokoneen näytöstä tai työvuorolistasta voi loukata pahimmillaan salassapitosopimusta (someturva 2023). Näytöllä näkyvät järjestelmät kertovat, millaisia järjestelmiä yrityksellä on käytettävissä, joka voi edesauttaa tietoturvauhkien lisääntymistä. Postaus toimistolta voi paljastaa taustalta yrityksen strategisia linjauksia mahdollisilla valkotauluilla tai seinillä. Avoimesti jaettu työvuorolista voi paljastaa ja vaarantaa muiden työntekijöiden yksityisyyttä sekä kertoa yrityksen henkilöstöstrategiasta. Esimerkkejä on lukuisia ja onkin äärimmäisen tärkeää miettiä, millainen kulttuuri sosiaalisen median suhteen missäkin yrityksessä haluaan säilyttää, millaisia asioita on sallittua jakaa ulkopuolelle ja millaisissa tiloissa on sallittua tehdä julkaisuja sosiaaliseen mediaan.

Työpaikan tietoturvallisuutta ajatellen yleisinä pidettyjä pikaviestisovelluksia, kuten WhatsAppia tai Signalia ei suositella käytettävän työelämässä, sillä sovelluksen käytössä piilee monia riskejä. Sovellusta voi olla hankala hallita, sillä sen hallinta perustuu siihen, että ryhmän ylläpitäjä päättää, ketä ryhmässä saa olla. Ryhmään voi huomaamatta päästä henkilöitä organisaation ulkopuolelta tai sinne voi jäädä henkilöitä, jotka eivät enää kuulu organisaatioon. Lisäksi haasteena on, että kaikki tiedot WhatsApp:ssa tallentuvat jäsenien omiin puhelimiin. Vaikka henkilö poistettaisiin ryhmästä, tiedot säilyvät silti puhelimessa tai varmuuskopiossa pilvessä. Suositeltavaa onkin, ettei WhatsAppin tyylisissä pikaviestisovelluksissa käytäisi lainkaan mitään työhön liittyviä keskusteluja. (Heikkilä 2020.)

2.7 Tietoturva etätyössä

Tämän opinnäytetyön aikaisemmissa kappaleissa on käsitelty tietoturvallisia toimintatapoja henkilöstön näkökulmasta läsnätyön tai lähityön näkökulmasta. Aihetta tulee kuitenkin käsitellä myös etätyön näkökulmasta, sillä Tilastokeskuksen tekemän tutkimuksen mukaan vuonna 2022 Suomessa tehtiin etätyötä viidenneksi eniten Euroopassa (Tilastokeskus 2023a). Etätyöllä tarkoitetaan ansiotyötä, joka tehdään työpaikan ulkopuolella, kuten esimerkiksi kotona tai junassa, kuitenkin siten, että siitä on sovittu työnantajan kanssa. Etätyö on luonteeltaan sellaista työtä, jonka voisi myös suorittaa työpaikalla, jolloin esimerkiksi lähetintyötä ei lasketa etätyöksi. (Tilastokeskus 2023b.) Kun läsnätyössä työpaikoilla tietoturvasta huolehtii työnantaja, etätyössä työntekijä joutuu itse ottamaan aiheesta enemmän vastuuta, jonka vuoksi tietoturvallisten toimintatapojen jalkauttaminen henkilökunnalle on tärkeää myös etätyöskentelyssä. Seuraavissa kappaleissa käsitelläänkin etätyöhön liittyviä tietoturvallisia tapoja toimia henkilökunnan näkökulmasta.

Etätyöskentelyssä verkon turvallisuus on avainasemassa. Kotitoimistolla oman, langattoman Wifi verkon turvallisuutta on syytä parantaa salamaalla liikenne. Reitittimen salasana tulisi vaihtaa oletussalasanasta ja kaikkien käyttöjärjestelmien, ohjelmien sekä selainten tulisi olla päivitetty viimeisimpiin versioihin. VPN:ää käyttämällä voi varmistaa oman yksityisyyden etätyöskentelyssä ja turvata näin ollen yhteyden ja salata verkkoliikenteen. Lisäksi virustorjunnan hankkiminen on suositeltavaa. (F-Secure 2023a.)

Kun etätyötä tehdään muualla, kuin kotona, esimerkiksi junassa tai kahvilassa, on tärkeää huomioida verkon turvallisuus sekä muut organisaation ulkopuoliset ihmiset ympärillä. Julkisen WiFi:in liittyminen ja sen käyttäminen heikentävät tietoturvaa merkittävästi. Julkisessa WiFi:ssä kuka tahansa samassa verkossa oleva voi nähdä käytetyt ja vieraillut verkkosivut sekä ne tiedot, joita on salaamattomasti lähetetty eteenpäin. Julkisten WiFi:ien tietoturvaa ei juurikaan paranna salasana, sillä mikäli sen voi pyytää kuka tahansa sitä tarvitseva, on se tällöin myös kaikkien halukkaiden

käytettävissä. Kaikki julkisiin verkkoihin liittyvät uhat eivät edes vaadi, että hakkeri on liittynyt samaan verkkoon. (F-Secure 2023c.) Oman haasteensa julkisiin, salasanattomiin WiFi-verkkoihin tuo myös Flipper Zero-laite, jonka avulla on mahdollista saada kerättyä muiden ihmisten käyttäjätunnukset sekä salasanat keräämällä tunnuksia muiden palveluntarjoajien tahojen kustannuksella (Talking Sasquach 1.5.2023, 1:12-16:32). Edellä mainittujen seikkojen vuoksi työnantajan päätelaitteilla ei suositella kirjautuvan mihinkään julkiseen verkkoon, joka on syytä ottaa huomioon etätyötä tehdessä.

Julkisissa tiloissa työskennellessä suurin riski on organisaation ulkopuoliset henkilöt. On tärkeää ymmärtää, ettei työpuheluun vastaaminen muiden ihmisten kuullen ole välttämättä kovin järkevää, sillä tällöin voi huomaamattaankin paljastaa yrityksestä tietoa, joka ei ole tarkoitettu muiden kuultavaksi. Samasta syystä on tärkeää käyttää näytön tietoturvasuojaa, eli näyttökalvoa, tietokoneella työskennellessä, jotta muut henkilöt eivät näe tietoja, joita heidän ei kuulu nähdä. Nämä säännöt olisi hyvä huomioida myös kotitoimistolla. Perheenjäsenetkin lukeutuvat organisaation ulkopuolisiin henkilöihin, eikä heilläkään tällöin ole tarvetta nähdä tietokoneen näyttöä tai kuulla palaveripuheluita. (M3 2023.)

Matkustaessa on hyvä huomioida, ettei edes hotellihuone ole hyvä säilytyspaikka, mikäli siellä ei ole lukollista kassakaappia. Erityisesti matkustaessa päätelaitteet, kuten tietokoneet, olisi hyvä sulkea, kun niitä ei käytetä, sillä tällöin parannetaan tietoturvallisuutta. Lepotilassa olevan koneen tiedostot on helpompi saada auki kun suljetun. (Järvinen 2022, 89).

2.8 Toiminta ongelmatilanteissa

On tärkeää kouluttaa henkilökuntaa tietoturvan osalta, sillä ennaltaehkäisy on paljon edullisempaa yritykselle, kun vahingon korvaaminen (Järvinen 2020, 33). On kuitenkin selvää, ettei kaikelta ole mahdollista varautua ja tällöin vahingon sattuessa on tärkeää, että jokainen henkilö organisaatiossa tietää, kuinka tulee toimia.

Ongelma- ja häiriötilanteiden varalta yrityksen johdon tehtävä on laatia toimintasuunnitelma ja jalkauttaa suunnitelma henkilökunnalle. Toimintasuunnitelman keskeisimmät pointit vahingon sattuessa ovat ensin muodostaa tilannekuva; mitä on tapahtunut ja kuinka vahinko vaikuttaa toimintaan, järjestelmään tai palveluun ja kuinka laaja ongelma on. On tärkeää rajata vahingot, jotta tiedetään, mitä lähdetään tutkimaan ja korjaamaan. Kerätään todisteet, eli tapahtumahistoria kaikkine klikkauksineen ja linkkeineen, jotta saadaan laadukas tilannekuva tapahtuneesta. Mikäli tapahtumapaikalla on ollut muita henkilöitä tai esineitä, esimerkiksi tilanteeseen on liittynyt vieras usb-tikku, on syytä ottaa nekin huomioon. Myös järjestelmien tai ohjelmien lokitiedoista olisi hyvä ottaa kopio ja pitää huolta, ettei niitä muokata millään tavalla. Työntekijän näkökulmasta nämä ovat tärkeimmät

askeleet, jotta tilanteen ratkaiseminen olisi mahdollisimman yksinkertaista. On myös ensisijaisen tärkeää, ettei saastunutta laitetta suljeta, ennen kun siihen annetaan lupa tai kerrota, millä tavoin se voidaan sammuttaa, sillä väärin sammutettu laite voi huonoimmassa tapauksessa tuhota todistusaineiston, kadottaa lokit ja jopa vaikuttaa siihen, saadaanko tietoa palautettua. Henkilökunnan näkökulmasta on myös kriittistä, että jokainen tietää, kenelle tietoturvapoikkeamista, ongelma- tai häiriötilanteista organisaatiossa informoidaan. (Järvinen 2020,236–237.)

Ongelmatilanteen aikana on syytä pohtia mahdollista viestintää, mikäli tilanne vaikuttaa muihin tahoihin. Jos kyseessä on rikos, on syytä ilmoittaa asiasta viranomaisille. Lähtökohtaisesti työntekijän näkökulmasta kriittisintä on kuitenkin kertoa ja dokumentoida tapahtumahetki tarkalleen, jotta vahingon jatkoselvitys olisi helpompaa. Tämä on tärkeää myös sen vuoksi, että voidaan jatkossa estää vahingon toistuminen. Kun tilanne on ohi, on tärkeää käydä tapahtumakulku uudelleen läpi, analysoida sitä, mitä tapahtui ja pohtia, kuinka vastaava tilanne olisi jatkossa ennaltaehkäistävissä. (Järvinen 2020, 238–240.)

3 Henkilöstön tietoturvaoppaan toteutuskuvaus

Tämän opinnäytetyön tietoturvaoppaan rakentaminen lähti liikkeelle pohtimalla oppaan rakentamisprosessia, joka muodostui seuraavanlaiseksi:

1. Tietoperustan laatiminen
2. Tietoperustan tiivistäminen
3. Oppaan rakenteen laatiminen
4. Oppaan rakenteen perusteella sisällön tuottaminen
5. Visuaalisen ilmeen rakentaminen
6. Viimeistely ja oikoluku

Ensin lähdettiin liikkeelle kohderyhmän pohtimisella. Opas haluttiin tehdä eri toimialoilla olevien yritysten henkilökunnalle siten, että siitä olisi apua sekä yrityksille, että henkilökunnalle. Toimialaa ei haluttu määrittää, sillä tietoturvaa koskien monet asiat ovat toimialariippumattomia. Kun kohderyhmä oli selvä, tuli tehdä aiherajaus. Aiherajauksen suhteen oli selvää, että liian tekniset yksityiskohdat jätettäisiin pois, jotta oppaan lukijalla ei tarvitsisi olla ict-taustaa ymmärtääkseen tietoturvaohjeistusta. Opinnäytetyön tietoperusta on rakennettu puhtaasti edellä mainittujen teemojen siivittämänä ja tietoperustaa hyödynnettiinkin täysin oppaan sisällöllisessä rakentamisessa. Ensin siis kirjoitettiin tietoperusta, jonka jälkeen luotiin opas.

Oppaan rakentamisen vaiheisiin kuului valmiin tietoperustan läpikäyminen ja tiivistäminen. Tietoperustasta napattiin kronologisessa järjestyksessä jokainen teema, joista luotiin oppaan sisällysluettelo. Jokainen teema pyrittiin asiasisällöllisesti tiivistämään muutamiin yhden, kahden lauseen kokonaisuuksiin. Oppaasta oli tarkoitus tehdä mahdollisimman helppolukuinen ja ymmärrettävä, jonka vuoksi teoreettinen osuus pyrittiin pitämään mahdollisimman lyhyenä ja vinkit tietoturvallisempaan toimintaan ilmaistiin passiivi- tai imperatiivimuotoisina lauseina. Oppaan visuaalinen ilme pyrittiin pitämään mahdollisimman selkeänä ja avarana, jotta sivut eivät täyttyisi liiallisesta informaatiosta. Helppolukuisuuden, avarien ja selkeiden sivujen tarkoitus oli puhtaasti tehdä oppaasta helposti lähestyttävä, ymmärrettävä ja kevyt lukea.

4 Pohdinta

Tämä opinnäytetyö luotiin yhteiskunnalliseen tarpeeseen ilmaiseksi avuksi yritysten henkilökunnalle tietoturvaoppaaksi. Opinnäytetyö sisältää tietoperustan liittyen tietoturvaan yritysten näkökulmasta sekä oppaan, joka on rakennettu puhtaasti edellä mainitun tietoperustan varaan tiivistetyssä muodossa. Tietoperusta ja opas perustuvat molemmat puhtaasti lähteisiin, eikä kokonaisuuden kasaamisessa ole käytetty muita laadullisia- tai määrällisiä tutkimusmenetelmiä, jotka loisivat mahdollisesti uutta tietoa. Tällöin koko työn uskottavuus perustuu siis lähteisiin ja lähteiden laadukkuuteen.

Lähdemateriaaleina on pyritty käyttämään mahdollisimman uusia, alle kolme vuotta vanhoja lähteitä, jotta opinnäytetyön luotettavuus ei kärsisi. It-alalla asiat vanhenevat nopeasti, jolloin jo pari vuotta vanhat lähteet voivat olla vanhentunutta tietoa, mikäli asia koskee teknisiä asioita. Mikäli tietoperustassa on viitattu johonkin yleisempään prosessiin tai työelämään liittyvään normiin, on tietoperustan lähteenä tällöin saatettu käyttää vanhempia lähteitä. Kriittisesti lähteitä tarkasteltuna voidaan kuitenkin todeta lähdeluettelon olevan siinä määrin suppea, että lähteitä olisi voinut olla monipuolisemmin esimerkiksi muun kielisistä lähteistä. Suomi on pieni maa ja suomalaiset tai suomenkieliset lähteet eivät yksin riitä kattamaan laajaa kokonaiskuvaa yritysten tietoturvallisuudesta, kun asiaa ajatellaan globaalilla tasolla. Monet tietoturvauhkiin tai -murtoihin liittyvät trendit saattavat rantautua Suomeen jopa pienellä viiveellä, jolloin olisi ollut hyödyllistä tutkia asiaa laajemmin myös muun kielisistä lähteistä, jotta olisi voitu luoda parempi kuva myös tulevaisuuden näkymistä Suomessa.

Oppaan tarkoitus oli olla mahdollisimman helppolukuinen ja ymmärrettävä, jotta mahdollisimman moni, eri toimialalta oleva, henkilö voisi hyötyä siitä. Oppaan ollessa valmis se luetutettiin muutamalla henkilöllä, joilla oli taustalla pitkä kokemus työelämästä, mutta ei it-alaan liittyvää tutkintoa tai taustatietämystä. Tällä tavoin saatiin kerättyä palautetta ja kehitysehdotuksia, joiden perusteella opasta muokattiin ja saatiin luotua viimeisin, julkaisukelpoinen versio. Oppaan heikkous lienee kuitenkin sen yleispätevyys. Opas on sisällöltään alkeistasoa, eikä se välttämättä tarjoa uutta tietoa henkilöille, jotka ovat saaneet tietoturvakoulutusta aiemmin tai työskentelevät it-alalla. Samalla kun opas on pyritty pitämään mahdollisimman yksinkertaisena ja sisällöltään selkeänä, kärsii sen informatiivisuus, eikä kaikkien imperatiivisten lausahduksien kausaliteetti välttämättä avaudu lukijalle, mikäli aihetta ei tutkita tarkemmin esimerkiksi opinnäytetyön tietoperustaa lukemalla. Ei ole suositeltavaa, että oppaassa kehotetaan toimimaan tietyllä tavalla, muttei kerrota syytä tähän. Se voi myös vaikuttaa oppaan uskottavuuteen negatiivisesti ja luoda sellaisen mielikuvan tekijästä, ettei hänellä ole vaadittavaa pätevyyttä tai tietotaitoa aiheeseen liittyen.

Kaiken kaikkiaan opas tarjoaa yleispätevän alkuponnahduksen asiasta tietämättömille henkilöille ja voi tarjota merkittäviä tietoturvaparannuksia monille yrityksille, joilla ei ole tarjottu aiemmin henkilöstölle minkäänlaista tietoturvakoulutusta. Opas voi myös herättää yrityksessä keskustelua tietoturvaan liittyvistä prosesseista, vastuuhenkilöistä tai pelisäännöistä. Yrityksissä voidaan huomata, että heiltä saattaa puuttua kokonaan tietoturvaan liittyviä vastuuhenkilöitä tai toimintasuunnitelmia tai että olemassa olevia prosesseja voidaan kehittää ja parantaa oppaan antamien vinkkien perusteella.

4.1 Opinnäytetyön jatkotutkimusehdotukset

Kun ajatellaan tämän opinnäytetyön jatkotutkimusehdotuksia, voitaisiin aihetta pohtia pienemmissä, spesifeimmissä osioissa yritysten näkökulmasta ja viedä tietoturvallisuusajattelua tarkemmin esimerkiksi joihinkin tiettyihin prosesseihin, kuten esimerkiksi projektien hallintaan. Tällöin tietoturvallista tapaa toimia henkilöstön näkökulmasta voitaisiin tarkastella puhtaasti projektinhallintaprosessin näkökulmasta ja pohtia tietoturvallisia toimintamalleja läpi projektien elinkaaren.

Aihetta olisi mielenkiintoista pohtia myös kvantitatiivisesta näkökulmasta tarkasteltuna. Kuten tämän opinnäytetyön alussa on todettu, niin on oletettavissa, että tietoturvauhkien määrät tulevat tulevaisuudessa nousemaan, jolloin olisi tärkeää, että yritykset kiinnittäisivät huomiota henkilökuntansa tietoturvakoulutuksiin. Olisi mielenkiintoista toteuttaa määrällinen tutkimus laajalti ja tutkia sitä, millaisella tasolla yritysten henkilökuntien tietoturvaosaaminen on ja kuinka moni, ei it-alalla työskentelevä, henkilö on saanut kuluneen kahden vuoden aikana tietoturvakoulutusta. Tällaisella aiheella voisi olla yhteiskunnallisesti merkittävä vaikutus sen osalta, että henkilökunnan tietoturvaan panostettaisiin entistä enemmän, mikäli tulokset osoittaisivat osaamisen olevan huonolla tasolla.

Lähteet

Aksela. M, Marchal. S, Patel. A, Rosenstedt, L. WithSecure. 2022. Tekoälyn mahdollistamat kyberhyökkäykset. Traficomin tutkimuksia ja selvityksiä 30/2022. Liikenne- ja viestintävirasto Traficom, Kyberturvallisuuskeskus. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/TRAFICOM_Teko%C3%A4lyn_mahdollistamat_kyberhy%C3%B6kk%C3%A4ykset%202022-12-12_web.pdf. Luettu: 10.11.2023.

Bäckström, A. 2017. Strateginen ja operatiivinen johtaminen Luettavissa: https://finfamilaatu.fi/laatukasikirja/strateginen-ja-operatiivinen-johtaminen/. Luettu: 12.11.2023.

Elisa Oyj 2023. Näin luot ja käytät vahvoja salasanoja helposti. Luettavissa: https://yrityksille.elisa.fi/ideat/nain-luot-ja-kaytat-vahvoja-salasanoja-helposti/. Luettu: 14.11.2023

El Kamel, S. 27.7.2018. Kannattaako tietokone sammuttaa vai jättää lepotilaan, ja kumpi säästää virtaa enemmän? Asiantuntijat vastaavat. Helsingin sanomat. Luettavissa: https://www.hs.fi/teknologia/art-2000005769998.html. Luettu: 9.9.2023.

F-Secure 2023. 8 tietoturvavinkkiä etätyön suojaamiseen. Luettavissa: https://www.f-secure.com/fi/articles/8-cyber-security-tips-for-remote-work. Luettu: 5.11.2023.

F-Secure 2023b. Mitä on kyberturvallisuus? Luettavissa: https://www.f-secure.com/fi/articles/what-is-cyber-security. Luettu: 7.11.2023.

F-Secure. 2023b.2023c. Onko julkinen Wi-Fi turvallinen. Luettavissa: https://www.f-secure.com/fi/articles/is-public-wi-fi-safe. Luettu 5.11.2023.

F-Secure 2023d. Mikä on tietokonevirus? Luettavissa: https://www.f-secure.com/fi/articles/what-is-a-computer-virus. Luettu:7.11.2023.

F-Secure 2023e. Mitä on tietojenkalastelu. Luettavissa: https://www.f-secure.com/fi/articles/what-is-phishing. Luettu: 7.11.2023.

Hive Systems, 18.4.2023. Are you tired of waiting? The 2023 Password Table is HERE! Read about our methodology, what's new for 2023, and what's changed since our 2022 models. http://ow.ly/Wina50NLGWh X-viesti @hivesystems. Luettavissa: https://twitter.com/hivesystems/status/1648363233714094091. Luettu: 14.12.2023.

Heikkilä, E. 2020. "Organisaation näkökulmasta Whatsapp on katastrofi", sanoo digikonsultti – mahdoton hallinnoitava, silti käytössä työpaikoilla. Luettavissa: https://yle.fi/a/3-11545657. Luettu 5.11.2023.

If 2023. Yrityksen tietoturva. Luettavissa: https://www.if.fi/yritysasiakkaat/vakuutukset/vastuuvakuutukset/tietoturvavakuutus/yrityksen-tietoturva. Luettu 6.9.2023.

Järvinen, P.2022. Yrityksen tietoturvaopas. Helsingin seudun kauppakamari / Helsingin Kamari Oy ja tekijä. Helsinki. E-kirja. Luettu: 8.9.2023.

Järvinen, P. & Rousku, K. 2017. Työpaikan tietoturvaopas. Tunnista uhat, hallitse riskit. Alma Talent Oy. E-kirja. Luettu: 6.11.2023.

Kaspersky 2023. Mustahattu-, valkohattu- ja harmaahattuhakkerien määritelmä ja selitys. Luettavissa: https://www.kaspersky.fi/resource-center/definitions/hacker-hat-types. Luettu: 14.12.2023.

KeePass 2023. KeePass Password Safe. Luettavissa: https://keepass.info/index.html. Luettu: 8.9.2020.

Kohvakka, R. Saarenmaa, K. 2021. Median merkitys on kasvanut pandemian aikana – monet ikäihmiset ovat ottaneet melkoiden digiloikan. Luettavissa: https://www2.stat.fi/tietotrendit/artikkelit/2021/median-merkitys-on-kasvanut-pandemian-aikana-monet-ikaihmiset-ovat-ottaneet-melkoisen-digiloikan/#:~:text=Vuonna%202020%20some%2Dpalveluita%20k%C3%A4ytti,lukemaan%20verkkouutisia%20ja%20seuraamaan%20nettitelevisiota. Luettu: 4.11.2023.

Kullas, J. 13.3.2023. Käytätkö tätä Chromen ominaisuutta? Ei välttämättä kannattaisi – ”Google näkee kaiken”. Tivi. Luettavissa: https://www.tivi.fi/uutiset/kaytatko-tata-chromen-ominaisuutta-ei-valttamatta-kannattaisi-google-nakee-kaiken/b84afc12-6cfe-42e9-9cf3-563723d887f2. Luettu: 19.11.2023.

Leppälä, S. 24.8.2023. Flipper Zero, osa 1: Tähän kaikkeen somesensaatioksi noussut ”hakkerin monitoimityökalu” pystyy. Mikrobitti. Luettavissa: https://www.mikrobitti.fi/uutiset/flipper-zero-osa-1-tahan-kaikkeen-somesensaatioksi-noussut-hakkerin-monitoimityokalu-pystyy/da511b22-a97e-43a3-b439-1c5a90b2df7d. Mikrobitti. Luettu: 8.11.2023.

Leppälä, S. 14.10.2023. Flipper Zero, osa 3: Älä ikinä kiinnitä tietokoneeseen vierasto usb-laitetta. Mikrobitti. Luettavissa: https://www.mikrobitti.fi/uutiset/flipper-zero-osa-3-ala-ikina-kiinnita-tietokoneeseen-vierasta-usb-laitetta/e2b24964-f3c1-462e-b635-dc9c8284b7ba. Luettu: 8.11.2023.

M3. 2023. Näytön yksityisyyssuoja ja tietosuoja. Luettavissa: https://www.3msuomi.fi/3M/fi_FI/privacy-protection-fi/. Luettu: 26.11.2023.

MySafetyOy. 2023. RFID-suojaus – suojaa lähimaksukorttisi kopioinnilta. Luettavissa: https://www.mysafety.fi/rfid-suojaus-suojaa-lahimaksukorttisi-kopioinnilta. Luettu: 25.11.2023.

Nielsen, S. 1.7.2023. Näin arvokkaita tietosi ovat. Kotimikro. Luettavissa: https://kotimikro.fi/tietoturva/tietosuoja/nain-arvokkaita-tietosi-ovat. Luettu: 11.11.2023.

Opetushallitus 2023. Tietoturvan peruskäsitteitä. Luettavissa: https://www.oph.fi/fi/koulutus-ja-tutkinnot/tietoturva-ja-suoja-koulussa. Luettu: 4.9.2023.

Poliisi 2023. Palvelunestohyökkäykset. Luettavissa: https://poliisi.fi/palvelunestohyokkays. Luettu: 7.11.2023.

Rauramo, P 2022. Sosiaalisen median työkäyttö, työsuojelunäkökulma. Luettavissa: https://ttk.fi/julkaisu/sosiaalisen-median-tyokaytto-tyosuojelunakokulma/. Luettu: 4.11.2023.

Ryhänen, N. 12.7.2020. Mitä on hallinnollinen tietoturvallisuus? Turvallisuus. Luettavissa: https://blog.seclion.fi/turvallisuus/hallinollinen-tietoturvallisuus?hs_amp=true. Luettu: 5.9.2023.

Someturva 2023. Tekeekö mielesi haukkua työpaikkaasi somessa – huomioi nämä 6 seikkaa. Luettavissa: https://www.someturva.fi/blog/criticizing-workplace-on-social-media-6-factors. Luettu: 4.11.2023.

Spear Innovation Oy LTd. 2023. SpearID FIDO2 – Unohda salasanat ja nauti turvallisuudesta. Luettavissa: https://fido2.fi/. Luettu: 19.11.2023.

Suomalaisen Työn Liitto. 2015. Selvitys: toiminnan avoimuus vahvin merkki yritysvastuullisuudesta. Luettavissa: https://suomalainentyo.fi/selvitys-toiminnan-avoimuus-vahvin-merkki-yritysvastuullisuudesta/. Luettu: 23.9.2023.

Talking Sasquach. 1.5.2023. Hacking WiFi Passwords with Flipper Zero Marauder, Wireshark and HashCat!. Video. Katsottavissa: https://youtu.be/subLBPJ3IxU?si=09PISWjHWVUNtYMc. Katsottu: 26.11.2023.

Tampereen yliopisto 2023. Mitä löytyy suomalaisesta ruokakorista? – Ostodataa kerätään jälleen tieteen hyväksi. Luettavissa: https://www.tuni.fi/fi/ajankohtaista/mita-loytyy-suomalaisesta-ruokakorista-ostodataa-kerataan-jalleen-tieteen-hyvaksi. Luettu: 12.11.2023.

Tervola, J. 7.4.2022. Kysely yrittäjille: Tietomurrot ovat liiketoimintariski – osaamisen puute on suurin tietoturvan hidaste. Kauppalehti. Luettavissa: https://www-kauppalehti-fi.ezproxy.haaga-helia.fi/uutiset/kysely-yrittajille-tietomurrot-ovat-liiketoimintariski-osaamisen-puute-on-suurin-tietoturvan-hidaste/c25e7cc7-7ecf-4186-bb2f-eae763ac3f13. Luettu: 9.11.2023.

Tietosuojavaltuutetun toimisto 2023a. Tietoturvaloukkaukset. Luettavissa: https://tietosuoja.fi/tietoturvaloukkaukset. Luettu: 12.11.2023.

Tietosuojavaltuutetun toimisto 2023b. Tietojen kalasteluun perustuvat tietoturvaloukkaukset. Luettavissa: https://tietosuoja.fi/tietojenkalastelu. Luettu: 7.11.2023.

Tilastokeskus 2023a. Suomi on etätyön yleisyydessä Euroopan toinen – tai toisella mittarilla viides. Luettavissa: https://www.sttinfo.fi/tiedote/70005454/suomi-on-etatyon-yleisyydessa-euroopan-toinen-tai-toisella-mittarilla-viides?publisherId=69818838&lang=fi. Luettu: 5.11.2023.

Tilastokeskus 2023b. Etätyö. Luettavissa: https://www.stat.fi/meta/kas/etatyo.html. Luettu: 5.11.2023.

Traficom 2023a. Tietoturva. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva. Luettu: 4.9.2023.

Traficom 2023b. Näin pidät huolta tietoturvasta kotona ja työpaikalla. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-pidat-huolta-tietoturvasta-kotona-ja-tyopaikalla. Luettu: 6.9.2023.

Traficom 2020. Pienyritysten kyberturvallisuusopas. Traficomin julkaisuja 228. Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf. Luettu 11.9.2023.

Ulkoministeriö 2020. Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille. Ulkoministeriö. Helsinki. Luettavissa: https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246. Luettu: 10.9.2023.

Valtioneuvosto 2022. Ajankohtaisselonteko turvallisuusympäristön muutoksesta. Valtioneuvoston julkaisuja 2022:18. Valtioneuvosto Helsinki 2022. Helsinki. Luettavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163999/VN_2022_18.pdf?sequence=1&isAllowed=y. Luettu: 12.11.2023.

Yle 15.2.2021. Psykoterapiakeskus Vastaamo asetettiin konkurssiin. Yle. Luettavissa: https://yle.fi/a/3-11790537. Luettu 12.11.2023.

Liitteet

Liite 1. Tietoturvaopas henkilöstölle

Tämä on toimialariippumaton tietoturvaopas, joka on tarkoitettu henkilöstölle koulutusmateriaaliksi. Oppaan tarkoituksena on edistää ja ylläpitää henkilöstön tietoturvaosaamista operatiivisessa työskentelyssään. Opas kattaa infopaketin tietoturvasta, yleisimmistä tietoturvauhkista, niiden seurauksista sekä antaa käytännön vinkkejä päivittäiseen työskentelyyn yleisellä tasolla, joita noudattamalla voidaan ennaltaehkäistä monia tietoturvariskejä. Opasta lukiessa ei tarvitse omata it-taustaa, sillä opas on luonteeltaan yleispätevä, jotta mahdollisimman monen toimialan henkilöstö hyötyisi sen sisällöstä.

Sisällys

TIETOTURVA

Mitä?

Tietoturva on tiedon turvaamista. Sen tarkoitus on säilyttää tieto eheänä, luottamuksellisena ja käytettävänä.

Eheys	Tieto on eheää, eli virheetöntä ja oikeaa. Tällöin tietoa ei pääse muokkaamaan kukaan ulkopuolinen taho.
Luottamuksellisuus	Tieto on luottamuksellista, eikä sitä pääse näkemään kukaan muu ulkopuolinen, kenellä ei tietoon ole pääsyoikeuksia.
Käytettävyys	Tieto on käytettävissä ja hyödynnettävissä palvelulupauksien mukaisesti.

Missä?

Kaikkialla, missä tietoa käsitellään digitaalisessa muodossa.

Miksi?

Tieto on erittäin arvokasta ja sen menettämisestä yrityksille seuraa mm. mainehaittoja, tietojen muokkaamista, siirtämistä tai levittämistä, häiriöitä palveluissa sekä asiakassuhteiden päättymistä. Tietoturvauhat ja -murrot ovat yleisiä ja jatkuvia. Niiden luonne vaihtelee ja kehittyy jatkuvasti, joten on syytä ajatella, että tietoturvauhat ovat riskejä, joihin kaikkien on varauduttava. Yritykset ovat hyviä kohteita, sillä esimerkiksi varastetut tietokannat voivat olla hinnaltaan hyvinkin arvokkaita pimeillä markkinoilla.

Kenelle?

Tietoturva on kaikkien vastuulla. On tärkeää ymmärtää tiedon arvo ja sen menettämisen seuraukset, jotta jokaisen olisi helpompi ymmärtää, miksi tietoturvallisuus on tärkeää.

Suurin riski?

Ihminen. Kyllä vain, tietoturvallisuuden heikoin lenkki on useimmiten ihminen. Muuttamalla päivittäisiä toimintatapojamme tietoturvallisemmaksi voimme kuitenkin vaikuttaa ympäristömme tietoturvallisuuteen merkittävästi. On tärkeää saada koulutusta tietoturvallisuuden osalta säännöllisesti ja tämän oppaan lukeminen on hyvä ensi askel.

YLEISIMMÄT TIETOTURVAUHAT JA NIIDEN SEURAUKSET

Madot, botit, troijalaiset, virukset, kalastelut, hakkeroijat, krakkeroijat jne. Edellä mainitut termit kuuluvat kaikki yhteen ja samaan teemaan: tietomurtoihin, haittaohjelmiin tai palvelunestohyökkäyksiin. Näitä kaikkia yhdistää tavoite, jossa halutaan vahingoittaa tai anastaa tietoa tai palvelua. Voi olla epäolennaista tietää teknisesti, kuinka mikäkin haittaohjelma toimii, mutta on tärkeää ymmärtää yleisimpien haittaohjelmien toimintaperiaatteet ja tavoitteet, jotta on helpompaa hahmottaa poikkeamat ja ennaltaehkäistä niiden etenemistä. Alla olevissa kuvissa jaotellaan tietoturvauhkia karkeasti kolmeen eri kategoriaan ja käydään läpi niiden yleisimmät esiintymismallit, levitystavat sekä seuraukset. On kuitenkin hyvä tiedostaa, että tietoturvauhat vaihtelevat ja kehittyvät jatkuvasti. Alla olevat jaottelut ovatkin enemmän suuntaa-antavia ja ne voivat poiketa malleista.

Tietoisku! Tunkeutumista luvattomasti johonkin järjestelmään kutsutaan usein termillä hakkerointi. Hakkerointi on kuitenkin hyvä erottaa termistä krakkerointi, sillä vaikka näillä kahdella on samat periaatteet, niillä on eri tavoite. Hakkerit toimivat usein jonkun yrityksen hyväksi ja koittavat tehdä tietoturvahyökkäyksiä parantaakseen yrityksen tietoturvaa, kun krakkerit pyrkivät hyökkäyksillään varastamaan tai vaurioittamaan tietoa. Puhekielessä ovat myös yleistyneet ilmaisut valkohattu- ja mustahattuhakkereista, joista valkohattuhakkerit edustavat hakkereita ja mustahattuhakkerit krakkereita.

Haittaohjelmat

Yleisimmät aiheuttajat:
Mato, virus, troijalainen

Yleinen levitystapa:
Sähköpostien ja tekstiviestien liitteet ja linkit, verkkosivustot, ohjelmat tai vieras esine (esim. usb-tikku)

Yleisiä seurauksia:
Verkkosivuilla hitautta, palvelu/laite ei toimi, tietoa puuttuu, verkkosivujen sisältö on muuttunut tai verkkosivut voivat kaatua kokonaan

Tietomurto

Yleisimmät aiheuttajat:
Tietojenkalastelu, krakkerit

Yleinen levitystapa:
Puhelin, sähköpostit, sähköpostien liitteet ja linkit, sosiaalinen media, vieras esine tai ulkopuolinen henkilö

Yleisiä seurauksia:
Tietoa tai järjestelmää voidaan vahingoittaa, dataa voidaan poistaa tai sitä voidaan yrittää myydä eteenpäin

Palvelunesto

Yleisimmät aiheuttajat:
Botit

Yleinen levitystapa:
Sähköpostien linkit ja liitteet, verkkosivustot, ohjelmat

Yleisiä seurauksia:
Verkkosivuilla hitautta, palvelu/laite ei toimi, tietoa puuttuu tai verkkosivut voivat kaatua kokonaan

2

PÄÄTELAITTEET

Työnantajan antamat päätelaitteet ovat työntekijän vastuulla. **Noudata siis suurta huolellisuutta käyttäessäsi niitä, olipa kyseessä tietokone, puhelin tai jokin muu saamasi laite.**

Työnantajan antamat päätelaitteet on tarkoitettu vain töitä varten.

→ Omat, henkilökohtaiset asiat hoidetaan omilla, henkilökohtaisilla laitteilla.

Riski piilee vieraissa selaimissa ja ohjelmissa, joita työnantaja ei ole varmistanut luotettaviksi.

Älä jätä työnantajan päätelaitteita vartioimatta.

→ Ei edes hetkeksi.

Työkoneita on varastettu ihmisiltä esim. lounasravintoloista, kun he ovat jättäneet koneen vartioimatta ripustaessaan takkiaan naulakkoon.

→ Älä säilytä päätelaitteita myöskään autossa.

Älä kiinnitä mitään vierasta esinettä, kuten usb-tikkua tai latausjohtoa, päätelaitteisiin.

→ Vieraat esineet voivat sisältää esim. haittaohjelmia ja olla täten tietoturvariski.

Suojaa laitteet pitkillä salasanoilla. Kirjaudu ulos, kun poistut hetkeksi paikalta.

→ Sammuta laitteet työpäivän päätteeksi.

3

SALASANAT

Salasana on käyttäjän ja palvelun välinen, yksilöllinen tunnus, jonka avulla käyttäjä saa pääsyn haluttuun ohjelmaan tai järjestelmään. Salasanat ovat edelleen erittäin yleinen tapa käyttää yksilöitäviä tunnuksia, mutta teknologioiden mennessä eteenpäin on salasanojen luonnekin muuttunut. Nykyisin tulisi ottaa huomioon, että hyvä salasana on oikeastaan salalause, jolloin sen tulisi sisältää vähintään 16 merkkiä – mielellään jopa enemmän.

Salasanojen murtamiseen on muutamia, harmillisen toimivia vaihtoehtoja, joilla lyhyet salasanat, jotka sisältävät esimerkiksi minkään maailmassa puhutun kielen sanakirjasanoja, ovat yllättävän nopeita ja helppoja murtaa. Lisäksi hyvässä salasanassa tulisi olla pieniä- ja isoja kirjaimia, merkkejä ja numeroita. Pitkiä salasanoja, joita voi olla jopa kymmenissä eri paikoissa, voi olla vaikea muistaa, jonka vuoksi salasanojen tallentaminen salasanojen omaan tallennusohjelmaan on järkevä tapa säilöä salasanoja.

HYVÄ SALASANA

- Tee salasanasta riittävän pitkä. Mielellään yli 16 merkkiä.
- Älä sisällytä salasanoihin sanakirjasanoja, esim. "kirja123" on huono salasana.
- Voit käyttää salasanoissa murresanoja tai tehdä kirjoitusvirheitä vaikeuttaaksesi salasanaa, esim. "miELuKasenKijaa".
- Kun salasanaan lisätään vielä numeroita ja merkkejä, salasanasta tulee hyvä. Esim. "miELu.!Kas4enKij%aa5".

- Käytä eri salasanoja eri palveluissa.
- Salasanoja ei tarvitse muistaa ulkoa; tallenna ne tallennusohjelmiin, esim. KeePassiin.
- Salasanan tallennusohjelmissa voi myös generoida salasanoja.
- Älä tallenna salasanoja selaimiin tai näkyviin paikkoihin, esim. post-it-lappuille tietokoneen viereen.

4

PÄIVITYKSET JA ASENNUKSET

Päivitykset paikkaavat tietoturva-aukkoja, haavoittuvuuksia, korjaavat virheitä, eli bugeja, sekä saattavat lisätä ominaisuuksia, jonka vuoksi niiden asentaminen olisi ensisijaisen tärkeää. Päivityksen asentamatta jättäminen voi altistaa käyttöjärjestelmän, ohjelman tai laitteen tietoturvariskille, jonka vuoksi päivitykset tulisi priorisoida. Päivitykset voivat viedä aikaa ja aiheuttaa katkoja operatiiviseen toimintaan, jonka vuoksi niitä ei tarvitse tehdä välittömästi, mutta niille olisi hyvä varata aikaa työpäivän päätteeksi.

Priorisoi ja asenna päivitykset työpäivän päätteeksi.

Asenna päätelaitteisiin vain tarvittavat ohjelmat.

- Ylimääräiset ohjelmat vievät turhaan muistia ja voivat heikentää laitteen tehoa.
- Ylimääräiset ohjelmat lisäävät tietoturvauhkien mahdollisuutta.

Sammuta tietokone työpäivän päätteeksi.

- Sammuttaminen nollaa järjestelmän ja ennaltaehkäisee ohjelmien tilttaamista.
- Jotkin päivitykset vaativat sammutuksen.

Älä hyväksy käyttöehtoja. tai mitään sellaista, josta et ole varma.

- Epävarmoissa tapauksissa luetuta ehdot tietoturvasta vastaavalla henkilöllä.

5

TOIMITILAT JA TYÖPISTEET

Työtä tehdessä ei tule välttämättä ajatelleeksi, että myös työtilat ovat osa yrityksen imagoa sekä paljastavat herkästi toimintatapoja, työkulttuuria sekä näin ollen mahdollisia liikesalaisuuksia, jotka voivat paljastua yrityksen ulkopuolisille henkilöille joko vierailijoiden tai muiden ulkopuolisten henkilöiden kautta.
Hyvä muistisääntö tietoturvallisesta työpisteestä on, että minkään, minkä ei tarvitse olla esillä, ei tarvitse olla esillä.

Siisti työpiste on myös tietoturvallinen työpiste.

Siivoa esillä olevat postit-laput, paperit tai muut näkyvällä olevat asiat pois.

Työpöydille ei ole syytä jättää valvomatta mitään sellaista tietoa tai esinettä, joka sisältää yrityksen dataa. Esim. muistitikkuja.

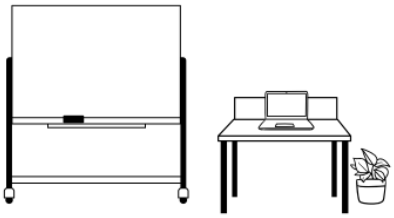
Säilytä tietoa sisältävät esineet ja asiat lukituissa kaapeissa tai kassakaapeissa.

Käytä toimistossakin näytönsuojaa, mikäli näytöllesi on hyvä näkyvyys rakennuksen ulkopuolelta.

Tietoa sisältävät paperitulosteet tulisi säilyttää lukituissa kaapeissa ja kierrättää paperisilppurin tai muun vastaavan, turvallisen keräysastian kautta.

Kaikki esillä olevat kirjoitustaulut, fläppitaulut tai valkotaulut tulisi repiä tai pyyhkiä pois palaverien jälkeen.

Ota neuvotteluhuoneissa huomioon läpikäytävän asian kriittisyys. Sulje mahdollisten ikkunoiden kaihtimet tai peitä näkyvyys verhoilla.



6

KULKULUVAT JA VIERAILIJAT

Tietoturvallisuudesta puhuttaessa ei voida välttyä termiltä ”vähemmän oikeuden periaate”. Tähän viitataan yleisemmin puhuttaessa käyttöoikeuksista järjestelmiin tai ohjelmiin, mutta kyseinen periaate soveltuu erinomaisesti myös toimistotiloihin. Vähemmän oikeuden periaate tarkoittaa sitä, että mahdollisimman pienelle määrälle ihmisiä annetaan mahdollisimman pienet oikeudet mahdollisimman vähäksi aikaa. Kulkulupia kaikille - ja kaikkialle - ei siis ole syytä jakaa perusteetta. On muutoinkin tärkeää kiinnittää huomiota ympäristöönsä ja työtiloissa liikkuviin henkilöihin. Kulkulupien tavoitteena on, ettei yrityksen tiloihin pääse kukaan ulkopuolinen taho ilman lupaa. Ulkopuolinen henkilö yrityksen tiloissa on aina sekä tietoturvallisuusriski että henkilöturvallisuusriski.

Vierailijat	Saata vierailijat neuvotteluhuoneeseen ja ulos rakennuksesta. Vaihtoehtoisesti ohjaa vierailijat kulkemaan vierailijoille tarkoitetuista käytävistä/ovista.	Vierailijoiden ei ole syytä päästä tiloihin -tai edes nähdä tiloja-, joissa työntekijät työskentelevät.		
Ympäristö	Kiinnitä huomiota ympäristössäsi kulkeviin henkilöihin. Tunnistatko henkilöt?	Mikäli työtiloissa kulkee tunnistamaton henkilö ilman saattajaa, käy saattamassa hänet odotustilaan.	Älä päästä tuntemattomia henkilöitä työtiloihin.	
Henkilökortti	Jos käytössä on kuvallinen henkilökortti, pidä kortti esillä.	Jos työtiloihin pyrkii tuntematon henkilö, vaadi saada nähdä henkilökortti.		
Kulkukortti/-lätkä	Älä koskaan säilytä kulkukorttia tai kulkulätkää kaulanauhassa, jossa näkyy yrityksen logo.	Säilytä kulkulätkät, muut avaimet ja mahdolliset henkilökortit aina erillisissä nipuissa.	Ilmoita kadonneista avaimista välittömästi, jotta oikeuksia voidaan muuttaa/nollata.	

7

SOSIAALINEN MEDIA

Sosiaalisessa mediassa voi törmätä päivityksiin, jossa ihmiset jakavat tietoa työpäivistään, työpäivien operatiivisista toimistaan, toimistotiloista, työympäristöistä tai työyhteistöistään. Nämä voivat kaikki vaikuttaa täysin harmittomilta postauksilta, mutta voivat harkitsemattomasti jaettuna sisältää paljon sellaista tietoa yrityksestä, jota ei todellisuudessa suositella jaettavan.

Työntekijää sitoo lain sekä mahdollisten erillisten sopimusten myötä salassapito- tai vaitiolovelvollisuus, jolloin työntekijällä ei ole oikeutta paljastaa työnantajan liikesalaisuuksia ulkopuolisille. Näin ollen onkin hyvä huomioida, että esimerkiksi täysin viaton sosiaaliseen mediaan postattu kuva tietokoneen näytöstä tai työvuorolistasta voi loukata pahimmillaan salassapitosopimusta. Tärkeintä onkin sopia yhteiset pelisäännöt sosiaalisen median käytöstä työpaikalla.

- Sopikaa somen pelisäännöt.
- Älä kuvaa päätelaitteiden näyttöjä.
- Älä jaa tietoja asiakkaista tai työkavereista.
- Älä käytä pikaviestisovelluksia, kuten WhatsAppia tai Signalia työasioiden käsittelyyn.

8

ETÄTYÖ JA MATKUSTUS

Tämän oppaan aikaisemmissa osioissa on käsitelty tietoturvallisia toimintatapoja henkilöstön näkökulmasta läsnätyön tai lähityön näkökulmasta. Aihetta on tärkeä käsitellä myös etätyön näkökulmasta, sillä Tilastokeskuksen tekemän tutkimuksen mukaan vuonna 2022 Suomessa tehtiin etätyötä viidenneksi eniten Euroopassa. Etätyöllä tarkoitetaan ansiotyötä, joka tehdään työpaikan ulkopuolella, kuten esimerkiksi kotona tai junassa, kuitenkin siten, että siitä on sovittu työnantajan kanssa. Etätyö on luonteeltaan sellaista työtä, jonka voisi myös suorittaa työpaikalla, jolloin esimerkiksi lähetintyötä ei lasketa etätyöksi.

Kotitoimisto

- Huolehdi, että kotitoimiston reitittimen salasana on vaihdettu oletussalasanasta.
- Käytä VPN:ää varmistamaan oma yksityisyys etätyöskentelyssä.
- Erillisen virustorjunnan hankkiminen voi olla suositeltavaa.
- Huomioi, että myös perheenjäsenet ovat ulkopuolisia.

Julkiset tilat & matkustaminen

- Huomioi muut, organisaation ulkopuoliset henkilöt ja käytä näytönsuojaa.
- Älä puhu puhelimessa, tai ääneen muiden kanssa, työasioita, mikäli paikalla on ulkopuolisia.
- Älä liity julkiseen WiFi:iin. Julkisen WiFin tietoturvallisuutta ei paranna se, että sen pääsyyn vaaditaan salasana.
- Älä säilytä päätelaitteita hotellihuoneissa, mikäli siellä ei ole kassakaappia.

9

TOIMINTA ONGELMATILANTEISSA

On äärimmäisen tärkeää kouluttaa henkilökuntaa tietoturvan osalta, sillä ennaltaehkäisy on paljon edullisempaa yritykselle, kun vahingon korvaaminen. On kuitenkin selvää, ettei kaikelta ole mahdollista varautua ja tällöin -vahingon sattuessa- onkin tärkeää, että koko henkilöstö tietää, kuinka ongelmatilanteissa toimitaan.

Tapahtuman aikana

- Älä sammuta laitetta, ennen kuin siihen annetaan lupa.
- Laadi tilannekuva: kirjoita ylös, mitä tarkalleen tapahtui? Mihin aikaan? Mitä linkkejä klikattiin, missä järjestyksessä? Oliko päätelaitteessa kiinni jokin vierasesine? Oliko paikalla ulkopuolisia? jne.
- Kerää kaikki todisteet. Nappaa myös lokitiedoista kopio, mikäli mahdollista. Älä muokkaa niitä millään tavalla.
- Ilmoita tietoturvapoikkeamasta välittömästi yrityksessänne asiasta vastaavalle henkilölle.

Tapahtuman jälkeen

- Viestintä: Kuinka laaja ongelma on? Keneen tietoturvapoikkeama, -ongelma tai -uhka vaikuttaa? Tuleeko asiasta tiedottaa yrityksen sisäisesti tai ulkoisesti?
- Käykää tapahtunut tarkalleen läpi kohta kohdalta. Analysoikaa tapahtunut. Miettikää, kuinka tilanne olisi jatkossa ennaltaehkäistävissä.

LÄHTEET

F-Secure 2023. 8 tietoturvavinkkiä etätyön suojaamiseen. Luettavissa: https://www.f-secure.com/fi/articles/8-cyber-security-tips-for-remote-work. Luettu: 5.11.2023.

Järvinen, P.2022. Yrityksen tietoturvaopas. Helsingin seudun kauppakamari / Helsingin Kamari Oy ja tekijä. Helsinki. E-kirja. Luettu: 8.9.2023.

Järvinen, P. & Rousku, K. 2017. Työpaikan tietoturvaopas. Tunnista uhat, hallitse riskit. Alma Talent Oy. E-kirja. Luettu: 6.11.2023.

Opetushallitus 2023. Tietoturvan peruskäsitteitä. Luettavissa: https://www.oph.fi/fi/koulutus-ja-tutkinnot/tietoturva-ja-suoja-koulussa. Luettu: 4.9.2023.

Rauramo, P 2022. Sosiaalisen median työkäyttö, työsuojelunäkökulma. Luettavissa: https://ttk.fi/julkaisu/sosiaalisen-median-tyokaytto-tyosuojelunakokulma/. Luettu: 4.11.2023.

Someturva 2023. Tekeekö mielesi haukkua työpaikkaasi somessa – huomioi nämä 6 seikkaa. Luettavissa: https://www.someturva.fi/blog/criticizing-workplace-on-social-media-6-factors. Luettu: 4.11.2023.

Tilastokeskus 2023a. Suomi on etätyön yleisyydessä Euroopan toinen – tai toisella mittarilla viides. Luettavissa: https://www.sttinfo.fi/tiedote/70005454/suomi-on-etatyon-yleisyydessa-euroopan-toinen-tai-toisella-mittarilla-viides?publisherId=69818838&lang=fi. Luettu: 5.11.2023.

Tilastokeskus 2023b. Etätyö. Luettavissa: https://www.stat.fi/meta/kas/etatyo.html. Luettu: 5.11.2023.

Traficom 2020. Pienyritysten kyberturvallisuusopas. Traficomin julkaisuja 228. Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf. Luettu 11.9.2023.